Microsoft Lync Server 2013 Documentation Help

Официальная документация компании Microsoft.
Дата выхода: 13/03/2013г.

Оптимизированный вариант.

Удалена информация:

1. Schema changes
2. Описание PowerShell командлетов

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

Создано:20.05.2013, 16:34

Table of Contents

1 Microsoft Lync Server 2013

Microsoft Lync Server 2013

Topic Last Modified: *2012-10-21*

Microsoft Lync Server 2013 communications software offers instant messaging (IM), presence, conferencing, and telephony solutions that can support enterprise-level collaboration requirements. The following tables list the topics in the Lync Server 2013 documentation library.

Getting Started

View online: Getting Started

Planning

View online: Planning
View online: Planning Primer: Planning for Your Organization
View online: Determining Your Infrastructure Requirements
View online: Planning for High Availability and Disaster Recovery
View online: Planning for Front End Servers, Instant Messaging, and Presence
View online: Planning for Conferencing
View online: Configuring Video
View online: Planning for External User Access
View online: Planning for Enterprise Voice
View online: Planning for Archiving
View online: Planning for Persistent Chat Server
View online: Planning for Clients and Devices in Lync Server 2013
View online: Planning for Remote Call Control
View online: Planning for Mobility

Supportability

View online: Supportability

Deployment

View online: Deployment

View online: Preparing Active Directory Domain Services for Lync Server 2013

View online: Deploying Lync Server 2013

View online: Deploying External User Access

View online: Deploying Enterprise Voice

View online: Deploying Monitoring

View online: Deploying Archiving

View online: Configuring Dial-in Conferencing

View online: Deploying Branch Sites

View online: Deploying Persistent Chat Server

View online: Deploying Clients and Devices

View online: Planning and Deploying Unified Contact Store

View online: Updating From the Evaluation Version of Lync Server 2013

View online: Deploying Remote Call Control

View online: Deploying Mobility

Migration

View online: Migration

View online: Migration from Lync Server 2010 to Lync Server 2013

View online: Migration from Office Communications Server 2007 R2 to Lync Server 2013

View online: Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server

Operations

View online: Operations

View online: Lync Server Administrative Tools

View online: Lync Server Management Shell

View online: Configuring Federation Support for a Lync Online Customer

View online: Managing Quality of Service (QoS)

View online: Using Monitoring Reports

View online: Monitoring Mobility for Performance

View online: Managing Server-to-Server Authentication (Oauth) and Partner Applications

Monitoring

View online: Using Monitoring Reports

Schema Reference

View online: Schema Reference
View online: Call Detail Recording (CDR) Database Schema
View online: Quality of Experience (QoE) Database Schema
View online: Persistent Chat Database Schema

1.1 Getting Started

Getting Started

Microsoft Lync Server 2013 >

Topic Last Modified: *2013-02-18*

Lync Server 2013 offers many features to enhance collaboration and communication in your organization. Many of these features are new compared to what was available in previous versions. The topics in this section give a brief overview of the new capabilities.

- Introduction to Lync Server 2013
- New Server Features
- New Client Features
- Release Notes for Lync Server 2013

1.1.1 Introduction to Lync Server 2013

Introduction to Lync Server 2013

Microsoft Lync Server 2013 > Getting Started >

Topic Last Modified: *2013-01-11*

Lync Server 2013 and its client software, such as Lync 2013, enable your users to connect in new ways and to stay connected, regardless of their physical location. Lync and Lync Server bring together the different ways that people communicate in a single client interface, are deployed as a unified platform, and are administered through a single management infrastructure.

This table and the following sections illustrate the major feature sets, or *workloads*, that Lync Server provides for your users.

Workload	Description
IM and presence	Instant messaging (IM) and presence help your users find and communicate with one another efficiently and effectively. IM provides an instant messaging platform with

	conversation history, and supports public IM connectivity with users of public IM networks such as MSN/Windows Live, Yahoo!, AOL, and Google Talk. **Important:** • As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013). • The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down. • More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice. Presence establishes and displays a user's personal availability and willingness to communicate through the use of common states such as **Available** or **Busy**, as well as more detailed states such as **Be Right Back** and **Do Not Disturb**. This rich presence information enables other users to immediately make effective communication choices.
Conferencing	Lync Server includes support for IM conferencing, audio conferencing, web conferencing, video conferencing, and application sharing, for both scheduled and impromptu meetings. All these meeting types are supported with a single client. Lync Server also supports dial-in conferencing so that users of public switched telephone network (PSTN) phones can participate in the audio portion of conferences. Conferences can seamlessly change and grow in real time. For example, a single conference can start as just instant messages between a few

	users, and escalate to an audio conference with desktop sharing and a larger audience instantly, easily, and without interrupting the conversation flow.
Enterprise Voice	*Enterprise Voice* is the Voice over Internet Protocol (VoIP) offering in Lync Server. It delivers a voice option to enhance or replace traditional private branch exchange (PBX) systems. In addition to the complete telephony capabilities of an IP PBX, Enterprise Voice is integrated with rich presence, IM, collaboration, and meetings. Features such as call answer, hold, resume, transfer, forward and divert are supported directly, while personalized speed dialing keys are replaced by Contacts lists, and automatic intercom is replaced with IM. Enterprise Voice supports high availability through call admission control (CAC), branch office survivability, and extended options for data resiliency.
Support for remote users	You can provide full Lync Server functionality for users who are currently outside your organization's firewalls by deploying servers called *Edge Servers* to provide a connection for these remote users. These remote users can connect to conferences by using a personal computer with Lync 2013 installed, the phone, or a web interface. Deploying Edge Servers also enables you to *federate* with partner or vendor organizations. A federated relationship enables your users to put federated users on their Contacts lists, exchange presence information and instant messages with these users, and invite them to audio calls, video calls, and conferences.
Mobile client support	Additionally, with Lync Server mobility services, your users can access Lync functionality when using supported Apple iOS, Android, Windows Phone, or Nokia mobile devices and perform such activities as sending and receiving instant messages, viewing contacts, and viewing presence. In addition, mobile devices support some Enterprise Voice features, such as click to join a conference, Call via Work, single number reach, voice mail, and missed calls. Push notifications are also supported for mobile devices that do not support applications running in the background.
Integration with other products	Lync Server integrates with several other products to provide additional benefits to your users and administrators. Meeting tools are integrated into Outlook to enable organizers to schedule a meeting or start an impromptu conference with a single click and make it just as easy for attendees to join.

	Presence information is integrated into Outlook and SharePoint. Exchange Unified Messaging (UM) provides several integration features. Users can see if they have new voice mail within Lync Server. They can click a play button in the Outlook message to hear the audio voice mail, or view a transcription of the voice mail in the notification message. Additionally, running Lync Server 2013 with Exchange 2013 enables several new features such as a unified contact store which can be accessed by clients of both products, as well as high-resolution photos for contacts which are stored in the Exchange 2013 database.
Simple deployment	To help you plan and deploy your servers and clients, Lync Server provides the Topology Builder. Topology Builder is an installation component of Lync Server. You use Topology Builder to create, adjust and publish your planned topology. It also validates your topology before you begin server installations. When you install Lync Server on individual servers, the installation program deploys the server as directed in the topology.
Simple management	After you deploy Lync Server, it offers the following powerful and streamlined management tools: • Central configuration management, which enables you to manage changes centrally and have them replicated quickly to the entire deployment. • Lync Server Control Panel, a web-based graphical user interface for administrators. With this web-based UI, Lync Server administrators can manage their systems from anywhere on the corporate network, without needing specialized management software installed on their computers. • Lync Server Management Shell command-line management tool, which is based on the Windows PowerShell command-line interface. It provides a rich command set for administration of all aspects of the product, and enables Lync Server administrators to automate repetitive tasks using a familiar tool.

While the IM and presence features are automatically installed in every Lync Server deployment, you can choose whether to deploy conferencing, Enterprise Voice, and remote user access, to tailor your deployment to your organization’s needs.

- IM and Presence
- Conferencing
- Enterprise Voice
- Scalability

1.1.1.1 IM and Presence

IM and Presence

Microsoft Lync Server 2013 > Getting Started > Introduction to Lync Server 2013 >

Topic Last Modified: *2013-01-11*

Instant messaging (IM) and presence are automatically installed in any Lync Server deployment.

Presence information enables users to approach colleagues at the right time with the right form of communication, to lead to a more productive work environment. A user's presence is a collection of information that includes availability, willingness to communicate, additional notes (such as location and status), and how the user can be contacted. Presence is enhanced in Lync Server with pictures, location information, and a rich set of presence states that includes "Off Work," "Do Not Disturb," and "Be Right Back," in addition to basic states such as "Available," "Busy," and "In a Conference." Administrators can also define customized, organization-specific presence states.

Contact management and user access options enable users to control what information others can see. Users can set different levels of contacts, each of which can view different levels of presence information.

By simply looking at a Contacts list, users can find everything they need to know at a glance. Simple colored icons indicate other users' presence status, and picture and location are also shown.

With the integration between Lync Server and other products such as Outlook and SharePoint, whenever a contact's name appears, such as in an email message or on a team website, the status and contact information is also displayed. Additionally, if you deploy Exchange 2013, Lync Server and Exchange 2013 can share a unified contact store, which can be accessed by clients of either product.

With instant messaging in Lync Server, users can quickly message each other with timely information. If you prefer, your users can also communicate with users of public IM networks such as MSN/Windows Live, Yahoo!, and AOL. Note that a separate license might be required for public IM connectivity with Windows Live, AOL, and Yahoo! Lync Server also includes Extensible Messaging and Presence Protocol (XMPP) compatibility, so your users can exchange IM messages and presence information with users of XMPP services such as Google Talk.

Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

Conversation history enables users to keep track of old IM conversations, and retrieve information that may have been communicated by IM months ago.

The Persistent Chat feature enables users to participate in multiparty, topic-based conversations that persist over time. Messages posted to chat rooms (discussion forums) can be persistent (that is, available over time), so that people from different locations and departments can participate, even when they are not all online at the same time.

If your organization must follow compliance regulations, you can deploy a message archiving feature to archive the content of instant messages for all users in your organization, or for only certain users you specify. If you also deploy Exchange 2013, your IM archive can be integrated with the In-Place Hold feature of Exchange, to provide a single administration experience for your compliance.

1.1.1.2 Conferencing

Conferencing

Microsoft Lync Server 2013 > Getting Started > Introduction to Lync Server 2013 >

Topic Last Modified: *2012-09-11*

With unified conferencing in Lync Server 2013, users can collaborate, share information, and coordinate their efforts in real time. All your users can use the full breadth of spontaneous collaboration, scheduled meetings, and meeting tools. Voice and video conferencing capabilities can be used from any location with an Internet connection, and users away from a computer can participate in audio conferences by dialing in with a public switched telephone network (PSTN) phone.

Meeting tools integrated into Outlook enable organizers to schedule a meeting or start an impromptu conference with a single click, and also make it just as easy for attendees to join. A web client extends rich conference features to participants who are not running the desktop version of Lync.

Audio and Video Conferencing

Lync Server provides a user experience that is familiar to users of traditional audio bridge services including PSTN dial-in services with touch-tone call control commands. At the same time, it incorporates powerful scheduling, joining, and management features available only with an integrated unified communications platform.

With a single click, users can schedule a meeting from Outlook. Details, such as meeting time, location, and attendees, follow the familiar Outlook template. Additionally, conference call-specific information, such as dial-in number, meeting IDs, and personal identification number (PIN) reminders, are automatically populated.

To help ensure that only the authorized people participate in a call, Lync Server provides multiple levels of authentication for participants. Users who join by using Lync are already authenticated by the Active Directory Domain Services and do not need to enter a PIN, pass code, or meeting ID.

Lync simplifies the video conferencing user experience by incorporating video into the unified client so that scheduling a meeting with video or escalating to video spontaneously is seamless and easy.

Lync Server makes it easy to add video to a standard phone call in just one click. When there are multiple participants in a video call or a conference, each user can see video from up to five other users simultaneously, or a presenter can choose just one video source to be seen exclusively by everyone.

High-definition video (resolution 1270 x 720; aspect ratio 16:9) and VGA video (resolution 640 x 480; aspect ratio 4:3) are supported for peer-to-peer calls between users running Lync on high-end computers. The resolution viewed by each participant in a single conversation may differ, depending on the video capabilities of each user’s respective hardware.

IT administrators can set policies to restrict or disable high-definition or VGA video on clients, depending on computer capability, network bandwidth, and the presence of a camera able to deliver the required resolution. These policies are enforced through in-band provisioning.

Web conferencing

Lync Server integrates conferencing sharing features such as desktop, application, attachment, whiteboard, poll and PowerPoint into the streamlined Lync. Combined with audio or video conferencing, the result is a highly immersive and collaborative session that is simple to facilitate.

To improve the overall experience of users presenting or viewing PowerPoint presentations, Lync Server 2013 employs Office Web Apps to handle PowerPoint presentations. Users can share a picture or copy and paste text using a Whiteboard in the Lync meeting. Presenters can conduct polls in the Lync meeting to solicit feedback from the attendees.

Desktop sharing enables presenters to broadcast any visuals, applications, webpages, documents, software, or part of their desktops to remote participants in real time, right from Lync. Audience members can follow along with mouse movements and keyboard input. Presenters can choose to share the entire screen or only a portion. By sharing their desktops, presenters are able to engage with their audiences in interactive product or software demos from any location.

Application sharing enables presenters to share control of software on their desktops without losing sight of participant feedback or text questions. Presenters can also delegate control of the application to meeting participants.

Dial-in Conferencing

For users that are not using a personal computer, there are several methods available for joining a Lync Server conference call. A PSTN user can dial an access number, access the meeting bridge, and then enter the meeting ID. For more secure meetings, the user can also be required to enter his or her PIN to authenticate against Active Directory. Lync Server also supports Lync Phone Edition devices, which are stand-alone IP phone devices provided by Microsoft partners.

1.1.1.3 Enterprise Voice

Enterprise Voice

Microsoft Lync Server 2013 > Getting Started > Introduction to Lync Server 2013 >

Topic Last Modified: *2013-02-11*

With Enterprise Voice, Lync Server delivers a stand-alone Voice over Internet Protocol (VoIP) offering to enhance or replace traditional private branch exchange (PBX) systems. Enterprise Voice users can call colleagues on your organization’s VoIP network or PBX, and they can call traditional phone numbers outside your organization. The Enterprise Voice solution includes common calling features such as answer, forward, transfer, hold, divert, release and park, and Enhanced 9-1-1 (E9-1-1) calling (E9-1-1 is available only in the United States.) Enterprise Voice also supports a broad range of current and older IP and USB devices.

Placing and Receiving Calls

Using Lync, users can place calls by typing a name or phone number on their keyboard, or using a dial pad displayed on their screen. Users can also initiate calls directly from their Contacts list. You can also deploy Lync Phone Edition devices, which are stand-alone IP phone devices provided by Microsoft partners.

Users can have multiple phone devices registered with Lync Server, and can switch between them easily.

Users are alerted to incoming calls on all their devices simultaneously, with customizable ringtones on IP phone devices and a notification similar to an instant message on their PC.

Users can also set a single telephone number that connects to their desk phone, PC and mobile phone, so they can be reached no matter where they are.

Basic Call Features

While on a call, a user can answer additional incoming calls or initiate outgoing calls, and the existing active call is automatically put on hold. Calls can be transferred from one user to another, either directly or after the first user speaks privately with the second user. Users can also transfer calls to another device; for example, they could transfer an active call to their mobile phone as they walk out the door of their office.

Richer Communications

When talking to another user with Lync, users can easily add text, video, or desktop sharing to the call. The Do-Not-Disturb feature is integrated with the presence settings in Lync.

With Exchange Unified Messaging (UM), Lync and Lync Server integrate with Exchange 2010 and Outlook 2010. Users can see if they have new voice mail both in their Lync window and in email. While in email they can click to play the voice mail audio in an email message, or view a transcript of the voice mail message.

Advanced Calling Features

Enterprise Voice includes several advanced calling features as well, such as delegation, team calling, Group Call Pickup, and Response Groups.

Delegation enables users to delegate call handling to one or more assistants. The delegate can perform multiple calling tasks on behalf of the user, including screening calls, placing calls, and initiating conferences.

Team calling enables a user to have incoming calls simultaneously ring the phones of teammates so that anyone on the team can answer the call.

Group Call Pickup, a new feature in Cumulative Updates for Lync Server 2013: February 2013, lets users answer incoming calls to their colleagues from their own phones. Group Call Pickup differs from team calling primarily in that an incoming call rings only at the intended recipient's phone, but any other user can choose to answer it by dialing a call pickup group number.

Response Groups can be set up for queuing and intelligently routing calls to designated agents. Common uses include IT helpdesks, human resources hotlines, and other internal contact centers.

Enterprise Voice Administration

Lync Server uses standards and published interfaces to interoperate with existing infrastructure. It supports both gateway and SIP options (such as SIP trunking) for interconnection to IP PBX systems and the PSTN networks, so that you can migrate users to Enterprise Voice over time, while minimizing disruption. Lync Server supports traditional codecs such as G.711, G.722, and G.723.1 for interoperability with traditional VoIP solutions.

With call admission control (CAC), administrators can set limits on the amount of Lync Server voice and video traffic carried on constrained network links, and specify the action to be taken if a new call would exceed the limit. The actions could include routing by an alternate path, or refusing the call.

Lync Server works with third-party Survivable Branch Appliances to provide local calling services and connection to PSTN at branch offices, in case of WAN failure at the central site.

1.1.1.4 Scalability

Scalability

Microsoft Lync Server 2013 > Getting Started > Introduction to Lync Server 2013 >

Topic Last Modified: *2012-06-25*

Lync Server is offered in two editions, Enterprise Edition and Standard Edition. The different editions are intended primarily for different sizes of organizations. As shown in the following table, both editions support all functionality in all workloads, except for high availability and disaster recovery.

Feature	**Supported in Enterprise Edition?**	**Supported in Standard Edition?**
Instant messaging (IM) and presence	Yes	Yes
Conferencing	Yes	Yes
A/V conferencing	Yes	Yes
Dial-in conferencing	Yes	Yes
Enterprise Voice	Yes	Yes
Virtualization	Yes	Yes
High availability, failover, and disaster recovery	Yes	No

1.1.2 New Server Features

New Server Features

Microsoft Lync Server 2013 > Getting Started >

Topic Last Modified: *2012-10-04*

Lync Server 2013 introduces many new features, along with significant enhancements to existing functionality. This section provides a high-level introduction to these new features and enhancements.

Discussions of new features in Lync Server 2013 are grouped among the topics in this section.

- New Management and Administration Features
- Topology Changes
- New Disaster Recovery and High Availability Features
- New Virtualization Features
- New IM and Presence Features
- New Conferencing Features
- New Features for External User Access
- New Enterprise Voice Features
- New Monitoring Features
- New Archiving Features
- New Exchange Server Integration Features
- New Persistent Chat Server Features
- New IPv6 Features
- New Unified Contact Store Feature
- New Video Features

1.1.2.1 New Management and Administration Features

New Management and Administration Features

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-09-26*

Lync Server 2013 includes the following new features to simplify the task of managing your deployment.

- Topology Builder Supports SQL Server Mirroring
- New Role Based Access Control (RBAC) Features
- Integration of Persistent Chat Management Tools

1.1.2.1.1 Topology Builder Supports SQL Server Mirroring

Topology Builder Supports SQL Server Mirroring

Getting Started > New Server Features > New Management and Administration Features >

Topic Last Modified: *2012-09-26*

Lync Server 2013 supports mirroring of your Back End Servers for high availability. You can use Topology Builder to set up mirroring, including setting up a witness.

1.1.2.1.2 New Role Based Access Control (RBAC) Features

New Role Based Access Control (RBAC) Features

See Also

Getting Started > New Server Features > New Management and Administration Features >

Topic Last Modified: *2012-09-20*

Lync Server 2013 enhances the role-based access control (RBAC) feature in two major ways. You can now create custom roles, which each have privileges for only a set of cmdlets you specify. These custom roles can also be given privilege to run scripts of cmdlets.

Additionally, Lync Server 2013 includes two new predefined roles.

- Users given the *Response Group Manager* role can manage specific Response Group queues in your organization, but not necessarily have management rights for other queues or the Response Group application as a whole.
- Users given the *Persistent Chat Manager* role can manage specific Persistent Chat rooms in your organization, but not necessarily have management rights for other rooms or the Persistent Chat feature as a whole.

Concepts

Planning for Role-Based Access Control

1.1.2.1.3 Integration of Persistent Chat Management Tools

Integration of Persistent Chat Management Tools

See Also

Getting Started > New Server Features > New Management and Administration Features >

Topic Last Modified: *2012-08-16*

Lync Server 2013 simplifies the administration of Persistent Chat Server by integrating its administration tools with the tools used for the rest of Lync Server.

Persistent Chat Server includes an administrative user interface experience integrated with the Lync Server Control Panel. Also, Persistent Chat Server includes a collection of Windows PowerShell cmdlets to administer and manage Persistent Chat Server categories, rooms (including deleting rooms and purging obsolete content), and add-ins.

Concepts

Overview of Persistent Chat Server

Other Resources

Managing Lync Server 2013, Persistent Chat Server

1.1.2.2 Topology Changes

Topology Changes

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-10-02*

Topology requirements and considerations for Lync Server 2013 are different from those for earlier releases, as described in this section.

New Front End Pools Architecture

In Lync Server 2013, the architecture of Enterprise Edition Front End pools has changed to a distributed systems architecture.

With this new architecture, the Back End database is no longer the real-time data store in a pool. Information about a particular user is kept on three Front End Servers in the pool. For each user, one Front End Server acts as the master for that user's information, and two other Front End Servers serve as replicas. If a Front End Server goes down, another Front End Server which served as a replica is automatically promoted to master.

This happens behind the scenes, and administrators do not need to know which Front End Servers are the masters for which users. This distribution of data storage improves performance and scalability within the pool, and eliminates the single point of failure of a single Back End Server.

The Back End Server serves as backup storage for user and conference data, and is also the primary storage for other databases such as the Response Group database.

These improvements also mean there are changes in how you plan and maintain your pools. We recommend that all your Enterprise Edition Front End pools include at least three Front End Servers, to provide the full number of replicas that the Front End pool architecture is designed for. Additionally, you must follow certain procedures when adding servers to a Front End pool, removing servers from it, or upgrading servers. For more information, see Topologies and Components for Front End Servers, Instant Messaging, and Presence.

Server Role Topology Changes

Some server roles that previously ran on separate servers are now consolidated into the Front End Server role, enabling you to save on hardware costs

- In Lync Server 2013, A/V Conferencing Server is always collocated with Front End Server.
- The front ends for both Monitoring and Archiving are now always collocated with Front End Server. Monitoring and Archiving each still require a separate Back-End Database, which can be collocated on the same server as the Front End Pool's back-end database, or can be hosted on separate Back-End Servers.
- Persistent Chat Server is now a server role. In Microsoft Lync Server 2010, Group Chat Server was a third-party trusted application for Microsoft Lync Server 2010. In Lync Server 2013, Persistent Chat Server functionality is implemented using three new server roles:
  - **PersistentChatService:** Main Persistent Chat Server services implemented as a front end role
  - **PersistentChatStore:** Back End Server role
  - **PersistentChatComplianceStore:** Back End Server role for Persistent Chat Compliance

1.1.2.3 New Disaster Recovery and High Availability Features

New Disaster Recovery and High Availability Features

See Also

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-09-20*

As in Lync Server 2010, the main high availability (HA) scheme for Lync Server 2013 is based on server redundancy via pooling. If a server running a certain server role fails, the other servers in the pool running the same role take the load of that server. This applies to Front End Servers, Edge Servers, Mediation Servers, and Directors.

Lync Server 2013 adds new disaster recovery measures by enabling you to pair Front End pools located in two datacenters. If one of the paired pools goes down, an administrator can fail over the users from that pool to the other pool in the pair, to provide continuation of service. This functionality does not require expensive network or hardware solutions such as storage networks or shared disks.

Lync Server 2013 also adds Back End Server high availability. This is an optional topology in which you deploy two Back End Servers for a Front End pool, and set up synchronous SQL mirroring for all the Lync databases running on the Back End Servers. You may choose whether to deploy a witness for the mirror.

Concepts

Planning for High Availability and Disaster Recovery

1.1.2.4 New Virtualization Features

New Virtualization Features

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-09-20*

Lync Server 2013 supports virtualization on both Windows Server 2012 and Windows Server 2008 R2. Support on Windows Server 2012 includes support for the Single Root I/O Virtualization (SR-IOV) capabilities. With SR-IOV, the virtual function of a physical network adapter is assigned directly to a virtual machine. This increases network throughput and reduces network latency while also reducing the host CPU overhead that is required for processing network traffic. To take advantage of SR-IOV, you must use a host server which has BIOS which supports SR-IOV, as well as use network adapters that support SR-IOV.

1.1.2.5 New IM and Presence Features

New IM and Presence Features

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-10-19*

Microsoft Lync Server 2013 adds the following new instant messaging (IM) and presence features to enrich your users' Lync experience.

- If your organization also runs Exchange 2013, users can take advantage of a unified contact store. Users can manage their contacts in Outlook 2013, Outlook Web App, as well as in Lync 2013.
- Your users can exchange instant messages and presence information with users of public IM providers that use Extensible Messaging and Presence Protocol, such as Google Talk, because of the **XMPP integration** feature of Lync Server 2013. XMPP integration built into Front End Servers and Edge Servers, and you can enable it and configure it to allow this feature.

Tasks

Enable Users for Unified Contact Store

Other Resources

Planning for Extensible Messaging and Presence Protocol (XMPP) Federation

1.1.2.6 New Conferencing Features

New Conferencing Features

See Also

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-11-08*

Lync Server 2013 introduces several new features that enhance conferencing, as described in the following list.

- **Join Launcher**
  Lync Server 2013 updates the Join launcher to validate each meeting before launching a client, and to provide support for opening a meeting in the following clients:
  - Windows Phone 7
  - Android devices
  - Apple iOS devices
  - Windows 8
  - Internet Explorer 10
- **Updated PowerPoint Sharing**
  Lync Server 2013 now uses Office Web Apps and the Office Web Apps Server (formerly known as WAC Server) to handle PowerPoint presentations. The use of Office Web Apps Server allows for higher-resolution displays and better support for PowerPoint capabilities, access to more types of mobile devices (Lync Server 2013 uses standard DHTML and JavaScript to broadcast PowerPoint presentations), and the ability for users with the appropriate privileges to scroll through a PowerPoint presentation independent of the presentation itself.
- **Gallery View and HD Video Conferencing**
  In video conferences, users can see videos of up to five conference participants at the same time.

  > **Note:**
  > Gallery View is experienced in conferences with up to 75 participants. When the conference gets larger than 75 participants, the experience reverts to single view.
- **HD Video**
  Users can experience resolutions up to HD 1080P in two-party calls and multiparty conferences.
- **Presenter Only Video Mode**
  Presenters can configure the conference so that only the video from the presenter is shown. This mode prevents distractions in large conferences when multiple video streams are available and locking to different sources. This mode also applies to video captured and provided by conferencing devices.
- **Video Spotlight**
  Presenters can configure the conference so that only the video from a selected participant who is a video source is seen by everyone in the conference. This mode also applies to video captured and provided by conferencing devices for panoramic video.
- **Dial-out Conferencing for non-Enterprise Voice users**
  Lync Server 2013 now allows participants that are not Enterprise Voice enabled to initiate dial-out calls from a meeting conference. This feature is configurable by the administrator.
- **Archiving**
  Any document that is shared during a conference is archived into Exchange 2013 data storage if Exchange Server integration is enabled with Archiving. This includes PowerPoint presentations, attachments, whiteboards and polls.

- **Meeting Invite Customization**
  Administrators can customize email invitations for online meetings using Lync Server Control Panel or Lync Server Management Shell. Customizations can include URLs for logos, help text, legal text, and footer text. All subsequent invitations will include the customizations.

Other Resources

Planning for Conferencing

1.1.2.7 New Features for External User Access

New Features for External User Access

See Also

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-10-17*

Lync Server 2013 introduces new features that extend the features and communications methods for your users. Also, Lync Server 2013 introduces changes to existing services to better integrate and extend the services that are available to your organization. Following is a summary of changes that may affect your planning and deployment of Lync Server 2013 Edge Server services.

- **Support for IPv6 addressing** Lync Server 2013 supports IPv6 addressing for all Edge Server services. If you have provided IPv6 addresses for the interfaces through configuration in Windows Server, you can use IPv6 addresses in your Edge Server configuration through the IP address configuration in Topology Builder.

Important:
Use of IPv6 addresses in Lync Server 2013 depends on support of IPv6 in routers and firewalls that your organization deploys, as well as support through your Internet service provider.

- **Extensible Messaging and Presence Protocol (XMPP)** Lync Server 2013 introduces a fully integrated XMPP proxy (deployed on the Edge Servers) and an XMPP gateway deployed on your Front End Servers. You can deploy XMPP federation as an optional component. Adding and configuring the XMPP proxy and XMPP gateway will allow your Microsoft Lync 2013 users to add contacts from XMPP-based partners for instant messaging (IM) and presence.

Note:
Currently, the XMPP services in Lync Server 2013 only provide instant messaging and presence between Lync clients and XMPP-based contacts.

- **Mobility services for Mobile clients** Introduced in a customer update for Lync Server 2010, Mobility services in Lync Server 2013 allow Microsoft Lync Mobile clients on mobile phones and tablet devices using supported Apple iOS, Android, Windows Phone, or Nokia mobile devices to perform such activities as sending and receiving instant messages, viewing contacts, and viewing presence. In addition, mobile devices support some Enterprise Voice features, such as click to join a conference, Call via Work, single number reach, voice mail, and missed call notification.

Note:
The mobility services use the reverse proxy and published services that are deployed on your Front End Servers. No changes are required to Edge Servers.

- **Directors are an optional role** The role of the Director server in the Lync Server 2013 topology has not changed. It still hosts web services, preauthenticates incoming user requests, and directs external users to their home pool. Changing the Director from a recommended role to an optional role does not diminish the value of the Director, but emphasizes reducing server count and other hardware requirements (for example, hardware load balancers for the Director) requirements without compromising features and functionality. Because the Front End Servers can do the same job as the Director with no impact to services provided, you can optionally deploy Directors if you choose to. You can safely exclude the Director with confidence that the Front End Servers will provide the same services in their place.

Concepts

Planning for and Configuring IPv6

Other Resources

Planning for External User Access
Planning for Extensible Messaging and Presence Protocol (XMPP) Federation

1.1.2.8 New Enterprise Voice Features

New Enterprise Voice Features

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2013-02-22*

Lync Server 2013 introduces several new routing and call management features that enhance Enterprise Voice.

Lync Server 2013 supports multiple trunks between Mediation Servers and gateways. A *trunk* is a logical association between a port number and Mediation Server with a port number and gateway. This means that a Mediation Server can have multiple trunks to different gateways, and a gateway can have multiple trunks to different Mediation Servers. Intertrunk routing makes it possible for Lync Server 2013 to interconnect an IP-PBX to a public switched telephone network (PSTN) gateway or to interconnect multiple IP-PBX systems. Lync Server 2013 serves as the glue (that is, the interconnection) between different telephony systems.

Microsoft Lync Server 2013 makes improvements in the areas of call forwarding, simultaneous ringing, voice mail handling, and caller ID presentation. These features enrich the Enterprise Voice call experience.

Lync Server 2013 introduces the following new enhancements to Enterprise Voice:

- New Call Features
- New Caller ID Feature
- New Voice Mail Feature
- New Trunk Feature
- New Intertrunk Feature
- New Call Management Features
- New Hybrid Voice Features

1.1.2.8.1 New Call Features

New Call Features

See Also

Getting Started > New Server Features > New Enterprise Voice Features >

Topic Last Modified: *2012-10-10*

Lync Server 2013 provides a significantly wider range of configuration options for call forwarding and simultaneous ringing. For example, if an organization does not want incoming calls to be forwarded externally to the public switched telephone network (PSTN), an administrator can apply a special voice policy to deploy this restriction.

Additionally, delegates can now set up simultaneous ringing to their mobile devices for incoming calls to their managers. This provides delegates with more flexibility, enabling them to answer calls on behalf of their manager without being tied to a desk phone.

Concepts

New Enterprise Voice Features

1.1.2.8.2 New Caller ID Feature

New Caller ID Feature

See Also

Getting Started > New Server Features > New Enterprise Voice Features >

Topic Last Modified: *2012-10-05*

Lync Server 2013 provides the administrator the flexibility to modify the format of the calling party's phone number. This Caller ID presentation feature enables the administrator to modify the calling party's phone number to a dialing format that is understood by the trunk peer, if necessary. For example, you can write a translation rule to remove +44 from the beginning of a dial string and replace it with 0144.

Now, with Lync Server 2013, both the caller's phone number and the callee's phone number can be translated into different formats, as needed. This flexibility makes it possible for Lync Server 2013 to serve as a trunk translator between different telephony systems.

Concepts

New Enterprise Voice Features

1.1.2.8.3 New Voice Mail Feature

New Voice Mail Feature

See Also

Getting Started > New Server Features > New Enterprise Voice Features >

Topic Last Modified: *2012-10-05*

Lync Server 2013 introduces Voice mail Escape, an enhancement for managing voice mail. This new feature can detect when a call has been routed to voice mail, and prevent the call from being immediately routed to the user's mobile phone voice mail without giving the user the opportunity to answer the call. This scenario occurs when the user enables simultaneous ringing to their mobile phone, and their mobile phone is turned off, out of battery, or out of range. Voicemail Escape detects that the call was immediately answered by the user's mobile phone voice mail, and disconnects the call to the mobile phone voice mail. The call continues to ring on the user's other endpoints giving the user the opportunity to answer the call. If the user does not answer the call, then the call is routed to the corporate voice mail.

Tasks

Configuring Voice Mail Escape

Concepts

New Enterprise Voice Features

1.1.2.8.4 New Trunk Feature

New Trunk Feature

See Also

Getting Started > New Server Features > New Enterprise Voice Features >

Topic Last Modified: *2012-09-21*

In Microsoft Lync Server 2013, multiple trunks between a Mediation Server and a gateway can be defined. Microsoft Lync Server 2010 only allowed for a single trunk between a Mediation Server and a PSTN gateway. This feature provides the flexibility to define additional trunks. A trunk is a logical association between a Mediation Server FQDN and listening port and a PSTN gateway FQDN and listening port. This new capability allows for easy trunk definition for resiliency (where multiple Mediation Servers can be used to route calls to the same PSTN Gateway), for PBX interoperability, where multiple trunks with different associated policies can be used between and IP-PBX and a Mediation Server, and for SIP trunk configurations where Mediation Servers at different sites have SIP trunks to the carrier referenced by the same carrier FQDN.

Concepts

New Enterprise Voice Features

1.1.2.8.5 New Intertrunk Feature

New Intertrunk Feature

See Also

Getting Started > New Server Features > New Enterprise Voice Features >

Topic Last Modified: *2012-10-08*

Lync Server 2013 provides basic session management through the support of intertrunk routing. This new capability enables Lync Server to provide call control functionalities to downstream telephony systems. With intertrunk routing, Lync Server can interconnect an IP-PBX to a public switched telephone network (PSTN) gateway so that calls from a private branch exchange (PBX) phone can be routed to the PSTN, and incoming PSTN calls can be routed to a PBX phone. Similarly, Lync Server can interconnect two or more IP-PBX systems so that calls can be placed and received between PBX phones from the different IP-PBX systems.

Concepts

Inter-Trunk Routing
New Enterprise Voice Features

1.1.2.8.6 New Call Management Features

New Call Management Features

See Also

Getting Started > New Server Features > New Enterprise Voice Features >

Topic Last Modified: *2012-12-18*

The following sections describe the changes in call management features in Lync Server 2013.

- New Response Group Application Features
- New Call Park Application Features
- New Group Call Pickup Feature

Concepts

New Enterprise Voice Features

1.1.2.8.6.1 New Response Group Application Features

New Response Group Application Features

See Also

New Server Features > New Enterprise Voice Features > New Call Management Features >

Topic Last Modified: *2012-10-29*

With the Response Group application, you can route and queue incoming calls to designated persons for special purposes, such as customer service, an internal help desk, or general telephone support for a department.

The following Response Group application features are new in Lync Server 2013:

- **Manager role**
  Lync Server 2013 introduces a new Response Group Manager role. Now there are two management roles for response groups: Response Group Manager and Response Group Administrator. While Response Group Administrators can still configure any element for any response group, Managers can configure only certain elements, only for response groups they own.
  This improvement in the administration model benefits Response Group scalability, especially for large deployment scenarios.
- **High availability**
  High availability support for the Response Group application, in the form of SQL Server mirroring, is enabled as part of the overall configuration and deployment of high availability for Lync Server 2013. If you configure for high availability and lose connectivity to the primary back-end server, Response Group functionality is not affected by leveraging the mirrored back-end server. Support for SQL Server mirroring for the Response Group application can’t be individually enabled or configured outside of the overall Lync Server 2013 high availability configuration.
- **Disaster recovery**
  Disaster recovery support for the Response Group application is enabled as part of the configuration and deployment of the paired Front End pools, which are part of the overall Lync Server 2013 disaster recovery configuration. In addition, Response Group import and export cmdlets support the failover process to the backup pool and the failback process to the primary pool or to a new pool. If an outage occurs in the primary pool, response groups can be failed over to the backup pool, and then failed back to the primary pool or to a new pool when the outage is over.

Other Resources

Planning for Response Groups

1.1.2.8.6.2 New Call Park Application Features

New Call Park Application Features

See Also

New Server Features > New Enterprise Voice Features > New Call Management Features >

Topic Last Modified: *2012-10-17*

The Call Park application makes it possible for Enterprise Voice users to put a call on hold and then retrieve it later from any phone. The user who parked the call can either dial the orbit number provided by Call Park to retrieve the parked call or use an external mechanism, such as instant messaging (IM) or a paging system, to ask someone else to retrieve the call.

Lync Server 2013 provides new disaster recovery mechanisms in the form of failover and failback processes. These failover and failback processes support recovery of Call Park functionality by allowing users who are homed in the primary pool to leverage the Call Park application of the backup pool when an outage occurs in the primary pool. Support for disaster recovery of the Call Park application is enabled as part of the configuration and deployment of paired Front End pools.

Other Resources

Planning for Call Park

1.1.2.8.6.3 New Group Call Pickup Feature

New Group Call Pickup Feature

See Also

New Server Features > New Enterprise Voice Features > New Call Management Features >

Topic Last Modified: *2013-02-12*

Cumulative Updates for Lync Server 2013: February 2013 introduces Group Call Pickup as a new Enterprise Voice feature. With Group Call Pickup, you can assign users to groups so that other users can answer incoming calls to users who are in the group from their own phones.

Group Call Pickup is based on the Call Park application. For Group Call Pickup, as with Call Park, you set up a range of virtual numbers to be used as group numbers. A user dials the group number to pick up a call that is ringing for another user who is in the group.

Other Resources

Planning for Group Call Pickup

1.1.2.8.7 New Hybrid Voice Features

New Hybrid Voice Features

See Also

Getting Started > New Server Features > New Enterprise Voice Features >

Topic Last Modified: *2012-10-22*

Hybrid voice enables customers to leverage the on-premises Enterprise Voice environment for Lync Online users as if they were on-premises Enterprise Voice users. The primary feature of a hybrid voice environment is that Lync Online users can place and receive calls from the on-premises gateway. Other important features are:

- Media bypass
- E9-1-1

These features require the tenant administrator to configure on-premises Lync settings onto Office 365.

Media bypass

Media bypass works the same way for Lync Online users as it does for on-premises users. Lync Online PSTN calls are bypassed whenever possible. This is so that the media traffic does not traverse the Lync Online data centers wherever possible.

E9-1-1

Enhanced 9-1-1 works the same way for Lync Online users as it does for on-premises users. The location information and policy of Lync Online users are automatically retrieved and transmitted during an emergency call.

⊟See Also

Concepts

New Enterprise Voice Features

Other Resources

Planning for Hybrid Voice

1.1.2.9 New Monitoring Features

New Monitoring Features

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-11-08*

Lync Server 2013 does not have a separate Monitoring Server role. Monitoring is an optional feature available on all Front End Servers in an Enterprise Edition deployment, and on Standard Edition servers, that can be implemented and configured for a pool or a site. New to Lync Server 2013, you can enable SQL Server database mirroring for your Monitoring database.

1.1.2.10 New Archiving Features

New Archiving Features

See Also

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-10-09*

Archiving in Lync Server 2013 can archive the following types of content:

- Peer-to-peer instant messages
- Conferences (meetings) that are multi-party instant messages
- Conference content, including uploaded content (for example, handouts) and event-related content (for example, joining, leaving, uploading sharing, and changes in visibility)

Additionally, Archiving in Lync Server 2013 provides new features that improve deployment and operations efficiency. These new features consist of:

- **Collocation of Archiving on Front End Servers.** Lync Server 2013 does not have a separate Archiving Server role. Archiving is an optional feature available on all Front End Servers in an Enterprise Edition deployment, and on Standard Edition servers, that can be implemented configured for a pool or a site.
- **Microsoft Exchange integration.** When you deploy Archiving, you can integrate data storage for Archiving with your existing Exchange 2013 storage for all users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold, so you don’t need to deploy separate SQL Server databases to archive Lync data. If you do not have an Exchange 2013 deployment, or if

you prefer not to integrate with it, or if you have any Lync 2013 users who are not homed on Exchange 2013 with their mailboxes put on In-Place Hold, you can deploy separate Archiving databases by using SQL Server to store archived data from Lync communications. You can use both Microsoft Exchange integration and Lync Server 2013 Archiving databases if you want to use Microsoft Exchange integration for some but not all users in your deployment. For details about In-Place Hold, see "In-Place Hold" at http://go.microsoft.com/fwlink/p/?LinkId=267500.

- **SQL Store Mirroring.** When you deploy Archiving, you can enable SQL Server database mirroring for your Archiving database.
- **Archiving of Whiteboards and Polls.** Archived conference content now includes whiteboards and polls that are shared during the meeting.

The following types of content are not archived:

- Peer-to-peer file transfers
- Audio/video for peer-to-peer instant messages and conferences
- Application sharing for peer-to-peer instant messages and conferences

Other Resources

Planning for Archiving

1.1.2.11 New Exchange Server Integration Features

New Exchange Server Integration Features

See Also

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-09-24*

Lync Server 2013 supports new features when it is deployed alongside Microsoft Exchange Server 2013, as described in the following list. For each of these features to work, both Lync Server 2013 and Exchange 2013 must be deployed.

- You can use a **unified contact store**, in which the Lync contact list is stored in Exchange 2013, and you can manage the contact store in Lync 2013, Outlook 2013, and Outlook Web App.
- You can use **high-resolution photos** for contacts. Photos with up to 648x648 pixels are stored in Exchange 2013 and made available to clients including Lync 2013, Outlook 2013, Microsoft Lync Web App, and Outlook Web App.
- You can enable **Lync Archiving integration**, which integrates Lync Server 2013 Archiving into the Exchange 2013 In-Place Hold feature, for users homed on Exchange 2013, which enables one common experience for administrators around compliance and eDiscovery.

Concepts

Planning and Deploying Unified Contact Store
How Archiving Works

1.1.2.12 New Persistent Chat Server Features

New Persistent Chat Server Features

See Also

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-10-29*

Lync Server 2013, Persistent Chat Server enables you to participate in multiparty, topic-based conversations that persist over time. Persistent Chat Server can help your organization do the following:

- Improve communication between geographically dispersed and cross-functional teams
- Broaden information awareness and participation
- Improve communication with your extended organization
- Reduce information overload
- Improve information awareness
- Increase dispersion of important knowledge and information

Lync Server 2013, Persistent Chat Server is not available in Microsoft Office 365. At this time, it is available only to on-premise Lync 2013 customers.

In Lync 2013, Persistent Chat functionality is integrated into the Lync 2013 client. As a result, users have access to Instant Messaging/Presence, Audio/Video, Conferencing, and Persistent Chat all in the Lync 2013 client. For more information about the Lync 2013 client, see http://go.microsoft.com/fwlink/p/?linkid=270877.

This topic describes feature changes between the new version of Lync Server 2013, Persistent Chat Server and the previous version (Microsoft Lync Server 2010, Group Chat), including:

- Provide an administrative experience in Lync Server Control Panel, and eliminate the Group Chat Admin Tool
- Integrate configuration settings for Persistent Chat Server into Topology Builder by eliminating the Group Chat Configuration tool
- Ease migration and upgrade from previous versions of Persistent Chat Server
- Provide high availability and disaster recovery solutions

For additional details about the latest version of Persistent Chat Server, see the following:

- The Persistent Chat Help at http://go.microsoft.com/fwlink/p/?linkid=270945 which provides a detailed list of Persistent Chat features, how they work, and how to use them while running Persistent Chat Server.
- The Planning for Persistent Chat Server in the Planning documentation, Deploying Persistent Chat Server in the Deployment documentation, Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server in the Migration documentation, and Managing Lync Server 2013, Persistent Chat Server in the Operations documentation, all of which provide instructions for setting up Persistent Chat Server.
- The Persistent Chat Server Documentation.msi file (Windows Installer file) lets users access comprehensive offline documentation about Persistent Chat Server.

Key Topology Changes for Persistent Chat Server

The following high-level changes for Persistent Chat Server include:

Persistent Chat Server is now a server role. In Microsoft Lync Server 2010, Group Chat Server was a third-party trusted application for Microsoft Lync Server 2010. Persistent Chat can be added to your Lync Server 2013 topology by using Topology Builder. In Lync Server 2013, Persistent Chat Server functionality is implemented by using three new server roles:

- **PersistentChatService:** This is the front end role for Persistent Chat. In Standard Edition deployments, Persistent Chat Server Service Role is collocated on the Standard Edition server deployed by Bootstrapper, like any other Lync Server role. In Enterprise Edition deployments, Persistent Chat Service Role is deployed on stand-alone computers by Bootstrapper, like any other Lync Server role.

- **PersistentChatStore:** Back End Server that corresponds to the Persistent Chat content database, where all the chat content is stored.
- **PersistentChatComplianceStore:** Back End Server role that corresponds to the Persistent Chat Compliance database, where all compliance events are stored.

These Persistent Chat Server roles are optional, and are installed only by customers who want comprehensive Persistent Chat Server functionality. The **PersistentChatComplianceStore** role is needed only if you choose to deploy Persistent Chat Compliance.

The **PersistentChatService** role runs two services:

- Persistent Chat service
- Persistent Chat Compliance service

Having these services run on each Persistent Chat Server provides high availability for these services in a multiserver Persistent Chat Server pool.

Additionally, to support the file upload and download in Persistent Chat rooms, Persistent Chat Server includes a web service. Previously, this service was collocated on the Persistent Chat Server, Front End Server and required Internet Information Services (IIS) to be installed as a prerequisite. In Lync Server 2013 Persistent Chat Server, the File Upload/Download web service is collocated with the Lync Server 2013 Front End Server. As a side effect, Internet Information Services (IIS) is no longer a prerequisite for Persistent Chat Server. The File Upload/Download web service is identified as **PersistentChat** in the Internet Information Services (IIS) Manager.

Important:

The **PersistentChatService** role can run on the same server as a Lync Server 2013 Front End Server only if that Front End Server is a Standard Edition Front End Server. The **PersistentChatService** role cannot run independently of a Lync Server 2013 Front End Server. It can be installed only in the context of a Lync Server 2013 deployment.

In Persistent Chat Server, Lookup service has been eliminated. In Lync Server 2010, Group Chat, the Lookup service ran on every Group Chat Server Front End Server, and performed routing to one of the Channel Servers. Lync Server 2013 relies on routing by using contact objects, where each Persistent Chat Server pool is represented by a contact object that is used by the Lync Server Front End Servers to identify and route requests to an appropriate Persistent Chat Server pool, and to one of the computers running Persistent Chat Server in the pool.

In Lync Server 2013, there are Compliance service modifications:

- In Lync Server 2010, the Compliance service ran stand-alone (non-collocated), and only on a single server. The Compliance service now runs on all the Persistent Chat Server Front End Servers, alongside the Persistent Chat service, and thereby provides high availability in a multiserver Persistent Chat Server pool. A single compliance adapter can be configured to extract data from the compliance database and into one of the other systems (XML file, Exchange-hosted archives, and so on). Persistent Chat Server includes an XML adapter.
- The Message Queuing (also known as MSMQ) queue that is shared by the Persistent Chat service and the Compliance service on each Persistent Chat Server Front End Server is now a private queue shared only by the two services. All compliance services write to the same Compliance Back End database. They also all read from that database, for the purpose of sending the data to their instance of the adapter. The Compliance Back End Server is

represented as a new Back End Server role.

Important:

As in previous versions, all compliance data is processed only once. The data may be processed by any of the adapter instances invoked by the compliance service running on the various Lync Server 2013, Persistent Chat Server computers. In Persistent Chat Server, any one of the adapter instances could process the data.

Note:

For information about installing Message Queuing, see Install Operating Systems and Prerequisite Software on Servers in the Deployment documentation.

In Lync Server 2013, there are improvements in both high availability and disaster recovery:

- High availability improvements: SQL Server mirroring is used to provide high availability for the Persistent Chat Server content database and Persistent Chat compliance database within a data center (in-site).
- Disaster recovery improvements: Persistent Chat Server supports a stretched pool architecture that enables a single Persistent Chat Server pool to be stretched across two sites (that is, a single logical pool in the topology, with servers in the pool physically located across two sites). SQL Server Log Shipping is used for cross-site disaster recovery.

For more information about high availability and disaster recovery, see Configuring Persistent Chat Server for High Availability and Disaster Recovery in the Deployment documentation.

Key Administration and Management Changes for Persistent Chat Server

Lync Server 2013 has made it easier to administer and manage Persistent Chat Server by providing:

- Unified administration and management. Lync Server 2013 makes it easier to manage and administer Persistent Chat Server by using tools that are already familiar to Lync administrators. Persistent Chat Server includes an administrative user interface experience that is integrated with the Lync Server Control Panel, which addresses performance issues with the previous versions of the Group Chat Server user interface. Also, Persistent Chat Server includes a collection of Windows PowerShell cmdlets to administer and manage Persistent Chat Server categories, Persistent Chat Server rooms (including deleting rooms and purging obsolete content), and add-ins.
- Simplified administration model. Lync Server 2013 has changed and simplified the Persistent Chat Server model by addressing the following key customer requirements:
  - Remove the complex nested hierarchies of scopes and categories.
  - Support to define deny lists as well as allowed lists (scopes) for current MindAlign customers who are planning to migrate to Persistent Chat Server.

What’s Different about User Roles from Previous Group Chat Server Versions?

Lync Server 2010, Group Chat had a user administrator role, a chat room administrator role and a Lync Server administrator role that could manage add-ins. Persistent Chat Server simply provides a Persistent Chat Administrator role (which is similar to other Lync

Server role-based access control (RBAC) roles). Anyone who is a member of this RBAC role can manage chat rooms, add-ins, and categories (and therefore gain user access for these categories), and configuration of the Persistent Chat Server pool.

What's Different about Chat Room Categories from Previous Group Chat Server Versions?

Chat room categories can no longer be nested, and the root category can no longer be modified. AllowedMembers/DeniedMembers comprise what a scope used to be in legacy Group Chat Server versions (except that it didn't support specifying a Denied list). Scopes can no longer be overridden, because there are no nested categories. A Persistent Chat Administrator in Lync Server 2013 can create and manage chat room categories. As part of creating and managing chat room categories, a Persistent Chat Administrator can configure principals (Active Directory groups/containers/users) that have access to be members/creators of chat rooms of a particular category. A Persistent Chat Administrator can also add DeniedMembers to a category, and these become explicit exclusions to the allowed list. DeniedMembers override what's in AllowedMembers.

What's Different about Chat Room Properties from Previous Group Chat Server Versions?

A new concept of open chat rooms exists in Lync Server 2013, Persistent Chat Server. All allowed members can join the chat room, without exclusive membership.

The following chat room properties that were included in previous versions of Persistent Chat Server have been eliminated:

- Topic: A Room now only has a Description.
- Create New Member list: In Persistent Chat Server, all chat rooms start with empty membership (and can maximize to a membership equaling the Allowed Members).
- File Upload: Used to be a setting per chat room to control whether file upload/ downloads were allowed. This is now set only the category level and applies to all rooms in that category.
- Chat History: Used to be a setting per chat room to control if Chat History was enabled, but is now set only at the category level and applies to all rooms in that category.
- Invites: A room always inherits the Invites setting for the category; or it can be turned off on the room. A room cannot turn on Invites if the category was previously set to Invites off.

What's Different about Policies from Previous Group Chat Server Versions?

Persistent Chat Server has a new Lync policy enabled with Persistent Chat, per user/pool/ site/global settings. In the Lync 2013 client, the Persistent Chat environment is available only for users who are enabled by policy for Persistent Chat (either directly or through the pool/site/global setting).

Previous versions of Group Chat Server did not have any policies integrated into the Lync

Server policies. On a per user and per category/room basis, by using the **Can Upload Files** per user feature, you could make the user a User administrator, a chat room administrator, or configure the user's ability to upload files. The Persistent Chat Server **File Upload** feature is just per category.

Logging

Logging for Persistent Chat Server and System Center Operations Manager is integrated into the Lync Server 2013 trace logging.

⊟See Also

Other Resources

Planning for Persistent Chat Server

1.1.2.13 New IPv6 Features

New IPv6 Features

See Also

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-08-16*

Lync Server 2013 includes support for IPv6 addresses. Due to an increasing number of devices requiring IP addresses, the number of available IPv4 addresses, which are 32-bit addresses, is running out. IPv6 provides a much larger number of available addresses, because it uses 128-bit addresses. Use of IPv6 addresses in your environment depends on support for IPv6 in the devices you use.

Because many existing devices do not yet support IPv6, a complete transition from IPv4 to IPv6 is likely to take several years. Therefore, Lync Server 2013 includes support for network environments with only IPv4 addresses, only IPv6 addresses, and dual-stack (both IPv4 and IPv6) addresses.

Concepts

Planning for and Configuring IPv6

1.1.2.14 New Unified Contact Store Feature

New Unified Contact Store Feature

See Also

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-09-13*

Lync Server 2013 introduces unified contact store. Unified contact store allows users to keep all their contact information in Microsoft Exchange Server 2013. After users' Lync contacts are migrated to Exchange 2013, the users can access and manage their contacts from Lync 2013, Outlook, or Outlook Web App, and their Favorites stay synchronized. For example, if a user adds a contact to Favorites in Outlook, the contact appears in the Favorites group in Lync 2013. Users do not need to be logged in to Lync to manage their contacts from Outlook or Outlook Web App.

Unified contact store is enabled by default. You can enable or disable users for unified contact store globally, by site, by tenant, or by individuals or groups of individuals.

Concepts

Planning and Deploying Unified Contact Store

1.1.2.15 New Video Features

New Video Features

See Also

Microsoft Lync Server 2013 > Getting Started > New Server Features >

Topic Last Modified: *2012-08-16*

Lync Server 2013 introduces the following new video features:

- **HD video** Users can experience resolutions up to HD 1080P in two-party calls and multiparty conferences.
- **Gallery View** In video conferences that have more than two people, users can see videos of participants in the conference. If the conference has more than five participants, video of only the most active participants appear in the top row, and a photo appears for the other participants.
- **H.264 video** The H.264 video codec is now the default for encoding video on Lync 2013 clients. H.264 video supports a greater range of resolutions and frame rates, and improves video scalability.

Other Resources

Configuring Video

1.1.3 New Client Features

New Client Features

Microsoft Lync Server 2013 > Getting Started >

Topic Last Modified: *2012-06-04*

The following sections describe new features and deployment updates for Lync Server 2013 clients.

- What's New for Clients
- What's New for Devices

1.1.3.1 What's New for Clients

What's New for Clients

See Also

Microsoft Lync Server 2013 > Getting Started > New Client Features >

Topic Last Modified: *2013-02-19*

Microsoft Lync 2013 has a redesigned user interface and important new features. For administrators, the client is now included with the Office setup program, providing a more streamlined approach to deploying Office and customizing clients in your organization.

Note:
For an illustrated view of Lync 2013 user interface updates, see "What's New in Lync 2013" at http://go.microsoft.com/fwlink/?LinkId=273885.

Integration with Office Setup

The Lync 2013 client and the Online Meeting Add-in for Lync 2013—which supports meeting management from within the Outlook messaging and collaboration client—are now both included with the Office 2013 Setup program.

In previous versions of Lync and Office Communicator, you could use Windows Installer properties to customize and control the Office installation. Because Lync 2013 is integrated with Office setup, you can use the following methods to customize Lync 2013 setup:

- Use the Office Customization Tool (OCT)
- Use the Config.xml to perform installation tasks
- Use Setup Command-Line Options

Note:

The Lync 2013 setup program does not uninstall previous versions of Lync or Office Communicator. The Lync 2013 client installs side-by-side with other Lync or Office Communicator clients

For details, see Deploying Lync Clients.

Group Policy Deployment

Because Lync 2013 is now included in Office setup, the method for deploying Lync Group Policy settings has changed. In previous versions of Lync and Office Communicator, you could use the Communicator.adm to define Group Policy settings, whereas in Lync 2013 you can now use the Lync ADMX and ADML administrative templates that are provided along with the Office Group Policy Administrative Templates.

For details, see Group Policy Settings for Lync 2013.

Outlook Scheduling Add-in Updates

The Online Meeting Add-in for Lync 2013 includes meeting invite customization and new meeting options.

- Administrators can customize the organization’s meeting invitations by adding a custom logo, a support URL, a legal disclaimer URL, or custom footer text. For details, see Customizing the Online Meeting Add-in.
- New attendee mute controls allow meeting organizers to schedule conferences that have attendee audio and video muted by default.

Virtual Desktop Infrastructure Plug-in

The Lync 2013 client now supports audio and video in a Virtual Desktop Infrastructure (VDI) environment. A user can connect an audio or video device (for example, a headset or a camera) to the local computer (for example, a thin client or repurposed computer). The user can connect to the virtual machine, sign in to the Lync 2013 client that is running on the virtual machine, and participate in real-time audio and video communication as though the client is running locally. The following features are supported in a virtual desktop environment:

- Device integration for audio and video, including the following:
  - Call controls from the device
  - Presence integration on the device
  - Multiple HID (human interface device) support
- Location and emergency services support.
- Support for all Lync modalities, including IM, audio, video, application sharing, desktop sharing, PowerPoint sharing, whiteboard, and file transfer.
- Audio and video support in person-to-person calls and conference calls.

For information about deploying the VDI plug-in, see Deploying the Lync VDI Plug-in.

Video Enhancements

Several new features significantly enhance the video experience for conference participants.

- Video is enhanced with face detection and smart framing, so that a participant's video moves to help keep them centered in the frame.
- High-definition video is now supported in two-party calls and multiparty conferences. Users can experience resolutions up to HD 1080P.
- Participants can select from different meeting layouts: Gallery View shows all participants' pictures or videos; Speaker View shows the meeting content and only the current speaker's video or picture; Presentation View shows meeting content only; Compact View shows just the meeting controls.
- With the new Gallery feature, participants can see multiple video feeds at the same time. If the conference has more than five participants, video feeds of only the most active participants appear in the top row, and pictures appear for the other participants.
- Participants can use video pinning to select one or more of the available video feeds to be visible at all times.
- Presenters can use the Video Spotlight feature to select one person's video feed so that every participant in the meeting sees that participant only.

Chat Room Integration

Lync 2013 now integrates the features previously provided by Lync 2010 Group Chat. A separate group chat client is no longer required.

- From within Lync 2013, users can search for chat rooms, add chat rooms to their contacts, monitor chat room activity, and read and post messages.
- Users can create topic feeds so that they'll be notified if someone in one of their chat rooms adds a post containing specific keywords.
- With the new **Persistent Chat** options page, users can set notification alerts and sounds that apply when people post messages to their chat rooms.

Lync Web App Updates

Lync Web App is the web-based conferencing client for Lync Server 2013 meetings. In this release, the addition of computer audio and video to Lync Web App provides a complete in-meeting experience for anyone who doesn't have a Lync client installed locally. Meeting participants have access to all collaboration and sharing features and presenter meeting controls.

When a user tries to join a meeting but doesn't have a locally installed client, Lync Web App opens. If you want to allow additional options for joining the meeting, you can configure the Meeting Join page; see Configuring the Meeting Join Page in the Deployment documentation.

Because of the enhancements to Lync Web App, an updated version of Attendee isn't available for Lync Server 2013. Lync Web App is the client of choice for participants outside your organization. No local client installation is required, although audio, video, and sharing features require a plug-in to be installed at first use.

Lync 2013 for Mobile Clients Updates

In addition to enhanced presence, contacts, and IM capabilities, Lync 2013 mobile clients now provide voice and video calling over the Internet and cellular data connections. With a single tap of the meeting link in a calendar item, mobile users can join Lync voice and video meetings. For more information about Lync 2013 mobile clients, see Planning for Mobile Clients.

Lync 2013 User Interface Updates

Accessibility Updates

Lync 2013 incorporates several new accessibility features.

- Lync 2013 supports high DPI resolution, enabling users to scale text and graphics for 125% and 150% dots per inch.
- Lync provides high-contrast support so that the user interface remains fully functional when used with high contrast themes in Windows.
- Lync offers more than 100 keyboard shortcuts so that users can access important functions without a mouse. For example, users can press Alt+C to accept a call, or Alt + I to ignore it, without having to tab or set the focus. Pressing (Alt+Q) ends a call, (Ctrl+N) starts OneNote, and (Alt+T) opens the Tools menu.
- Extensive screen reader support in Lync 2013 ensures that all notifications, incoming requests, and instant messages are read aloud when a screen reader is enabled.

Presence While Sharing

When Lync detects that a user is sharing, Lync automatically assigns the user a Presenting presence status. This status blocks all incoming communications unless the sender is assigned the Workgroup privacy relationship. If the user is using the sharing feature entirely on a secondary monitor, Lync does not assign a Presenting presence status.

Conversation Window Updates

The redesigned Conversation window provides quicker access to important features.

- With the new tabbed conversations feature, users can now keep all their IMs and chat rooms in one Conversation window. The tabs along the left side of the Conversation window let users navigate easily among all active conversations.
- Users can pop out an individual conversation into a separate window, and then resize the window. They can also pop the window back into the main Conversation window.
- Lync 2013 reopens a user’s conversations when the user signs out and signs back in to Lync.
- Users can quickly add IM, video, program sharing, desktop sharing, or web conferencing tools (whiteboard, meeting notes, shared notebooks, and attachments) to any conversation.
- In a meeting where video or content is being shared, users can pop out the meeting video or shared content, and then resize the window.

Lync Main Window Updates

The new streamlined look retains familiar features such as the **What’s happening today?** note field, the status selector, and the **Set Your Location** selector.

- When chat rooms are enabled, users see a new **Chat Rooms** icon on the main Lync page. With the **Chat Rooms** icon, users can quickly access their chat rooms and filters.
- Users can click the view icons to switch to the **Contacts** view, **Chat Rooms** view, **Conversations** view, or **Phone** view.
- If users have been migrated to Exchange 2013, they can upload a high resolution picture.

Contacts View and Contact Card Updates

Lync 2013 gives users different ways to view contacts and groups in their **Contacts** view.

- With the new unified contact store, after users' Lync contacts are migrated to Exchange 2013, the users can access and manage their contacts from Lync 2013, Outlook, or Outlook Web App, and their Favorites stay synchronized. For example, if a user adds a contact to Favorites in Outlook, the contact appears in the Favorites group in Lync 2013.
- If you have added and configured the XMPP proxy and XMPP gateway, users can add contacts from XMPP-based partners for instant messaging and presence.
- A new **Add a Contact That's Not in My Organization** feature gives users an easy way to add people who are external to the organization.
- A new **Favorites** group lets users build a list of people users contact most often for quicker access.
- Users can use the new **Contacts List** options page to choose how users want to sort and display contacts. Users can select an expanded, two-line view that shows contacts' pictures, or a condensed one-line view. Users can also sort contacts alphabetically or by availability.

Conferencing Updates

Lync 2013 offers several enhancements to conferencing features.

- Depending on the type of meeting, users can now mute the audience and allow or block video sharing when scheduling the meeting. These options are available on the **Meeting Options** page and are recommended for large meetings with more than 20 participants.
- Easy to use audio controls in the meeting room allow the user to control audio options, such as mute, unmute, change device, and so on.
- When sharing programs, users can select multiple programs to share if they need to work with more than one program.
- Users can now upload presentations that contain video clips by uploading the PowerPoint file, and pointing the mouse over the slide to display video controls, such as play, pause, and audio controls.
- While in a meeting, users can merge another open conversation into the meeting by using **Merge This Call Into** on the **More Options** (**...**) menu.
- To see the participants' names, users can hover the mouse over the **View Participants** button, or click **Show Participant List** to dock the panel in the meeting.
- Depending on the meeting type, users can select from several different content and participant views.
- Meeting recordings are automatically saved in a format that plays in Windows Media Player (MP4). Users can easily share the file with anyone, or use the **Publish** feature in recording manager to post the recording on a shared location.
- OneNote enables new ways to collaborate in a meeting. During a meeting, users can take notes with OneNote for personal use after the meeting, or use shared notebooks and co-edit with meeting participants in real time. All team members can access the shared notes to contribute information, brainstorm ideas, or use the notebook pages as a virtual whiteboard. People and content shared in the meeting are automatically added to the Notes.
- Users can switch between content types using **Share content and lead meeting activities** at the bottom of the meeting room. Users can also use the **Manage Presentable Content** menu to choose which content they want to share.

⊟See Also

Other Resources

Planning for Clients

1.1.3.2 What's New for Devices

What's New for Devices

See Also

Microsoft Lync Server 2013 > Getting Started > New Client Features >

Topic Last Modified: *2012-06-22*

Lync Server 2013 includes Lync Phone Edition, software that runs on qualified devices and provides traditional and advanced telephony features, integrated security, manageability, and more. Lync Phone Edition works the same way with Lync Server 2013 as it does with Lync Server 2010. For details about the newest features related to devices, see What's New for Devices in the Lync Server 2010 TechNet Library.

Other Resources

Planning for Devices
Deploying Devices

1.1.4 Release Notes for Lync Server 2013

Release Notes for Lync Server 2013

Microsoft Lync Server 2013 > Getting Started >

Topic Last Modified: *2013-03-12*

Welcome to the Lync Server 2013 Release Notes. Refer to this file for information regarding known issues about Lync Server 2013.

About this document

This document contains important information that you should know before you deploy and use Lync Server 2013. For details about Lync Server 2013, refer to the Microsoft Lync Server 2013 documentation.

This document contains the following sections:

Lync Server

If Lync Server Storage Service data replication fails, administrators will need to check performance counters for stale Storage Service queue items (3225121)

Issue:

The Lync Server Storage Service uses Windows Fabric for replication. If data is deleted on a primary Front End Server, but the deletion on a secondary Front End Server fails—for example, if there is an unexpected shutdown or error on the Front End Server—data can be left behind and "orphaned." The orphaned data can cause performance to degrade and waste drive space.

Workaround:

To work around this issue, if the events LYSS_DB_SPACE_USED_ERROR (Id=32058) and LYSS_DB_SPACE_USED_CRITICAL (Id=32059) are generated in the event log, administrators should check the performance counter on the Front End Server under **LS:LYSS - Storage Service API** with a name of **LYSS - Current number of Storage Service stale queue items**. If this performance counter has a high value—for example, greater than 50,000—then the administrator should run the CleanuUpStorageServiceData.exe tool in the Lync Server 2013 Resource Kit, which will delete all orphaned data from the pool. For details about the tool, see the Lync Server 2013 Resource Kit documentation.

Whenever the IP Address configuration is changed for a server or pool, Lync Server services need to be restarted (3212447)

Issue:

When the IP Address configuration is changed for a Lync Server 2013 deployment, such as changing from IPv4 to Dual Stack, or from Dual Stack to Ipv6, not all server components pick up the configuration change until the services are restarted.

Workaround:

To work around this issue, restart Lync Server services after changing the IP Address configuration for the deployment. To do so, run the following cmdlets in the Lync Server Management Shell:

```
Stop-CsWindowsService -graceful
```

```
Start-CsWindowsService
```

The dial-in conferencing synthetic transaction cmdlet is no longer available in the Lync Server 2013 Management Pack (3212342)

Issue:

The dial-in conferencing synthetic transaction cmdlet **Test-CsDialInConferencing** is no longer available in the Lync Server 2013 Management Pack.

Workaround:

Use of the Dial-In Conferencing Synthetic Transaction cmdlet **Test-CsDialInConferencing** is supported only internally to an enterprise.

Administrators may continue to use the cmdlet in Lync Server Management Shell for troubleshooting purposes. If required, an enterprise can also develop a private management pack to run the cmdlet internally.

The Centralized Logging Service stops if network traffic is disrupted when log files are being copied to network share (3212464)

Issue:

When the Centralized Logging Service is configured to use a network path (the value of the CacheFileNetworkFolder parameter of the **Get-CsClsConfiguration** cmdlet is a valid UNC path), cached log files are copied to the network share. If there is a disruption in network traffic while the files are being copied, an exception will occur that will cause the centralized logging service to stop.

The service is configured to automatically restart up to three times, so the service will recover from the first three exceptions.

Workaround:

There is no workaround for this issue. To identify the issue, monitor the event log for Event ID 7031 from the "Service Control Manager" that logs when the "Lync Server Centralized Logging Service Agent" service has terminated unexpectedly. If this happens more than three times, manually restart the service by using the **Start-CsWindowService** cmdlet.

Storage Service Queue Items need to be imported manually (3211368)

Issue:

Lync Server 2013 stores data about conferencing and instant messaging, such as archived messages and call detail recording (CDR), on a database on each Front End Server. The data is stored in the database while it is being processed before being delivered to the intended destination. To improve performance, Lync Server 2013 periodically exports the queue items from the local database that are not processed for an extended period of time, and saves them on the file store. If the file store is unavailable, the items are stored on each Front End Server. The same operation occurs to prevent data loss during pool failover.

During the export operation, the Lync Server Storage Service records every stage in the event log with event IDs of 32075 (full flush operation is started), 32076 (full flush is completed), 32082 (maintenance level flush is started), 32083 (maintenance level flush is completed), 32089 (flush occurred due to filling up of database). This data will not automatically be imported back to the system to be processed and delivered to its final destination (SQL Server or Exchange Server).

Workaround:

To import the data to the system, administrators will need to use the ImportStorageServiceData tool in the Lync Server Resource Kit, which will add the data back into the system to be processed and delivered to its final destination.

Address Book Web Query searches will fail if the default value for UseNormalizationRules is changed to False (3175514)

Issue:

If the default value for UseNormalizationRules is changed to False, Address Book Web Query searches will fail. After the default value is changed, Lync Client users will not be able to use Lync Address Book web query to search for users.

Workaround:

If the default value for UseNormalizationRules is set to False so that users can use phone numbers as defined in Active Directory Domain Services (AD DS) without Lync Server 2013 applying normalization rules, work around this issue by doing the following:

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Do one of the following:
    - If your deployment includes only Lync Server 2013 servers, run the following cmdlet at the global level to change the values for

UseNormalizationRules and IgnoreGenericRules to True:

```
Set-CsAddressBookConfiguration -identity <XdsIdentity> -UseN
```

- If your deployment includes a combination of Lync Server 2013 and Lync Server 2010 or Office Communications Server 2007 R2, run the following cmdlet and assign it to each Lync Server 2013 pool in the topology:

```
new-csAddressBookConfiguration -identity <XdsIdentity> -UseN
```

3. Wait for CMS replication to occur on all pools.
4. Modify the phone normalization rules file for your deployment to clear the content. The file is on the file share of each Lync Server 2013 pool. If the file is not present, then create an empty file named "Company_Phone_Number_Normalization_Rules.txt."
5. Wait several minutes for all Front End pools to read the new files.
6. Run the following cmdlet on each Lync Server 2013 pool in your deployment.

```
Update-csAddressBook
```

Address Book Server error event 20154 is generated once daily for each Lync 2013 pool (3195918)

Issue:

Lync Server 2013 Address Book Server will generate error event 20154 once every day when performing daily maintenance. The error is also generated every time an administrator runs the **Update-csAddressBook** cmdlet, even when the update is successful. However, this error event can safely be ignored when the update is successful.

Workaround:

When you encounter this error event, run the following cmdlet:

```
Debug-csAddressBookReplication -Poolfqdn <Pool FQDN for which the event was gener
```

If the cmdlet reports that there are no unindexed or abandoned objects, the error event 20154 can be safely ignored.

Additionally, the Key Health Indicator (KHI) "Address Book Users Correctly Indexed" should be turned off in System Center Operations Manager.

Requests may fail when IPv6 is configured on an Edge pool (3205810)

Issue:

When IPv6 is configured on an Edge pool, some requests to the Edge pool may fail.

Workaround:

To work around this issue, do not configure an Edge pool with IPv6.

The invoke-csPoolFailback cmdlet may fail during pool failback (3206153)

Issue:

When attempting to fail back a pool, the **invoke-csPoolFailback** cmdlet may fail with the error, "Failed to complete hydration process after repeated attempts."

Workaround:

To work around this issue, run the cmdlet again, and wait until the cmdlet succeeds. Note that the failback process can take several minutes to complete. It may take up to 60 minutes for a pool with 20,000 users.

Data loss may occur when you add a Front End Server to an already established pool (3015990) – Hybrid, Lync Online

Issue:

You may encounter this issue in an environment where a pool has more than one Front End Server, and you either restart one of the Front End Servers, or add a new Front End Server that was not previously part of the pool.

Users whose data is being archived may experience data loss until a stable distribution of data archiving is established for the pool. This period of potential data loss is limited to 15 minutes for person-to-person conversations, and 30 minutes for conferences.

Workaround:

When you perform maintenance, instead of starting Front End Servers in the pool one by one, you should fail over the pool to another pool, and then perform maintenance tasks on the servers. You can also make the service unavailable before performing maintenance tasks, and then restore availability when maintenance is complete.

Administrators cannot get licensee count by using the Get-CsClientAccessLicense cmdlet (3012255)

Issue:

Administrators cannot get accurate client license usage by using the **Get-CsClientAccessLicense** cmdlet.

Workaround:

To check the server license type, you can run the **Get-CsService** cmdlet to retrieve the fully qualified domain names (FDQNs) of all databases. If the FQDN of the Front End Server is the same as the FQDN of the back-end database, the license is a Standard edition license. Otherwise, the license is an Enterprise edition license.

Client licensee count is not accurately reported (3010175)

Issue:

When determining client license counts, you may experience the following conditions:

1. **Inaccurate license count for mobile users**
   The license count is based on the number of unique IP addresses for device-based users. The license count will be limited in the following ways:
   - Licenses will be overcounted if the IP address for the user changes during Lync sessions. This can occur when a user connects to Lync Server from more than one location with a desktop client.
   - Licenses will be undercounted if a user connects with a mobile client, because the IP address for the device cannot be determined.
2. **Licenses are counted twice for public switched telephone network (PSTN) calls to Lync client, Lync client calls to PSTN lines, and Lync calls forwarded to PSTN lines**
   In the following scenarios, two additional licenses will be counted instead of one because both the phone number and the Lync user are counted to determine the number of licenses used. To obtain accurate licensing data, manually remove the licenses generated by a phone number.
   - A PSTN phone call to Lync
   - A Lync call to a PSTN line
   - A PSTN call to Lync, and then Lync forwards the call to a PSTN line. One of

the PSTN lines will be counted.

3. **A license will not be counted for a logged-on Lync phone**
   When a user uses a Lync-certified phone, if the phone logs in and stays connected, which retains its logon status, the phone will not be counted as using a license if the query for licenses occurs after the phone logged in.
4. **Licenses counted for PSTN phones joining conferences**
   When a user joins a conference with a PSTN phone, a license will inaccurately be counted for joining the conference. However, no license is needed to join a conference with a PSTN phone.

Workaround:

1. **Inaccurate license count for mobile users**
   - You can manually identify the IP addresses that belong to the same device and then remove one of them in the license count.
   - There is no workaround for this issue with mobile devices connecting with Lync client.
2. **Licenses are counted twice for PSTN calls to Lync client, Lync client calls to PSTN lines, and Lync calls forwarded to PSTN lines**
   You will need to manually identify the PSTN phone number and remove the license count generated for it.
3. **A license will not be counted for a logged-in Lync phone**
   You can configure the Lync phone to log off, and then log on again, at a regular interval, such as every 3 months.
4. **Licenses counted for PSTN phones joining conferences**
   You can manually identify the PSTN phone number that is used to join the conference and remove the license generated by the phone number.

The Lync Server Control Panel stops working in a VMware environment after upgrading to Silverlight 5 (3010077)

Issue:

If you use the Lync Server Control Panel in a VMware environment, the Lync Server Control Panel may stop working after you upgrade Microsoft Silverlight to version 5.

Workaround:

To work around this issue, do one of the following:

- Uninstall Silverlight 5, and install Silverlight 4 from http://go.microsoft.com/fwlink/p/?LinkID=149156&v=4.0.
- Access the Lync Server Control Panel from a computer that is not a VMware virtual computer.
  To do so, you can start the Lync Server Control Panel from the Windows **Start** menu on the server, if the Lync Server Administration tools are installed on the computer.
  You can also access the Lync Server Control Panel by using a web browser. The URL will be similar to https://<frontend_pool_fqdn>/cscp.

User information in the Address Book Service is not updated after the distinguished name for the user is modified in Active Directory (3211549)

Issue:

If a user’s distinguished name (also known as DN) is changed in Active Directory Domain Services (AD DS), any additional changes will not be updated in the Address Book Service (ABS). This does not affect sign-in or presence for the user, but it will prevent communication for the user if the SIP address is also changed, because searches will return an outdated SIP address.

Workaround:

To work around this issue, do not change a user’s DN. If you revert the DN for the user to the previous value, updates will be reflected in the Address Book Service.

Installation

The hotfix for "Heap corruption occurs when a module calls the InsertEntityBody method in IIS 7.5" must be installed prior to installing Lync Server 2013.

Issue:

The hotfix for "Heap corruption occurs when a module calls the InsertEntityBody method in IIS 7.5" (http://go.microsoft.com/fwlink/p/?LinkId=268602), described in Microsoft Knowledge Base article 264886 (http://go.microsoft.com/fwlink/p/?LinkId=268603), must be installed prior to installing Lync Server 2013.

Workaround:

Download and install the hotfix from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?LinkId=268602.

Lync Server 2013 fails to install on ITA Windows Server 2012 OS RTM version (3179467)

Issue:

Lync Server 2013 installation fails on ITA Windows Server 2012 due to Windows Fabric installation failing.

Windows Fabric installation fails because fabric traces are created with the time format of HH:MM:SS. However, in ITA Windows Server, the time format is HH.MM.SS.

Workaround:

To work around this issue, update the system registry before installing Lync Server 2013. The registry key that needs to be updated is: HKEY_USERS\.DEFAULT\Control Panel \International\sTimeFormat. Change the value of sTimeFormat to HH:mm:ss by using the Windows PowerShell command-line interface as follows:

1. Start Windows PowerShell and run the following cmdlets:

   ```
   New-PSDrive -Name HKU -PSProvider Registry -Root HKEY_USERS
   ```

   ```
   $a="HKU:\.Default\Control Panel\International"
   ```

2. To view the current value, run the following cmdlet:

   ```
   Get-itemproperty $a -Name sTimeFormat
   ```

   Make note of the current value for sTimeFormat so it can be restored after the installation is complete.

3. To set to new value, run the following cmdlet:

   ```
   Set-ItemProperty $a -Name sTimeFormat -Value "HH:mm:ss"
   ```

4. After Lync Server 2013 has been successfully installed, restore the original value for the sTimeFormat by running the following cmdlet:

   ```
   - Set-ItemProperty $a -Name sTimeFormat -Value "<Value noted down in S
   ```

Mobility

Issues for mobile clients during the server failover process (3345992)

Issue:

When a Lync Server fails and the failover process begins, the following issues may affect mobile client users:

- No incoming Lync call or signal for up to 10 minutes after failover begins.
- Cannot accept incoming Chat requests
- Cannot join meetings if the failed server is the home server for the user

Workaround:

There is no workaround for this issue. Normal functionality will be restored once the failover process is complete.

If a mobile user declines an incoming call from another Lync endpoint, the call is displayed as a missed conversion on Lync Mobile clients (3346251)

Issue:

If a mobile user declines an incoming call, and the call originated from another Lync endpoint, the call is displayed as a missed conversation in the Lync Mobile client instead of a call in the device call list.

Workaround:

There is no workaround for this issue.

The mobile client may not display a federated contact’s display name when searching for contacts (3346256)

Issue:

The display name for federated contacts may not be displayed in some scenarios, such as when searching for a federated contact in the contact list. This can occur when the there is no active presence subscription for the contact from the Lync mobile client.

Workaround:

There is no workaround for this issue.

In the mobile client, invitee and timestamp information are missing from a missed conversation that is an invitation to a conference (3346265)

Issue:

In the mobile client, when a missed conversation is an invitation to a conference, the invitee and timestamp information is missing from the missed conversation message.

Workaround:

There is no workaround for this issue.

Mobile client users making calls using VoIP are not be able to leave voice mail for users whose voice mail is configured in Exchange 2010 or earlier versions (3346260)

Issue:

If a mobile client user is using VoIP to place calls, the user will not be able to leave voice mail messages for users configured to use voice mail in Microsoft Exchange Server 2007 or Microsoft Exchange Server 2010.

Workaround:

To work around this issue, use Exchange 2010 with SP1 or later version of Microsoft Exchange Server.

When using Block with URL for Client Version Configuration on mobile clients, an incorrect error message may be displayed (3346258)

Issue:

When using **Block with URL** for Client Version Configuration on mobile clients, an incorrect error message may be displayed when the client version is not supported.

Workaround:

To work around this issue, configure Client Version Configuration to use **Block** instead of **Block with URL**.

Conferencing

Antivirus software running on Lync Server 2013 Front End Servers can cause Application Domain recycling, which temporarily interrupts service for Lync Web App 2013, Lync Mobile 2010, and Lync Mobile 2013 clients (3212531)

Issue:

Antivirus software can trigger application domain restarts, which can result in Lync Mobility Service 2013 and unified communications (UC) Web API client applications (Lync Web App 2013, Lync Mobile 2010, and Lync Mobile 2013) to lose their state.

Workaround:

To work around this issue, exclude the folders containing Web components and .NET framework from antivirus scanning. For details, see Microsoft Knowledge Base article 312592, "PRB: Random application restarts with 'Application is restarting' error in ASP.NET," at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=312592.

The following folders should be excluded:

- %ProgramFiles%\Microsoft Lync Server 2013\Web Components\Mcx\Ext
- %ProgramFiles%\Microsoft Lync Server 2013\Web Components\Mcx\Int
- %ProgramFiles%\Microsoft Lync Server 2013\Web Components\Ucwa\Int
- %ProgramFiles%\Microsoft Lync Server 2013\Web Components\Ucwa\Ext
- %Windows%\Microsoft.NET\Framework64\v4.0.30319\Config

ActiveX Controls or native XMLHTTP support must be enabled in Windows Internet Explorer to successfully join conferences (2798163)

Issue:

If a user has disabled both ActiveX Controls and native XMLHTTP support in Windows Internet Explorer Internet browser settings, the user will not be able to join a meeting if

Internet Explorer is selected as the default browser.

Workaround:

Enable either ActiveX Controls or "native XMLHTTP support" in Internet Explorer.

Lync Server Web Conferencing service cannot recover from critical mode (2788663)

Issue:

If critical mode is turned for archiving, in case of system failures, critical mode will start and the conferences will no longer work for the participants. After the administrator fixes the system failures (such as fixing a database issue), the data conferencing service doesn't automatically recover, and the administrator must manually restart the conferencing service for conferencing to resume.

Workaround:

An administrator needs to manually restart the conferencing service after the system failure is fixed.

Web Conferencing service ignores the HTTP proxy for external Office Web App Servers (2602182)

Issue:

If you have deployed an Office Web Apps Server external to the Web Conferencing service (that is, a server that is not in the internal corporate network) in the Internet, perimeter network, and the Web Conferencing service requires an HTTP proxy to connect to this, the Office Web Apps Server discovery will fail. The Web Conferencing service ignores the HTTP proxy setting, as defined in Topology Builder for Office Web Apps Server setup. As a result, the Lync client will not be able to do Microsoft PowerPoint 2010 sharing with other participants in the conference. If you are installing Lync Server on-premises and also configure Office Web Apps Server on-premises in the internal network, a proxy configuration is not required.

Workaround:

The only workaround is to not have a deployment configuration that requires the use of HTTP proxy to communicate with an external Office Web Apps Server.

Adding video to an audio conferencing provider conference is not supported (2603861)

Issue:

Adding a video is not supported if the user is joined to an audio conferencing provider conference for audio.

Workaround:

There is no workaround for this issue.

Topologies with IPv6 enabled force the Lync Web App Silverlight plug-in auto-update to ensure screen sharing functionality can work from Lync Web App (2604634)

Issue:

When a topology is configured with IPv6 enabled, users cannot share their screen from the Lync Web App client if an earlier version of the screen-sharing plug-in is already installed.

Workaround:

To force an update to the most recent version of the screen-sharing plug-in when joining meeting via Lync Web App, modify the value of **MinSupportedBuildVersion** from "4.0.7457.0" to "4.0.7577.380" in both of the following files:

- %ProgramFiles%\Microsoft Lync Server 15\Web Components\Reach\Int\Client \Plugins\ReachAppShPluginProperties.xml
- %ProgramFiles%\Microsoft Lync Server 15\Web Components\Reach\Ext\Client \Plugins\ReachAppShPluginProperties.xml

Enterprise Voice

In some cases, a Lync client running on a computer configured to use IPv4 and IPv6 dual stack might not support capabilities that rely in the IP subnet of the computer such as E911, Media Bypass, Call Admission Control and Location Based Routing (3335508)

Note:

The information in this section pertains to Cumulative Updates for Lync Server 2013: February 2013.

Issue:

When a Lync client is running on a computer that is enabled for IPv4 and IPv6 dual stack and based on the DNS resolution of the proxy server, the client may use the IPv6 address of the computer to sign in. After doing so, the Lync Client will support only the capabilities supported for IPv6, which excludes E911, Media Bypass, Call Admission Control and Location Based Routing.

Workaround:

To work around this issue, disable IPv6 support on the client computer.

If Enterprise Voice is not configured for a user, the user will need to use E164 format to dial out from a conference (3215342)

Issue:

If Enterprise Voice is not configured for a user, that user will need to use the E164 format to successfully dial out from a conference. If the E164 format is not used, the user will not be able to dial out from the conference.

Workaround:

To work around this issue, users who are not enabled for Enterprise Voice should dial out from a conference by using numbers in the E164 format.

Presence

If a user has selected "Block all invites and communications" while the unified contact store is turned on for the user,

Presence status is not rejected when it should be (3204526)

Issue:

If a user has selected "Block all invites and communications" while the unified contact store is turned on for the user, Presence status is not rejected when it should be.

Workaround:

To work around this issue, you can turn off the unified contact store for the user. To do so, run the following cmdlets:

```
Set-CsUserServicesPolicy -Identity "<user display name>" -UcsAllowed $False
```

For example:

```
Set-CsUserServicesPolicy -Identity "Ken Myer" -UcsAllowed $False
```

Office Communications Server 2007 R2 users homed on-premises are not able to see the Presence status of Lync Online users in hybrid deployments (3014624) - Hybrid

Issue:

The issue may occur in a hybrid deployment when you are using a Lync Server 2013 Director.

Presence status for users homed to Lync Online is displayed as Presence Unknown for on-premises users. Also, users homed to Lync Online are not able to see presence status for Office Communications Server R2 on-premises users.

Workaround:

To partially work around this issue, change the Home Server (msrtcsip-presencehomeserver) of the Lync Online users to point to a Lync Server 2013 on-premises pool instead of the Lync Server 2013 Director. You can modify this setting on the on-premises Front End Server.

This workaround will correctly display the Presence status of users homed to Office Communications Server 2007 R2 to Lync Online users.

Response Group application, Call Park application, and Group Call Pickup

A caller might hear one second of music-on-hold during the establishment of a call with the retrieving party (3334097)

> **Note:**
>
> The information in this section pertains to Cumulative Updates for Lync Server 2013: February 2013.

Issue:

When a call is retrieved via Group Call Pickup, the caller might hear one second of music-on-hold during the establishment of the call with the retriever party.

Workaround:

There is no workaround for this issue.

A Response Group agent can sign in and sign out through a Lync Server 2010 Agent Console to Lync Server 2010 formal Agent Groups only (2773455)

Issue:

A Lync Server 2013 Response Group agent can sign in and sign out through a Lync Server 2010 Agent Console to Lync Server 2010 formal Agent Groups only. In the Lync Server 2010 Agent Console, users can see only the Lync Server 2010 Response Group that they belong to. They cannot see any of the Lync Server 2013 Response Groups that they belong to.

Workaround:

If the Response Group agent is a Lync Server 2013 user, and part of a Lync Server 2013 formal Agent Group, the user must access the Lync Server 2013 Agent Console directly via a web link in a browser to sign in to and sign out from Lync Server 2013 Agent Groups.

A Lync Server 2010 Response Group agent cannot place calls on behalf of a Lync Server 2013 Response Group (2773471)

Issue:

A Lync Server 2010 user who is an Agent of a Lync Server 2013 Response Group is not able to place a call on behalf of the Response Group. The Lync Server 2013 Response Group will not be available in the Lync Client to place a call.

Workaround:

To work around this issue, you must move the Lync Server 2010 user to Lync Server 2013.

Removing a Response Group from Lync Server 2010 after it has been migrated to Lync Server 2013 will prevent the Response Group from accepting any incoming calls (3016227)

Issue:

If a Response Group that has been migrated from Lync Server 2010 to Lync Server 2013 is removed from Lync Server 2010 through the Lync Server Control Panel or the Lync Server Management Shell, the Response Group in Lync Server 2013 will stop receiving any incoming calls.

Workaround:

To work around this issue, do not remove any Response Groups from Lync Server 2010 that have been migrated from Lync Server 2010 to Lync Server 2013.

If the Response Group has already been removed, you should redeploy it in Lync Server 2013.

When a new managed workflow is set to inactive when created, deployment of the workflow will fail (3207527)

Issue:

When a new managed workflow is set to inactive when created, deployment of the workflow will fail. This issue is encountered when the workflow is set to inactive when created, but does not affect a workflow that is edited to set it to inactive after is has been deployed.

Workaround:

When creating and deploying a workflow, set the workflow as active and then deploy it. After the workflow is successfully deployed, the workflow can be edited and set to inactive.

Removing a Response Group from the Owner pool will prevent the Response Group of the Backup pool from accepting any incoming calls during failover if the Response Group has been imported to the Backup pool (3016214)

Issue:

If a Response Group that is owned by the primary pool has been imported to the backup pool without overwriting the owner, and the Response Group is removed from the owner pool, the Response Group in the Backup pool will not accept any incoming calls during failover.

Workaround:

You will need to redeploy the Response Group in the Primary pool. You will then need to export the Response Group configuration from the Primary pool and import it to the Backup pool again.

You can also recreate the Response Group in the Backup pool. In this case, the Backup pool will be the owner pool of the Response Group.

A parked call can't be retrieved from the Call Park application if the retrieve request is done on behalf of a Response Group (3211798)

Issue:

When the following conditions are true, a retrieve request for a parked call will fail:

- An agent is part of an anonymous Response Group
- The agent attempts to retrieve a parked call from the Call Park application through the anonymous Response Group
- The agent attempts to retrieve the call by dialing the orbit number through the Call On Behalf option or through the same option in the Lync attendant client

Workaround:

There are no workarounds for this issue. The parked call should be retrieved without doing so on behalf of a Response Group.

Lync Server Control Panel, Topology Builder, and Planning Tool

Planning Tool Limitations (3331056 and 3331059)

Note:

The information in this section pertains to Cumulative Updates for Lync Server 2013: February 2013.

Issue:

The Planning Tool has the following limitations when planning for your deployment:

- There is a maximum of 10 central sites supported
- Each central site can have a maximum of 14 branch sites
- Each central site can have a maximum of 240,000 users

In addition, the Planning Tool does not include values for the following when calculating the recommended topology:

- The number of users that are homed online
- The percentage of users that are enabled for XMPP federation
- Percentage of users that are using Lync Web App
- The percentage of users that are configured for Hybrid Voice

Workaround:

There is no workaround for these issues. For more information about the Planning Tool, see Designing the Topology by Using the Planning Tool.

Planning Tool may not use previously defined IP addresses for the Edge network when updating options

Issue:

After you complete your design using the Planning Tool, if you make changes to the Edge Network options, additional IP addresses may be added to the design instead of updating the existing IP addresses. This can occur when you are viewing the details of the Edge Network Diagram, select **Click here to update your options**, and then, on the Configuration Options dialog, you select Edge Network select **I want to use the same FQDNs and IP addresses, but different ports for the edge services on my Edge Server**. Applying any changes may result in new IP addresses and Edge servers being added to the design.

Workaround:

There is no workaround for this issue at this time.

In Lync Server Control Panel, "Move all users to pool" may not work as expected (3199270)

Issue:

When using the Lync Server Control Panel to move all users from one pool to another pool in a complex Active Directory environment, such as one with multiple Domain Controllers and parent/child domains, an error message may be returned that states, “Specified user is not a legacy user, use Move-CsUser cmdlet instead.” This is a result of longer replication times in complex Active Directory environments.

Workaround:

To work around this issue, do one of the following:

- Use filters in the Lync Server Control Panel to search for legacy users, select those users, and then use the **Move selected users to pool command** instead of **Move all users to pool**.
- Use the Lync Server Management Shell to move legacy users in batches by using Lync Server cmdlets.

The Lync Server Control Panel stops working in a VMware environment after the Microsoft Silverlight browser plug-in is

updated to version 5 (3199270)

Issue:

If you use the Lync Server Control Panel in a VMware environment, the Lync Server Control Panel may stop working after you upgrade Silverlight to version 5.

Workaround:

To work around this issue, do one of the following:

- Uninstall Silverlight 5, and then install Silverlight 4 from http://go.microsoft.com/fwlink/p/?LinkID=149156&v=4.0.
- Open the Lync Server Control Panel from a computer that is not a VMware virtual computer.
  To open the Lync Server Control Panel from a remote computer, install Lync Server Administration tools on the computer, and then start the Lync Server Control Panel from the Windows **Start** menu.
  You can also open the Lync Server Control Panel by entering the URL in a web browser. The URL will be similar to https://<frontend_pool_fqdn>/cscp.

An administrator cannot run the Uninstall-csMirrorDB cmdlet after removing the mirroring database in Topology Builder (3199266)

Issue:

When an administrator disables a mirroring database in Topology Builder, and then deletes the mirroring database in Topology Builder, a message is displayed in the To do list for the administrator to run the **Uninstall-csMirrorDatabase** cmdlet to remove mirroring from SQL Server. When the administrator attempts to run the cmdlet, it fails.

Workaround:

To remove SQL mirroring of a pool in Topology Builder, you must first use a cmdlet to remove the mirror in SQL Server. You can then use Topology Builder to remove the mirror from the topology. To remove the mirror in SQL Server, use the following cmdlet:

```
Uninstall-CsMirrorDatabase -SqlServerFqdn <SQLServer FQDN> [-SqlInstanceName <SQL
```

For example, to remove mirroring and drop the databases for the user databases, type the following:

```
Uninstall-CsMirrorDatabase -SqlServerFqdn primaryBE.contoso.com -SqlInstanceName
```

The *DropExistingDatabasesOnMirror* parameter causes the affected databases to be deleted from the mirror. Then, to remove the mirror from the topology, do the following:

1. In Topology Builder, right-click the pool and click **Edit Properties**.
2. Clear **Enable SQL Store Mirroring** and click **OK**.
3. Publish the topology.

◆**Important:**
Whenever you make a change to a back-end database mirroring relationship, you must restart all the Front End Servers in the pool.

Validation errors are returned in Topology Builder when an administrator attempts to remove a deployment with a Front End pool that has an associated witness store (3199266)

Issue:

If an administrator attempts to use the **Remove Deployment** command in Topology Builder to remove a deployment that includes a Front End pool with an associated witness store, a validation error is displayed in Topology Builder and the action will not proceed.

Workaround:

To work around this issue, do one of the following:

- Remove the witness store before attempting to remove the deployment.
- Add a witness store for the Front End pool and then remove it.

Persistent Chat Server deployment information is inconsistent between the Planning Tool and Topology Builder (3012228)

Issue:

When the Lync Server 2013, Planning Tool outputs the site topology diagram for a Persistent Chat Server deployment with disaster recovery enabled, the site topology diagram includes multiple (physical) sites, with evenly assigned Persistent Chat Servers at each site. In Topology Builder, all Persistent Chat Servers are represented as belonging to a single (logical) site, and are listed under the same Persistent Chat Server pool node.

Workaround:

Currently, we do not have a workaround for this issue. The user should analyze the output of the Planning Tool for the Persistent Chat Server deployment, and modify the plan to meet their specific needs.

Localization

Monitoring

The Deploy Monitoring Reports wizard displays incorrect characters under certain circumstances when using the East Asian version of Lync Server (3113565)

Issue:

When using an East Asian version of Lync Server 2013—for example, Chinese (Simplified), Chinese (Traditional), Japanese, or Korean—on an operating system that has the system locale not set to an East Asian language, the Deploy Monitoring Reports wizard will display question marks or other characters instead of localized messages.

Workaround:

To correct this issue, set the locale for the operating system and Lync Server 2013 to the same language, which will display all messages correctly.

Lync Server Control Panel

In certain cases, the first item in the top navigation bar on a page of Lync Server Control Panel disappears when the last item in the top navigation bar is clicked (3158118)

Issue:

There are three known cases where clicking the last item in the top navigation bar on a page of the Lync Server Control Panel will cause the first item in the top navigation bar to disappear:

- In the French of version, on the page "Féderation et accès externe," the item "Stratégie d'accès externe" will disappear when "Partenaires fédérés XMPP" is clicked.

- In the German version, on the "Clients" page, the item "Clientversionskonfiguration" disappears when "Pushbenachrichtigungskonfiguration" is clicked.
- In the Russian version, on "Конфигурация сети" page, the item "Глобально" disappears when "Маршрут региона" is clicked.

Workaround:

To work around this issue, refresh the page of the Lync Server Control Panel in your browser. The page will load in the browser with all of the items in the top navigation bar displayed.

Address Book

Indexing in the Address Book does not work as expected in some languages (3336047)

> **Note:**
> The information in this section pertains to Cumulative Updates for Lync Server 2013: February 2013.

If a user’s properties contain an indexed field, and that field contains only characters that cannot be indexed, then the user will not appear in searches performed in the Address Book.

The following characters and locales cannot be indexed:

- Upper-case Cyrillic, Greek, and Armenian characters
- Upper-case accented characters
- Thai
- Lao
- Myanmar
- Devanagari
- Ethiopic
- Tibetan
- Bengali
- Gujarati
- Telugu
- All other Indic scripts

Lync Web App, Web Scheduler, and Web components

Language fallback for certain languages in Lync Web Scheduler, Dial-In, Join Launcher, Persistent Chat Room Management, and OCTab might not work as expected (3079700)

Issue:

When selecting a neutral locale in a web browser (in Internet Explorer, for example, the language name without further specification, like "Norwegian [no]") instead of a locale specifying language, script and locale (such as "Norwegian, Bokmål (Norway) [nb-NO]") might lead to unexpected display behavior for certain languages in Lync Web Scheduler, Dial-In, Join Launcher, Persistent Chat Room Management, and OCTab. For example, users might see the English page when one of the following languages is selected:

- Norwegian
- Portuguese
- Serbian

Workaround:

If you want to select a language with a neutral locale, always make sure that you also add the language with a specific locale (with script and/or country code) as an additional language in your browser's language preference list.

There is limited support for Azeri and Uzbek locales when using Lync Web Scheduler, Dial-In, Join Launcher, Persistent Chat Room Management, and OCTab in some web browsers (3336748)

Note:
The information in this section pertains to Cumulative Updates for Lync Server 2013: February 2013.

Issue:

When you use Internet Explorer 8 or Internet Explorer 9, and set the browser language to Azeri (Latin) or Uzbek (Latin), the Dial-in and Join Launcher pages will be displayed in English or the preferred language set in the browser.

When you use Firefox or Chrome browsers, and you set the browser language to Azeri (Latin) or Uzbek (Latin), the Lync Web App, Lync Web Scheduler, and RGS OCTab will be shown in English or the preferred language set for the browser.

The Uzbek (Latin) locale is not supported in the Safari browser.

Workaround:

There is not workaround for these issues.

The drop-down arrow is missing for "Join meeting from" list in the Romanian version of Lync Web App (3154899)

Issue:

When a user who is using the Romanian version of Lync Web App performs the following steps, the drop-down arrow is not displayed for **Join meeting** in drop-down list:

1. Select **Remember me on this computer** on the **General** tab.
2. Select the **Phone** tab.
3. Click the drop-down list for **Join meeting from**.
   Users will not see an arrow that indicates that there are more options than the default **Lync Web App**, which include: **Don't join audio** (in Romanian, "Nu se asociaža la componenta audio") and **New number**" (in Romanian, "Numar nou").

Workaround:

Even though the arrow for this drop-down list is not displayed, users can still select the additional settings in the list by clicking on the default value.

When using the Turkish version of Lync Web Scheduler, a meeting cannot be saved when using the "People I choose" option under "Who is a presenter" (3169483)

Issue:

When creating or editing a meeting in the Turkish version of the Lync Web Scheduler, the option "People I choose" under "Who is a presenter" is not supported. When this option is selected, the meeting can't be saved. Instead, an error message appears, indicating that one or more people cannot be made presenters.

Workaround:

To work around this issue, users can use the default option of "People from my company," or any other choice, such as "Only Organizer" or "Everyone including people outside of my company." The organizer can demote or promote people to their correct roles later, after they have joined the meeting.

Alternatively, users who understand another language can change the language selection in their browser to one of the other 43 supported languages and attempt to use the “People I choose” option.

Copyright

1.2 Supportability

Supportability

Microsoft Lync Server 2013 >

Topic Last Modified: *2012-04-23*

Microsoft Lync Server 2013 communications software supports topologies that are designed to meet the needs of organizations that are small, medium, or large and that have varying requirements for performance, high availability, and scalability.

- Active Directory Support
- Supported Lync Server 2013 Topologies
- Supported Server Collocation
- Supported Migration Paths and Coexistence Scenarios
- Supported Hardware
- Server Software and Infrastructure Support
- Additional Server Support and Requirements
- Client and Device Software and Infrastructure Support

1.2.1 Active Directory Support

Active Directory Support

Microsoft Lync Server 2013 > Supportability >

Topic Last Modified: *2012-12-04*

The Active Directory Domain Services (AD DS) on-premises topologies that are supported by Lync Server 2013 are as follows:

- Single forest with single domain
- Single forest with a single tree and multiple domains
- Single forest with multiple trees and disjoint namespaces
- Multiple forests in a central forest topology
- Multiple forests in a resource forest topology

Note:

Lync Server 2013 does not support single-label domains. For example, a forest with a root domain named **contoso.local** is supported, but a single-label root domain named **local** is not supported. For details, see Microsoft Knowledge Base article 300684, "Information about configuring Windows for domains with single-label DNS names," at http://go.microsoft.com/fwlink/p/?linkId=143752.

Note:

Lync Server 2013 does not support renaming domains. If you need to rename a domain where Lync Server is deployed, you need to first uninstall Lync Server, then rename the domain, and then reinstall Lync Server.

For details about supported topologies and requirements for on-premises deployments, see Active Directory Domain Services Requirements, Support, and Topologies in the Planning documentation.

1.2.2 Supported Lync Server 2013 Topologies

Supported Lync Server 2013 Topologies

Microsoft Lync Server 2013 > Supportability >

Topic Last Modified: *2012-11-08*

Lync Server 2013 supports deployment of sites on premises in an organization and integration of on-premises deployments with Lync Online deployments, which is known as a hybrid deployment. In a hybrid deployment, some users are homed on-premises and some users are homed online.

For on-premises deployments, Lync Server 2013 supports deployment of one or more sites that can be scaled to meet high availability and location requirements. You can structure these sites and their components to meet the access and resiliency requirements of your organization.

A Lync Server 2013 on-premises deployment consists of the following:

- Your deployment must include at least one central site (also known as a data center). Each central site must contain at least one Enterprise Edition Front End pool or one Standard Edition server. These consist of the following:
    - Enterprise Edition Front End pool, which consists of one or more Front End Servers (typically, at least two Front End Servers for scalability) and a separate Back End Server. A Front End pool can contain a maximum of twelve Front End Servers. Load balancing is required for multiple Front End Servers. For SIP traffic, we recommend DNS load balancing, but hardware load balancing is also supported. If you use DNS load balancing for SIP traffic, you still need a hardware load balancer for HTTP traffic. We recommend SQL Server mirroring for high availability of databases. The back-end database requires a separate instance, but you can collocate the archiving database, monitoring database, persistent chat database, and persistent chat compliance database with it. Lync Server 2013 supports the use of a shared cluster for the file shares in your deployment. For details about database storage requirements, see Database Software Support. For details about file storage requirements, see File Storage Support.

        > **Important:**
        > If you collocate Lync Server databases, we highly recommend assessing all factors that might affect availability and performance. To verify failover capabilities, we recommend testing all failover scenarios.

    - Standard Edition server, which includes a collocated SQL Server Express database.
- Your deployment can also have one or more branch sites associated with a central site.

This section describes the sites and components of a Lync Server 2013 deployment. For details about Lync Server 2013 site, topology, and component planning, see Topology Basics You Must Know Before Planning and Reference Topologies in the Planning documentation. For details about integration of components of previous releases, see Supported Migration Paths and Coexistence Scenarios.

Central Site Topologies and Components (On-Premises)

Although a central site topology must include one Front End pool or one Standard Edition server, each central site can also contain the following:

- Multiple Front End pools, which can be in the same domain or different domains. However, all Front End Servers in a Front End pool, and the Back End Server for that pool, must be in the same domain.
- Multiple Standard Edition servers.
- Office Web Apps Server, which is used with Office Web Applications in Lync Server 2013 to handle the sharing and rendering of Microsoft PowerPoint 2010 presentations.
- Edge Server or Edge pool in your perimeter network, if you want your deployment to support federated partners, public IM connectivity, an extensible messaging and presence protocol (XMPP) gateway, remote user access, participation of anonymous users in meetings, or Exchange Unified Messaging (UM). You cannot collocate any other server role with an Edge Server. We recommend DNS load balancing, where appropriate, but hardware load balancing is also supported. The internal Edge interface and external

Edge interface must use the same type of load balancing. You cannot use DNS load balancing on one Edge interface and hardware load balancing on the other Edge interface. For details about load balancing requirements and support, see Planning for External User Access in the Planning documentation and Deploying External User Access in the Deployment documentation.

- Mediation Server or pool, if you want to support Enterprise Voice or dial-in conferencing in a Front End pool at the central site. Depending on how you deploy Enterprise Voice support, you can collocate the Mediation Server in a Front End pool (the default) or deploy a stand-alone Mediation Server or pool. You can use DNS, hardware, or application load balancing (when appropriate) to distribute traffic from a Mediation Server pool's gateway peer, including a PSTN gateway, IP-PBX, or SIP trunk Session Border Control (SBC).For details about planning the appropriate Mediation Server topology, see Deployment Guidelines for Mediation Server in the Planning documentation.
- Persistent Chat Server, if you want to users to be able to participate in multiparty, topic-based conversations that persist over time. To provide more capacity and increased reliability, your topology can include multiple computers running Persistent Chat Server. You cannot collocate Persistent Chat Server with other server roles in an Enterprise pool. However, you can collocate Persistent Chat Server on a Standard Edition server. Persistent chat requires a database and, if you implement persistent chat compliance, a persistent chat compliance database, but the databases can be collocated with the Archiving database, Monitoring database, or on the Back End Server of an Enterprise Edition Front End pool. For details about planning the appropriate Persistent Chat Server topology, see Planning for Persistent Chat Server in the Planning documentation.
- Monitoring, if you want to support data collection for audio/video Quality of Experience (QoE) and call detail recording (CDR) for Enterprise Voice and A/V conferences in your deployment. Optionally, you can install the Microsoft System Center Operations Manager (formerly Microsoft Operations Manager), which uses Monitoring CDR and QoE data to generate near real-time alerts that show the health of call reliability and media quality. Monitoring, when deployed, is collocated on Front End Servers or a Standard Edition server. Monitoring requires a database, but the database can be collocated with the Archiving database, persistent chat database, persistent chat compliance database, or on the Back End Server of an Enterprise Edition Front End pool.
- Archiving, if you want to archive IM communications and meeting content (for compliance reasons) in your deployment. Archiving, when deployed, is collocated on Front End Servers or a Standard Edition server. Archiving storage requires either deployment of an Archiving database or integration with Exchange 2013 storage. If you use both, which is known as *mixed mode*, Exchange 2013 storage is used to store archive data for users who are homed on Exchange 2013, and the Archiving database is used to archive data for all other users in your deployment. If you require an Archiving database, the database can be collocated on the Monitoring database, persistent chat database, persistent chat compliance database, or on the Back End Server of a Front End pool. For details about planning the appropriate Archiving topology, see Planning for Archiving in the Planning documentation.
- Director or Director pool, if you want to facilitate resiliency and redirection of Lync Server 2013 user requests to the user's home pool, which can be either an Enterprise Edition Front End pool or a Standard Edition server. We recommend that you deploy a Director or Director pool in each central site that supports external user access and in each central site in which you deploy one or more Front End pools. Each Director pool can contain a maximum of ten Directors. A Director cannot be collocated with any other server role. For details about planning the appropriate Director topology, see Scenarios for the Director in the Planning documentation.
- Reverse proxy, which is not a Lync Server 2013 component, but is required if you want to support sharing of web content for federated users or to support Mobility traffic. You cannot collocate a reverse proxy server with any Lync

Server 2013 server role, but you can implement reverse proxy support for a Lync Server 2013 deployment by configuring the support on an existing reverse proxy server in your organization that is used for other applications. For details about reverse proxy servers, see Setting Up Reverse Proxy Servers in the Deployment documentation.

Note:
In Lync Server 2013, A/V Conferencing, Monitoring, and Archiving run on Front End Servers and are no longer separate server roles.

All Front End pools and Standard Edition servers that you deploy at a central site share any of the following that you deploy for the central site:

- Director or Director pool
- Stand-alone Mediation Server or pool
- Office Web Apps Server
- Edge Server or Edge pool
- Persistent Chat Server or pool
- Monitoring
- Archiving

Note:
An Exchange UM Server can be implemented with your Lync Server 2013 deployment if you want to support integration of Exchange 2013 Unified Messaging, but it is not a component of the Lync Server 2013 site.

Multiple central sites can also share any of the following that you deploy in one central site:

- Stand-alone Mediation Server or pool
- Edge Server or Edge pool
- Persistent Chat Server or pool
- Archiving
- Monitoring

Note:
An Exchange UM Server can be implemented with your Lync Server 2013 deployment and shared by multiple central sites, but it is not a component of the Lync Server 2013 site.

For details about Lync Server 2013 server roles and functionality, see Server Roles in the Planning documentation.

For a summary of Lync Server 2013 server collocation support, see Supported Server Collocation.

In addition to the server roles and functionality covered previously in this section, Lync Server 2013 has additional components and options, which can include some or all of the following:

- Firewalls
- PSTN gateways (if deploying Enterprise Voice)
- Exchange UM Server
- DNS load balancing
- Hardware load balancers
- SQL Server databases
- File shares

For details about all of the Lync Server 2013 features, components, and options, see the Planning documentation.

Branch Site Topologies and Components (On-Premises)

A branch site is associated with a central site, and each Survivable Branch Appliance in a branch site is associated with an Enterprise Edition Front End pool or a Standard Edition server in the associated central site. Branch sites depend on the central site for most of their functionality, so components at a branch site contain only the following:

- A Survivable Branch Appliance, which combines a public switched telephone network (PSTN) gateway with some Lync Server functionality. A Mediation Server can be collocated with the instance of the Registrar on the Survivable Branch Appliance, and you can deploy a stand-alone Mediation Server or pool of Mediation Servers.
- A Survivable Branch Server, which is a server running Windows Server that has Lync Server 2013 Registrar and Mediation Server software installed.
- A stand-alone PSTN gateway (not part of the Survivable Branch Appliance) and a stand-alone Mediation Server.

The requirements for Survivable Branch Servers are the same as the requirements for any Lync Server 2013 server role.

1.2.3 Supported Server Collocation

Supported Server Collocation

Microsoft Lync Server 2013 > Supportability >

Topic Last Modified: *2012-06-29*

Lync Server 2013 supports collocation of some server roles and features. Which server roles and features you can collocate depends, in part, on whether you are deploying a Front End pool or a Standard Edition server.

- Server Collocation in an Enterprise Edition Front End Pool Deployment
- Server Collocation in a Standard Edition Server Deployment

1.2.3.1 Server Collocation in an Enterprise Edition Front End Pool Deployment

Server Collocation in an Enterprise Edition Front End Pool Deployment

Microsoft Lync Server 2013 > Supportability > Supported Server Collocation >

Topic Last Modified: *2012-10-29*

This section describes the server roles, databases, and file shares that you can collocate in a Lync Server 2013 Front End pool deployment.

Server Roles

In Lync Server 2013, A/V Conferencing service, Mediation service, Monitoring, and Archiving are collocated on the Front End Server, but additional configuration is required to enable them. If you do not want to collocate the Mediation Server with the Front End Server, you can deploy it as a stand-alone Mediation Server on a separate computer.

You can collocate a trusted application server with the Front End Server.

The following server roles must each be deployed on a separate computer:

- Director
- Edge Server
- Mediation Server (if not collocated with the Front End Server)
- Office Web Apps Server

Databases

You can collocate each of the following databases on the same database server:

- Back-end database
- Monitoring database
- Archiving database
- Persistent Chat database
- Persistent Chat compliance database

You can collocate any or any or all of these databases in a single instance of SQL Server or use a separate instance of SQL Server for each, with the following limitations:

- Each instance of SQL Server can contain only a single back-end database, a single Monitoring database, a single Archiving database, a single Persistent Chat database, and a single Persistent Chat compliance database.
- The database server cannot support more than one Front End pool, one Archiving deployment, and one Monitoring deployment, but it can support one of each, regardless of whether the databases use the same instance of SQL Server or separate instances of SQL Server.

You can collocate a file share with the databases, as described later in this section.

Note:

In Lync Server 2013, you have the option of integrating Monitoring and Archiving storage with Exchange 2013 storage for some or all users in your deployment. You cannot deploy any servers running Lync Server or components on the same servers as the Exchange storage.

Important:

Although collocation of databases is supported, the size of the databases can grow quickly. For example, when you consider collocating the Archiving database with other databases, be aware that if you are archiving the messages of more than a few users, the disk space needed by the Archiving database can grow very large. For this reason, we do not recommend collocating multiple databases, especially the Archiving database, the Persistent Chat database, or the Persistent Chat compliance database with the back-end database.

File Share

The file share can be a separate server or can be collocated on the same server as any or all of the following:

- Database server, including the Back End Server of an Enterprise Edition Front End pool
- Archiving database
- Monitoring database
- Persistent Chat database
- Persistent Chat compliance database

A single file share can be used for multiple Front End pools, Standard Edition servers (all in the same site).

Note:

In Lync Server 2013, Monitoring and Archiving use the Lync Server file share as the Front End Server.

Other Components

You cannot collocate a reverse proxy server, which is not a Lync Server 2013 component, but is required in your deployment if you want to support sharing of web content for federated users with any Lync Server 2013 server role. You can, however, implement reverse proxy support for a Lync Server 2013 deployment by configuring the support on an existing reverse proxy server in your organization that is used for other applications.

You cannot collocate any Exchange Unified Messaging (UM) component or SharePoint component with any SharePoint Server role.

1.2.3.2 Server Collocation in a Standard Edition Server Deployment

Server Collocation in a Standard Edition Server Deployment

Microsoft Lync Server 2013 > Supportability > Supported Server Collocation >

Topic Last Modified: *2013-01-20*

This section describes the server roles, databases, and file shares that you can collocate in a Lync Server 2013 Standard Edition server deployment.

Server Roles

In Lync Server 2013, A/V Conferencing service, Mediation service, Monitoring, and Archiving are collocated on the Standard Edition Server, but additional configuration is required to enable them. You can choose to deploy Mediation service on separate servers.

You can collocate a trusted application server with a Standard Edition server.

The following server roles must each be deployed on a separate computer:

- Director
- Edge Server
- Mediation Server (if not collocated with the Standard Edition server)
- Office Web Apps Server

Databases

By default, the SQL Server Express back-end database is collocated on the Standard Edition server. You cannot move it to a separate computer. With one exception, you cannot collocate other databases on the Standard Edition server. If you choose to deploy Persistent Chat Server on a Standard Edition server, you can collocate the Persistent chat database and the Persistent Chat Compliance database on the same Standard Edition server.

You can collocate each of the following databases on a single database server:

- Monitoring database
- Archiving database
- A back-end database for an Enterprise Edition Front End pool

You can collocate any or any or all of these databases in a single SQL instance or use a separate SQL instances for each, with the following limitations:

- Each SQL instance can contain only a single back-end database (for an Enterprise Edition Front End pool), single Monitoring database, single Archiving database, single persistent chat database, and single persistent chat compliance database.
- The database server cannot support more than one Enterprise Edition Front End pool, one server running Archiving, one server running Monitoring, single Persistent Chat database, and single Persistent Chat compliance database, but it can support one of each, regardless of whether the databases use the same instance of SQL Server or separate instances of SQL Server.

You can collocate a file share with the databases, as described later in this section.

Note:

In Lync Server 2013, you have the option of integrating Monitoring and Archiving storage with Exchange 2013 storage for some or all users in your deployment. You cannot deploy any servers running Lync Server or components on the same servers as the Exchange storage.

Important:

Although collocation of databases is supported, the size of the databases can grow quickly. For example, when you consider collocating the Archiving database with other databases, be aware that if you are archiving the messages of more than a few users, the disk space needed by the Archiving database can grow very large. For this reason, we do not recommend collocating multiple databases, especially the Archiving database, Persistent Chat database, and Persistent Chat compliance database with the back-end database of an Enterprise pool.

File Shares

The file share can be a separate server or can be collocated on the same server as any or all of the following:

- Database server, including the Back End Server of an Enterprise Edition Front End pool
- Archiving database
- Monitoring database
- Persistent Chat database
- Persistent Chat compliance database

A single file share can be used for multiple Front End pools, Standard Edition servers (all in the same site).

Note:

In Lync Server 2013, Monitoring and Archiving use the Lync Server file share as the Standard Edition server.

Other Components

You cannot collocate a reverse proxy server, which is not a Lync Server 2013 component, but is required in your deployment if you want to support sharing of web content for federated users with any Lync Server 2013 server role. You can, however, implement reverse proxy support for a Lync Server 2013 deployment by configuring the support on an existing reverse proxy server in your organization that is used for other applications.

You cannot collocate any Exchange UM component or SharePoint component with any Lync Server 2013 role.

1.2.4 Supported Migration Paths and Coexistence Scenarios

Supported Migration Paths and Coexistence Scenarios

Microsoft Lync Server 2013 > Supportability >

Topic Last Modified: *2012-04-30*

Lync Server 2013 supports migration from Microsoft Lync Server 2010 and Microsoft Office Communications Server 2007 R2, including coexistence with specific client and server components of those previous deployments.

- Supported Server Migration Paths and Coexistence Scenarios
- Supported Clients from Previous Deployments

1.2.4.1 Supported Server Migration Paths and Coexistence Scenarios

Supported Server Migration Paths and Coexistence Scenarios

Microsoft Lync Server 2013 > Supportability > Supported Migration Paths and Coexistence Scenarios >

Topic Last Modified: *2012-10-16*

Lync Server 2013 supports migration from either of the following:

- Microsoft Lync Server 2010
- Microsoft Office Communications Server 2007 R2

Migration from an environment running both of these previous versions is not supported. Migration from earlier versions, such as Microsoft Office Communications Server 2007 or Live Communications Server 2005, is not supported. If your previous deployment included Group Chat, you must migrate it separately.

Migration Methods

Migration of all Lync Server topologies and server roles is supported. You can migrate from one topology to a different topology, including from Standard Edition server to Enterprise Edition server.

Lync Server 2013 supports only the following migration method:

- **Side-by-side migration.** In side-by-side migration, Lync Server 2013 is deployed alongside an existing Microsoft Lync Server 2010 or Office Communications Server 2007 R2 deployment, and then you transfer operations to the new servers and move users to Lync Server 2013. This method requires additional server platforms, including hardware and software, during migration, and system names and pool names are different in the new configuration. If it becomes necessary to roll back to the previous version, you can shift operations back to the previous servers.

Migration across Active Directory Domain Services (AD DS) forests is not supported.

The recommended migration path is a phased approach. For details about migrating from a previous release, including the appropriate phasing of component deployment, see the following topics in the Migration documentation:

- Migration from Lync Server 2010 to Lync Server 2013
- Migration from Office Communications Server 2007 R2 to Lync Server 2013

- Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server

Coexistence Scenarios

Lync Server 2013 can coexist with components of either a Lync Server 2010 deployment or an Office Communications Server 2007 R2 deployment. Concurrent deployment of Lync Server 2013 with both Lync Server 2010 and Office Communications Server 2007 R2 (concurrent deployment of all three versions) is not supported.

During a phased migration in which a previous Lync Server 2010 or Office Communications Server 2007 R2 deployment coexists temporarily with the new Lync Server 2013 deployment, support for mixed version routing is limited. For details, see the Migration documentation.

You must use separate and distinct computers running Microsoft SQL Server 2008 R2 or Microsoft SQL Server 2012 for your Lync Server 2013 database instances. You cannot use the same instance of SQL Server for a Lync Server 2013 Front End pool that you use for a Lync Server 2010 or Office Communications Server 2007 R2 Front End pool. If you define and configure Lync Server 2013 in Topology Builder for a deployment that already has Lync Server 2010 or Office Communications Server 2007 R2 deployed, Topology Builder will not allow you to define an instance of a Lync Server 2013 that is already in use in the topology.

Topology Builder will display the following message to inform you of this issue: "The SQL server [FQDN of the server] already contains a SQL instance hosting role 'User Store'."

Note:
If you intend to deploy server roles that are new to your Lync Server 2013 deployment, you should first upgrade your existing deployment as described in the Migration documentation and the Deployment documentation, and then deploy the new server roles as described in the Planning documentation and Deployment documentation. If you are migrating a previous version of Group Chat, migrate it last, after completing the process for migrating all other components from Lync Server 2010 or Office Communications Server 2007 R2.

For specific coexistence requirements and other details about coexistence and migration of Lync Server 2010 or Office Communications Server 2007 R2 and Lync Server 2013 components, see Migration from Lync Server 2010 to Lync Server 2013 and Migration from Office Communications Server 2007 R2 to Lync Server 2013 in the Migration documentation. For details about mixed version support for clients, see Supported Clients from Previous Deployments.

1.2.4.2 Supported Clients from Previous Deployments

Supported Clients from Previous Deployments

Microsoft Lync Server 2013 > Supportability > Supported Migration Paths and Coexistence Scenarios >

Topic Last Modified: *2012-12-14*

In a coexistence scenario, Lync Server 2013 clients can interact with clients from earlier versions of Lync Server and Office Communications Server. Unlike previous releases, Lync Server 2010 supports the new Lync 2013 clients. This allows organizations who are upgrading from Lync Server 2010 to roll out new clients independent of Lync Server upgrades.

Supported Server and Client Combinations

The following table shows the supported combinations of client versions and server versions. Lync Server 2013 supports two previous client versions, and Lync Server 2010 supports the new Lync 2013 client.

Client	Lync Server 2013	Lync Server 2010	Office Communications Server 2007 R2
Lync 2013	Supported	Supported	Not Supported
Lync Web App 2013	Supported	Not Supported	Not Supported
Lync 2010	Supported	Supported	Not Supported
Lync 2010 Attendant	Supported	Supported	Not Supported
Lync 2010 Group Chat	Not Applicable	Supported[1]	Not Applicable
Lync Web App 2010	Not Supported	Supported	Not Supported
Lync 2010 Attendee	Not Supported[2]	Supported	Not Supported
Office Communicator 2007 R2	Interoperable[3]	Supported	Supported
Microsoft Office Communications Server 2007 R2 Attendant	Not Supported	Supported	Supported
Office Communicator 2007	Not Supported	Supported	Supported
Office Live Meeting 2007	Not Supported	Supported	Supported

[1] In Microsoft Lync Server 2010, group chat functionality was available with Group Chat Server, a third-party trusted application for Lync Server 2010. Lync 2013 clients are not compatible with Lync Server 2010, Group Chat.

[2] Lync Web App 2013 now provides a full in-meeting experience, including computer audio and video, and is considered the replacement for Lync 2010 Attendee.

[3] The presence and IM features in Office Communicator 2007 R2 are compatible with Lync Server 2013, but conferencing features are not. During migration from Office Communications Server 2007 R2, Office Communicator 2007 R2 is suitable for presence and IM interoperability, but users should use Lync Web App 2013 to join Lync Server 2013 meetings.

Note:

For details about the ability of Lync Server 2013 clients to coexist and interact with clients from earlier versions of Lync Server and Office Communications Server, see Client Interoperability in Lync 2013 in the Planning documentation.

1.2.5 Supported Hardware

Supported Hardware

Microsoft Lync Server 2013 > Supportability >

Topic Last Modified: *2012-09-21*

Lync Server 2013 hardware requirements vary according to server role, topology, storage requirements, and the specific deployment scenario.

- Server Hardware Platforms
- Client and Device Hardware Support
- File Storage Support

1.2.5.1 Server Hardware Platforms

Server Hardware Platforms

Microsoft Lync Server 2013 > Supportability > Supported Hardware >

Topic Last Modified: *2013-01-07*

Lync Server 2013 server roles and computers running Lync Server administrative tools require 64-bit hardware.

The specific hardware used for Lync Server 2013 deployment can vary, depending on size and usage requirements. This section describes the recommended hardware. Although these are recommendations, not requirements, using hardware that does not meet these recommendations may result in significant performance issues and other issues.

Recommended Hardware Platform

For best performance, we recommend that you run Lync Server on servers with hardware that meets the requirements in the following table. If you use less powerful hardware, you may experience functionality problems or poor performance. Note that these hardware requirements are higher than those of previous versions of Lync Server, primarily because in Lync Server 2013, all Front End Servers run SQL Server.

Recommended Hardware for Front End Servers, Back End Servers, Standard Edition Servers, and Persistent Chat Store and Persistent Chat Compliance Store (Back End Server Roles for Persistent Chat Server)

Hardware component	Recommended
CPU	64-bit dual processor, hex-core, 2.26 gigahertz (GHz) or higher Intel Itanium processors are not supported for Lync Server server roles.
Memory	32 gigabytes (GB)
Disk	• 8 or more 10,000 RPM hard disk drives with at least 72 GB free disk space. Two of the disks should use RAID 1, and six should use RAID 10. - OR - • Solid state drives (SSDs) which provide performance similar to 8 10,000-RPM

	mechanical disk drives.
Network	• 1 dual-port network adapter, 1 Gbps or higher (2 recommended, which requires teaming with a single MAC address and single IP address)

Recommended Hardware for Edge Servers, Standalone Mediation Servers, and Directors

Hardware component	Recommended
CPU	• 64-bit dual processor, quad-core, 2.0 gigahertz (GHz) or higher - OR - • 64-bit 4-way processor, dual-core, 2.0 GHz or higher Intel Itanium processors are not supported for Lync Server server roles.
Memory	16 gigabytes (GB)
Disk	• 4 or more 10,000 RPM hard disk drives with at least 72 GB free disk space - OR - • Solid state drives (SSDs) which provide performance similar to 4 10,000-RPM mechanical disk drives.
Network	• 1 dual-port network adapter, 1 Gbps or higher (2 recommended, which requires teaming with a single MAC address and single IP address)

1.2.5.2 Client and Device Hardware Support

Client and Device Hardware Support

Microsoft Lync Server 2013 > Supportability > Supported Hardware >

Topic Last Modified: *2012-10-01*

Client computers must meet certain hardware requirements to support clients in your Lync Server 2013 deployment. Additional hardware configurations must be in place before you deploy IP phones and analog devices.

- Lync Client Hardware Support
- Device Hardware Support
- Mobility Support

1.2.5.2.1 Lync Client Hardware Support

Lync Client Hardware Support

Supportability > Supported Hardware > Client and Device Hardware Support >

Topic Last Modified: *2012-12-14*

This section describes the recommended hardware for Lync 2013 and the Online Meeting Add-in for Lync 2013.

Recommended Hardware for Lync 2013 and the Online Meeting Add-in for Lync 2013

System component	Minimum requirement
Computer/processor	Intel Pentium 4, AMD Athlon 64, or equivalent
Memory	2 gigabytes (GB) of RAM
Data and Voice	Minimum 1.6 gigahertz (GHz) or faster processor. We recommend 2.0 gigahertz (32-bit or 64- bit).
Video	See Lync Client Video Requirements
Display resolution	1024x768 required
Graphics hardware	• Support for Microsoft DirectX 9 application programming interface • 128 megabytes (MB) of graphics memory (minimum). We recommend 256 MB of graphics memory. • Windows Display Driver Model driver • Pixel Shader 2.0 in hardware • 32 bits per pixel
Telephony	Microphone and speakers, headset with microphone, or equivalent device(s). Recommended devices: • Phones with the "Optimized for Microsoft Lync" logo (see Phones and Devices Qualified for Microsoft Lync at http://go.microsoft.com/fwlink/p/?LinkID=208938 for a list) • Phones that run Lync Phone Edition
Video source	USB 2.0 video camera or Polycom CX5000 HD device (RoundTable device)
Bandwidth Requirements	See Network Bandwidth Requirements for Media Traffic

1.2.5.2.2 Device Hardware Support

Device Hardware Support

Supportability > Supported Hardware > Client and Device Hardware Support >

Topic Last Modified: *2012-12-14*

Specific hardware configurations must be in place before you deploy IP phones and analog devices.

IP phones running Lync Phone Edition support Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) and Power over Ethernet (PoE). To take advantage of LLDP-MED, the switch must support IEEE802.1AB and ANSI/TIA-1057. To take advantage of PoE, the switch must support PoE802.3AF or 802.3at.

To enable LLDP-MED, the administrator must enable LLDP by using the switch console window and set the LLDP-MED network policy with the correct voice VLAN ID.

In addition, if your deployment includes analog devices, you must configure the analog gateway to use Lync Server, and the gateway must be one of the following:

- An analog telephone adapter (ATA)
- A PSTN analog gateway
- A Survivable Branch Appliance that includes a PSTN analog gateway
- A Survivable Branch Appliance that includes a PSTN gateway that communicates with an ATA

To learn how to configure an analog gateway, see "Planning to Deploy Analog Devices" at http://go.microsoft.com/fwlink/p/?LinkId=268537 in the Lync Server 2010 TechNet Library. (Analog devices work the same way in Lync Server 2013 as they do in Lync Server 2010.)

◆**Important:**
You can configure the switch for Enhanced 9-1-1 (E9-1-1), if the switch supports this.

1.2.5.2.3 Mobility Support

Mobility Support

Supportability > Supported Hardware > Client and Device Hardware Support >

Topic Last Modified: *2012-06-29*

With Lync Server 2013 mobility, users have access to Lync 2013 functionality on their mobile devices. Supported mobile devices include the following:

- Supported Apple iOS devices
- Windows Phone
- Android
- Nokia

For details about mobility features and requirements, see Planning for Mobility in the Planning documentation.

1.2.5.3 File Storage Support

File Storage Support

Microsoft Lync Server 2013 > Supportability > Supported Hardware >

Topic Last Modified: *2012-10-16*

Lync Server 2013 uses the same file store for all file storage. File storage support includes the following:

- A file share on either direct attached storage (DAS) or a storage area network (SAN), including Distributed File System (DFS), and on a redundant array of independent disks (RAID) for file stores. For details about storage requirements, see Technical Requirements for Front End Servers, Instant Messaging, and Presence and Hardware and Software Requirements for the Director in the Planning documentation. For details about DFS for Windows Server 2008 operating system, see the DFS Step-by-Step Guide for Windows Server 2008 at http://go.microsoft.com/fwlink/p/?linkId=202835.
- A shared cluster for the file share. If you use a shared cluster, you should use cluster servers running Windows Server 2008 or Windows Server 2008 R2. Using cluster servers running an older version of Windows may result in permission issues that prevent some features from being available. Use the Cluster Administrator to create the file shares. For details about using the Cluster Administrator, see Microsoft Knowledge Base article 284838, "How to

Create a Server Cluster File Share with Cluster.exe" at http://go.microsoft.com/fwlink/p/?linkId=140899.

1.2.6 Server Software and Infrastructure Support

Server Software and Infrastructure Support

Microsoft Lync Server 2013 > Supportability >

Topic Last Modified: *2012-06-29*

Software support for server components, including all Lync Server 2013 server roles and storage, includes supported operating systems, database software, infrastructure software, and other software required to support specific functionality. It also includes virtualization of server components.

- Server and Tools Operating System Support
- Database Software Support
- Exchange Server and SharePoint Integration Support
- Certificate Infrastructure Support
- Wildcard Certificate Support
- Domain Name System (DNS) Infrastructure Support
- Internet Information Services (IIS) Support
- IP and Networking Protocol Support
- Public Instant Messaging Support
- Browser Support for Lync Server 2013 Control Panel
- Voice Support
- Virtualization Support

1.2.6.1 Server and Tools Operating System Support

Server and Tools Operating System Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-10-22*

All server roles support the same Windows Server operating systems. The required operating system support for other server roles, such as database servers, depends on what software you install on those servers.

Lync Server 2013 administrative tools are installed by default on the server running Lync Server 2013, but you can install administrative tools separately on other computers running Windows operating systems. For example, you can use a client computer running Windows 7 with Service Pack 1 (SP1) as an administrative console for planning purposes.

◆**Important:**
Lync Server 2013 is available only in 64-bit, which requires 64-bit hardware and 64-bit editions of Windows Server. This means that all server roles and computers running Lync Server 2013 administrative tools run a 64-bit edition operating system.

Operating Systems for Server Roles

Lync Server 2013 supports the 64-bit editions of the following operating systems:

- The Windows Server 2008 R2 with Service Pack 1 (SP1) Standard operating system (required) or latest service pack (recommended)
- The Windows Server 2008 R2 with SP1 Enterprise operating system (required)

or latest service pack (recommended)
- The Windows Server 2008 R2 with SP1 Datacenter operating system (required) or latest service pack (recommended)
- The Windows Server 2012 Standard operating system
- The Windows Server 2012 Datacenter operating system

Lync Server 2013 is not supported on the following:
- The Server Core installation option of Windows Server 2008 R2 or Windows Server 2012
- The Windows Web Server 2008 R2 operating system or the Windows Web Server 2012 operating system
- Windows Server 2008 R2 HPC Edition or Windows Server 2012 HPC Edition

Operating Systems for Other Servers

Operating system support for servers other than those on which you deploy Lync Server 2013 server roles depends on the software that you plan to install on those servers. For details about requirements for Back End Servers and other database servers, see Database Software Support in the Supportability documentation. For details about requirements for reverse proxy servers (for Edge deployment), see Internet Information Services (IIS) Support in the Supportability documentation. For details about other software requirements, including infrastructure and virtualization support, see the other topics in the Server Software and Infrastructure Support section of the Supportability documentation.

Additional Operating Systems for Administrative Tools

Lync Server 2013 supports installation of the administrative tools, which includes the Topology Builder, on computers running any of the 64-bit editions of the operating systems supported for deployment of server roles (as described in the previous section). Additionally, you can install administrative tools on the 64-bit editions of the following operating systems:
- The Windows 7 operating system with SP1 operating system (required) or latest service pack (recommended)
- The Windows 8 operating or latest service pack (recommended)

1.2.6.2 Database Software Support

Database Software Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2013-03-12*

The following list contains the database management systems for the back-end database, the Archiving database, the Monitoring database, the Persistent Chat database, and the Persistent Chat compliance database that are supported by Lync Server 2013:
- **Back-end database of a Front End pool, Archiving database, Monitoring database, persistent chat database, and persistent chat compliance database**
  - Microsoft SQL Server 2008 R2 Enterprise database software (64-bit edition). Additionally running the latest service pack is recommended.
  - Microsoft SQL Server 2008 R2 Standard (64-bit edition). Additionally running the latest service pack is recommended.
  - Microsoft SQL Server 2012 Enterprise (64-bit edition). Additionally running the latest service pack is recommended.

  - Microsoft SQL Server 2012 Standard (64-bit edition). Additionally running the latest service pack is recommended.
- **Standard Edition server database and local configuration store databases**
  - Microsoft SQL Server 2012 Express (64-bit edition)

Note:
Microsoft SQL Server 2012 Express (64-bit edition) is automatically installed by Lync Server 2013 on each Standard Edition server and each Lync Server 2013 server on which the local configuration store is deployed.

Important:
- Lync Server 2013 does not support the 32-bit edition of SQL Server. You must use the 64-bit edition.
- SQL Server Web edition and SQL Server Workgroup edition are not supported. You cannot use them with Lync Server 2013.
- Lync Server 2013 does support native database mirroring.
- To use the Monitoring Server role, you should install SQL Server Reporting Services.

In a Front End pool, the back-end database can be a single SQL Server computer.

Important:
If you collocate Lync Server databases with other databases, we highly recommend assessing all factors that might affect availability and performance, as well as ensuring that, if one node fails, the remaining node can handle the load. To verify failover capabilities, we recommend testing all failover scenarios.

SQL Clustering Topologies

SQL clustering topologies are not supported for new Lync Server 2013 deployments. For Back End Server high availability, SQL mirroring is the recommended and supported option.

If you are upgrading from a previous version of Lync Server and you have deployed an Enterprise Edition Front End pool that uses SQL clustering in that existing Lync Server topology, we recommend that you implement SQL Mirroring as a replacement for the existing SQL clustering deployment. However, continuing to use the existing SQL cluster with Lync Server 2013 is supported, but not recommended.

1.2.6.3 Exchange Server and SharePoint Integration Support

Exchange Server and SharePoint Integration Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-09-30*

Lync Server 2013 and Lync 2013 can securely and seamlessly communicate with other applications and server products, including Office 2013, Exchange 2013, and SharePoint, if you integrate these products. Integrating Lync Server 2013 and Office provides users with in-context access to the instant messaging (IM), enhanced presence, telephony, and conferencing capabilities of Lync. Office users can access Lync features from within the Outlook 2013 messaging and collaboration client and other Office programs or from a Microsoft SharePoint Server 2010 page. Users can also view a record of Lync conversations in the Outlook Conversation History folder. When integrated with Exchange 2013, Lync Server 2013 also supports the following the following:

- Unified contact store, which enables users to store all contact information in

Exchange 2013 so that the information is available globally across Lync 2013, Exchange 2013, Outlook, and Outlook Web App.

- Conversation history and Web conferencing history, which is stored in Exchange 2013 user folders.
- Archive data for users who are homed on Exchange 2013, if their mailboxes have been put on In-Place Hold.

Note:

Lync Server 2013 supports integration with previous versions of Microsoft Exchange Server and SharePoint, but not all functionality is supported with these previous versions, such as integration of Archiving storage with Microsoft Exchange.
If you are migrating your users to Exchange 2013, you can use both Exchange storage and Lync Server storage on an interim basis, while you complete the migration. Permanent use of both Exchange and Lync Server storage is not supported.

Integration of Lync Server 2013 with Exchange 2013 and SharePoint Server requires server-to-server authentication between servers running Lync Server 2013, Microsoft Exchange Server, and SharePoint Server. Lync Server 2013 supports OAuth (Open Authorization) protocol for server-to-server authentication and authorization. For on-premises server-to-server authentication between two Microsoft servers, there is no need to use a third-party token server. Lync Server 2013, Exchange 2013, and SharePoint have a built-in token server that can be used for authentication purposes with each other. For example, Lync Server 2013 can issue and sign a security token by itself, and use that token when communicating with Exchange 2013. In this case, there is no need to use a third-party token server.

Lync Server 2013 supports the two server-to-server authentication scenarios. These include configuration of server-to-server authentication between the following:

- An on-premise installation of Lync Server 2013 and an on-premises installation of Exchange 2013 and/or SharePoint Server.
- A pair of Office components (for example, between Microsoft Exchange 365 and Microsoft Lync Server 365, or between Microsoft Lync Server 365 and Microsoft SharePoint 365).

Note:

Server-to-server authentication between an on-premises server and an Office 365 component is not supported in this Lync Server 2013 release. Among other things, this means that you cannot set up server-to-server authentication between an on-premises installation of Lync Server 2013 and Microsoft Exchange 365.

For details about server-to-server authentication, see Managing Server-to-Server Authentication (Oauth) and Partner Applications in the Deployment documentation or Operations documentation.

1.2.6.4 Certificate Infrastructure Support

Certificate Infrastructure Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-11-16*

Lync Server 2013 requires a public key infrastructure (PKI) to support Transport Layer Security (TLS) and mutual TLS (MTLS) connections. By default, Lync Server 2013 is configured to use TLS for client-to-server connections. MTLS is used for connections between servers.

MTLS certificates must be issued by trusted certification authorities (CAs) for Lync Server

2013. Lync Server supports certificates that are issued from the following CAs:

- Certificates issued from an internal CA:
  - The Windows Server 2003 operating system CA
  - The Windows Server 2008 operating system CA
  - The Windows Server 2008 R2 operating system CA
  - The Windows Server 2012 operating system CA
- Certificates issued from a public CA

Communication with other applications and servers, such as Exchange 2013, requires a certificate that is supported by the other applications and products. For the 2013 release, Lync Server 2013 and other Microsoft server products, including Exchange 2013 and SharePoint Server, support the Open Authorization (OAuth) protocol for server-to-server authentication and authorization. For details, see Managing Server-to-Server Authentication (Oauth) and Partner Applications in the Deployment documentation or the Operations documentation.

For connections from clients running Windows 7 operating system, Windows Server 2008 R2 operating system, and Microsoft Office Communicator 2007 Phone Edition, Lync Server 2013 includes support for (but does not require) certificates signed using the SHA-256 cryptographic hash function. To support external access using SHA-256, the external certificate is issued by a public CA using SHA-256.

For details about certificate requirements, see Certificate Infrastructure Requirements in the Planning documentation. For details about use of wildcards with certificates, see Wildcard Certificate Support in the Supportability documentation.

1.2.6.5 Wildcard Certificate Support

Wildcard Certificate Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-09-21*

Lync Server 2013 uses certificates to provide communications encryption and server identity authentication. In some cases, such as web publishing through the reverse proxy, strong subject alternative name (SAN) entry matching to the fully qualified domain name (FQDN) of the server presenting the service is not required. In these cases, you can use certificates with wildcard SAN entries (commonly known as “wildcard certificates”) to reduce the cost of a certificate requested from a public certification authority and to reduce the complexity of the planning process for certificates.

⚠**Warning:**
To retain the functionality of unified communications (UC) devices (for example, desk phones), you should test the deployed certificate carefully to ensure that devices function properly after you implement a wildcard certificate.

There is no support for a wildcard entry as the subject name (also referred to as the common name or CN) for any role. The following server roles are supported when using wildcard entries in the SAN:

- **Reverse proxy.** Wildcard SAN entry is supported for simple URL publishing certificate.
- **Director.** Wildcard SAN entry is supported for simple URLs in Director web components.
- **Front End Server (Standard Edition) and Front End pool (Enterprise Edition).** Wildcard SAN entry is supported for simple URLs in Front End web components.

- **Exchange Unified Messaging (UM).** The server does not use SAN entries when deployed as a stand-alone server.
- **Microsoft Exchange Server Client Access server.** Wildcard entries in the SAN are supported for internal and external clients.
- **Exchange Unified Messaging (UM) and Microsoft Exchange Server Client Access server on same server.** Wildcard SAN entries are supported.

Server roles that are not addressed in this topic:

- Internal server roles (including, but not limited to the Mediation Server, Archiving and Monitoring Server, Survivable Branch Appliance, or Survivable Branch Server)
- External Edge Server interfaces
- Internal Edge Server

> **Note:**
> For the internal Edge Server interface, a wildcard entry can be assigned to the SAN, and is supported. The SAN on the internal Edge Server is not queried, and a wildcard SAN entry is of limited value.

For details about certificate configurations, including the use of wildcards in certificates, see the following topics:

- Certificate Requirements for Internal Servers
- Certificate Requirements for External User Access
- Certificate Summary - DNS and HLB Load Balanced
- Certificate Summary - Single Director
- Certificate Summary - Scaled Director Pool, Hardware Load Balancer
- Certificate Summary - Reverse Proxy
- Guidelines for Integrating On-Premises Unified Messaging and Lync Server 2013

For details about configuring certificates for Exchange, including the use of wildcards, see the Exchange 2013 product documentation.

1.2.6.6 Domain Name System (DNS) Infrastructure Support

Domain Name System (DNS) Infrastructure Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2013-03-08*

Lync Server 2013 requires Domain Name System (DNS) and uses it in the following ways:

- To discover internal servers or pools for server-to-server communications.
- To enable clients to discover the Front End pool or Standard Edition server used for various SIP transactions.
- To associate the simple URLs for conferences with the servers hosting those conferences.
- To enable external servers and clients to connect to Edge Servers or the HTTP reverse proxy for instant messaging (IM) or conferencing.
- To enable unified communications (UC) devices that are not logged in to discover the Front End pool or Standard Edition server running Device Update Web service, obtain updates, and send logs.
- To enable mobile clients to automatically discover Web Services resources without requiring users to manually enter URLs in device settings.
- For DNS load balancing.

Note:
Lync Server 2013 does not support internationalized domain names (IDNs).

Important:
The name you specify must be identical to the computer name configured on the server. By default, the computer name of a computer that is not joined to a domain is a short name, not a fully qualified domain name (FQDN). Topology Builder uses FQDNs, not short names. So, you must configure a DNS suffix on the name of the computer to be deployed as an Edge Server that is not joined to a domain. **Use only standard characters** (including A–Z, a–z, 0–9, and hyphens) when assigning FQDNs of your Lync Servers, Edge Servers, and pools. Do not use Unicode characters or underscores. Nonstandard characters in an FQDN are often not supported by external DNS and public CAs (that is, when the FQDN must be assigned to the SN in the certificate).

1.2.6.7 Internet Information Services (IIS) Support

Internet Information Services (IIS) Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-06-29*

Several Lync Server 2013 components require Internet Information Services (IIS). Supported versions of IIS included the following:

- IIS 8.0
- IIS 7.5

For details about the IIS requirements for Lync Server 2013 components, see Internet Information Services (IIS) Requirements in the Planning documentation.

1.2.6.8 IP and Networking Protocol Support

IP and Networking Protocol Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-09-21*

Lync Server 2013 supports the following IP and networking protocols:

- **IP Protocols.** Lync Server 2013 supports either IP version 4 (IPv4) or IP version 6 (IPv6) for the server network.

  Note:
  Lync Server 2013 can function in a network with dual IP stack enabled.

- **SIP Transport Protocols.** Generically, SIP can use at least three transport types: User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Transport Layer Security (TLS). In the default SIP transport configuration, TLS runs over TCP. TLS is used within the Lync Server 2013 network. At the edge of the network, Lync Server 2013 can interoperate over TCP. Lync Server 2013 does not support UDP for SIP transport because it doesn’t meet the minimum standards for enterprise communications security, reliability, and scalability. For details, see the NextHop blog article, "To UDP, or not to UDP, that is the question," at http://go.microsoft.com/fwlink/p/?linkId=185369.

  Note:

The content of each blog and its URL are subject to change without notice.

1.2.6.9 Public Instant Messaging Support

Public Instant Messaging Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2013-01-11*

Lync Server 2013 supports the use of licensed public instant messaging (IM) connectivity providers, as well as the use of eXtensible Messaging and Presence Protocol (XMPP) to implement a special type of federation that enables a Lync Server to access configured XMPP domain partners by using the Lync 2013 client.

Public IM Connectivity Provider Support

The currently supported public instant messaging connectivity partners are:

- America Online
- Windows Live
- Yahoo!

For communications with Windows Live users, Lync Server 2013 supports peer-to-peer IM and audio and video calls. For communications with AOL and Yahoo!, Lync Server 2013 supports peer-to-peer IM. A separate license may be required.

Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

XMPP Federation Support

XMPP federation supports Lync users communication with configured XMPP domain users who use a public provider, such as GTalk. Communications with these users can include the following:

- Peer-to-peer IM and presence
- Creation of XMPP federated contacts in the Lync client

1.2.6.10 Browser Support for Lync Server 2013 Control Panel

Browser Support for Lync Server 2013 Control Panel

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-09-28*

Lync Server 2013 supports the use of Topology Builder and Lync Server 2013 Control Panel is supported when using the following browsers:

- Internet Explorer 10, 32-bit
- Internet Explorer 9, 32-bit
- Internet Explorer 8, 32 bit

1.2.6.11 Voice Support

Voice Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-06-29*

If your deployment includes a Front End pool, you can deploy support for Enterprise Voice, the Voice over IP (VoIP) solution offered by Microsoft. Voice over IP (VoIP) is a software-based alternative to traditional PBX-based telephony. Although the VoIP call experience is similar to the traditional telephony experience, Enterprise Voice includes features that enable richer communication and collaboration. For example, your Enterprise Voice deployment can be configured to make it possible for Lync 2013 and Lync Phone Edition users to view enhanced presence information or location information for contacts in your organization's address book. Some Lync Server 2013 features are enabled through integration with other Lync Server 2013 workloads and with Exchange Unified Messaging (UM). For details about the features and functionality available with Enterprise Voice and how to plan for deployment, see Planning for Enterprise Voice in the Planning documentation.

- SIP Trunking Support
- Direct SIP Connections Support
- Exchange Unified Messaging (UM) Support
- E9-1-1 Support

1.2.6.11.1 SIP Trunking Support

SIP Trunking Support

Supportability > Server Software and Infrastructure Support > Voice Support >

Topic Last Modified: *2012-10-03*

If you plan to use Enterprise Voice with SIP trunking, you must deploy a Mediation Server and make sure that other infrastructure and components meet the support requirements appropriate to your deployment model. For details about determining whether to implement SIP trunking, see Overview of SIP Trunking in the Planning documentation.

You can use the Microsoft Unified Communications Open Interoperability Program for enterprise telephony infrastructure to find qualified public switched telephone network (PSTN) gateways, IP-PBXs, and SIP trunking services, including qualified IP telephony service providers. For details, see the Microsoft Unified Communications Open Interoperability Program website at http://go.microsoft.com/fwlink/p/?LinkId=203309.

Mediation Server Support

To implement SIP trunking, you must route the connection through a Mediation Server, which acts as a proxy for communications sessions between Lync Server 2013 clients and the service provider. The Mediation Server decodes the media traffic from clients and servers and re-encodes it before sending it to the service provider. The re-encoding is needed because SIP trunks do not support some codecs used, such as Real Time Audio (RTA) or Interactive Connectivity Establishment (ICE) protocol negotiation for firewall traversal.

Each Mediation Server can have two network adapters, which provide an internal and an external network interface. The external interface is commonly called the gateway interface because, traditionally, it has been used to connect to a PSTN gateway or an IP-PBX. To implement a SIP trunk, you connect the external interface to a Session Border Controller (SBC) at a service provider.

Centralized vs. Distributed SIP Trunking

Centralized SIP trunking routes all Voice over Internet Protocol (VoIP) traffic, including branch site traffic, through your data center. The centralized deployment model is simple, cost-effective, and is generally the preferred approach for implementing SIP trunks with Lync Server 2013.

Depending on usage patterns within your enterprise, you may not want to route all users through the centralized SIP trunk. To analyze your needs, answer the following questions:

- How big is each site? How many users?
- Which Direct Inward Dialing (DID) numbers at each site get the most phone calls?

Distributed SIP trunking is a deployment model in which you implement a local SIP trunk at one or more branch sites. VoIP traffic is then routed from the branch site directly to their service provider, without going through your data center.

Distributed SIP trunking is required only in the following cases:

- The branch site requires survivable phone connectivity (for example, if the WAN goes down). If the branch does need redundancy and failover, the service provider will charge more and the configuration will take longer. This should be analyzed for each branch site. Some of your branches may require redundancy and failover, while others may not.
- The branch site and data center are in different countries/regions. For compatibility and legal reasons, you need at least one SIP trunk per country/region.

Deciding whether to deploy centralized or distributed SIP trunking requires a cost-benefit analysis. In some cases, it may be advantageous to opt for the distributed deployment mode, even if it is not required. In a completely centralized deployment, all branch site traffic is routed over WAN links. Instead of paying for the bandwidth required for WAN linking, you may want to use distributed SIP trunking.

Note:
For details about why and how you might use distributed SIP trunking, see Branch Site SIP Trunking in the Planning documentation.

Supported SIP Trunking Connection Types

Lync Server 2013 supports the following connection types for SIP trunking:

- Multiprotocol Label Switching (MPLS) is a private network that directs and carries data from one network node to the next. The bandwidth in an MPLS network is shared with other subscribers, and each data packet is assigned a label to distinguish one subscriber's data from another's. This connection type does not require VPN. A potential drawback is that excessive IP traffic can interfere with VoIP operation unless VoIP traffic is given priority.
- A private connection with no other traffic is typically the most reliable and secure connection type (for example, a leased fiber-optic connection or T1 line). This connection type provides the highest call-carrying capacity, but is typically the most expensive. VPN is not required. Private connections are appropriate for organizations with high call volumes or stringent security and availability requirements.
- The public Internet is the least expensive connection type, but also the least reliable, and the one with the lowest call-carrying capacity. Your Internet Telephony Service Provider (ITSP) can help secure this SIP trunk connection type if it supports Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) to encrypt signaling and media traffic. If you cannot configure a SIP trunk connection through the Internet to use TLS and SRTP, we strongly recommend that you use a VPN tunnel to provide a more secure connection. Contact your ITSP to determine whether it provides support for TLS with SRTP.

Selecting a Connection Type

The most appropriate SIP trunking connection type for your enterprise depends on your needs and your budget.

- For a mid-size or larger enterprise, an MPLS network generally provides the most value. It can provide the necessary bandwidth at a cheaper rate than a specialized private network.
- Large enterprises may require a private fiber-optic or T1 connection.
- For a small enterprise or branch site with low call volume, SIP trunking through the Internet may be the best choice. However, this connection type is not recommended for mid-size or larger sites.

Codec Support

The service provider proxy must support the following codecs:

- G.711 a-law (used primarily outside North America)
- G.711 µ-law (used in North America)

1.2.6.11.2 Direct SIP Connections Support

Direct SIP Connections Support

Supportability > Server Software and Infrastructure Support > Voice Support >

Topic Last Modified: *2012-06-29*

Lync Server 2013 supports the use of direct SIP connections to connect Lync Server 2013 to either of the following:

- An IP-PBX
- A PSTN gateway

The Mediation Servers in a Lync Server 2013 pool can control multiple gateways, Session Border Controllers (SBCs) provided by telephony service providers, or some combination thereof. Additionally, multiple Mediation Servers in the pool can interact with a single gateway.

You can use the Microsoft Unified Communications Open Interoperability Program for enterprise telephony infrastructure to find qualified PSTN gateways, IP-PBXs, and SIP trunking services. For details, see the Microsoft Unified Communications Open Interoperability Program website at http://go.microsoft.com/fwlink/p/?linkId=203309.

For details about the topology and deployment options for direct SIP connections, see Direct SIP Connections in the Planning documentation.

1.2.6.11.3 Exchange Unified Messaging (UM) Support

Exchange Unified Messaging (UM) Support

Supportability > Server Software and Infrastructure Support > Voice Support >

Topic Last Modified: *2012-09-21*

Lync Server 2013 supports integration with Exchange Unified Messaging (UM) for combining voice messaging and email messaging into a single messaging infrastructure. In Exchange 2013, Exchange UM consists of the Exchange UM service, which is installed and runs on the Mailbox server, and the UM Call Router, which is installed and runs on the Client Access server. For Lync Server 2013 Enterprise Voice deployments, Exchange UM combines voice messaging and email messaging into a single store that is accessible from a telephone (that is, Outlook Voice Access) or a computer. Exchange UM and Lync Server 2013 work together to provide call answering, Outlook Voice Access, and auto attendant services to users of Enterprise Voice.

In addition to the support for integration with on-premises deployments of Exchange UM, Lync Server 2013 supports integration with hosted Exchange UM. This enables you to provide voice messaging to your users if you migrate some or all of them to a hosted Exchange service provider such as Microsoft Exchange Online.

Lync Server 2013 supports the following versions:

- Microsoft Exchange 2013
- Microsoft Exchange Server 2010 (required) or with latest service pack (recommended)
- Microsoft Exchange Server 2007 with Service Pack 1 (SP1) (required) or latest service pack (recommended)

You cannot collocate Exchange UM with Lync Server 2013 or a Lync Server 2013 database. You can install Exchange UM and Lync Server 2013 in separate forests.

Note:

Exchange UM may not be required for Enterprise Voice deployments that have a PBX deployed, because the PBX can continue to provide voice mail and related services to all users. If you eventually retire the PBX (for example, if you deploy SIP trunking for public switched telephone network (PSTN) connectivity), you must reconfigure Exchange UM to provide voice mail to users who previously used the PBX voice mail system.

- Components and Topologies for On-Premises Unified Messaging
- Support for Hosted Exchange UM Integration

1.2.6.11.3.1 Components and Topologies for On-Premises Unified Messaging

Components and Topologies for On-Premises Unified Messaging

Server Software and Infrastructure Support > Voice Support > Exchange Unified Messaging (UM) Support >

Topic Last Modified: *2012-09-25*

This topic describes the Microsoft Exchange Server 2013 components required to provide Exchange Unified Messaging (UM) features to Lync Server 2013 deployment. It also describes the supported topologies for on-premises Exchange UM integration.

Exchange Server Components

To provide the Exchange UM features and services described in Features of Integrated Unified Messaging and Lync Server 2013 to Enterprise Voice users in your organization, you must deploy an Microsoft Exchange Mailbox server and Client Access server, which hosts user mailboxes and provides a single storage location for email and voice mail. Exchange UM runs as a service on Exchange Mailbox and Client Access servers.

For details about Exchange UM components in Microsoft Exchange Server 2007 and Microsoft Exchange Server 2010, see Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail in the Deployment documentation.

Supported Topologies

You can deploy Lync Server 2013 and Exchange Unified Messaging (UM) in the same forest or multiple forests. If the deployment spans multiple forests, you must perform the Exchange integration steps for each Exchange UM forest. Furthermore, you must configure each Microsoft Exchange forest to trust the Lync Server 2013 forest and the Lync Server 2013 forest to trust each Exchange UM forest. In addition to this forest trust, the Exchange UM settings for all users must be set on the user objects in the Lync Server 2013 forest.

Lync Server 2013 supports the following topologies for Exchange UM integration:

- Single forest
- Single domain (that is, a single forest with a single domain). Lync Server 2013, Microsoft Exchange, and users all reside in the same domain.
- Multiple domain (that is, a root domain with one or more child domains). Lync Server 2013, and Microsoft Exchange servers are deployed in different domains from the domain where you create users. Exchange UM servers can be deployed in different domains from the Lync Server 2013 pool they support.
- Multiple forest (that is, resource forest). Lync Server 2013 is deployed in a single forest, and then users are distributed across multiple forests. The users' Exchange UM attributes must be replicated over to the Lync Server 2013 forest.

Note:
Exchange can be deployed in multiple forests. Each Exchange organization can provide Exchange UM to its users, or Exchange UM can be deployed in the same forest as Lync Server 2013.

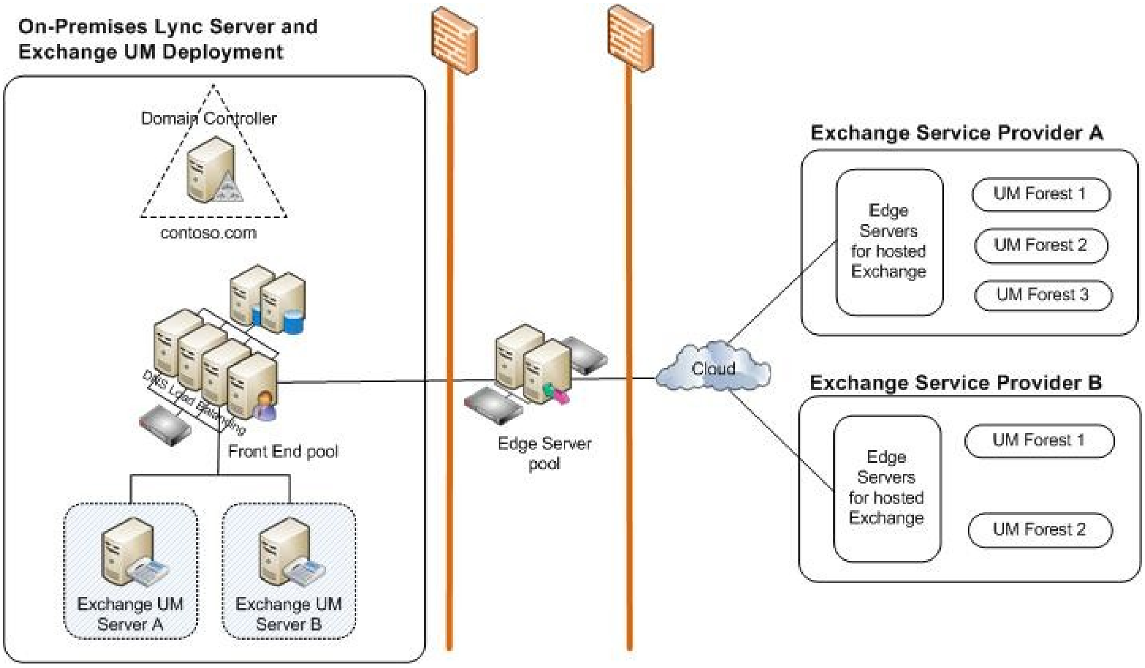
1.2.6.11.3.2 Support for Hosted Exchange UM Integration

Support for Hosted Exchange UM Integration

Server Software and Infrastructure Support > Voice Support > Exchange Unified Messaging (UM) Support >

Topic Last Modified: *2012-09-21*

The Lync Server 2013 ExUM Routing application supports integration with Exchange Unified Messaging (UM) in an on-premises environment, where Lync Server 2013 and Exchange UM are both installed locally within your enterprise, or in with Exchange UM hosted by a service provider, as shown in the following diagram.



The following modes are supported:

- **On-premises Mode** Lync Server 2013 and Exchange UM are both deployed on local servers within your enterprise.
- **Cross-premises Mode** Lync Server 2013 is deployed on local servers within your enterprise and Exchange UM is hosted in an online service provider's facility, such as a Microsoft Exchange Online data center.
- **Mixed Mode** Your Lync Server 2013 deployment has some user mailboxes homed on local servers running Microsoft Exchange Server within your enterprise and some mailboxes homed in a hosted Exchange service data center.

Note:

Mixed mode can be used as a transitional solution during evaluation and stepwise migration of users to hosted Exchange UM, or as a permanent solution if you opt to keep some users' Exchange UM services on-premises after migrating others.

To integrate Lync Server 2013 with hosted Exchange UM, you must configure a *shared SIP address space* (also called a *split domain*). In this configuration, both Lync Server 2013 and the third-party hosted Exchange UM service provider can access the same SIP domain address space. For details, see Hosted Exchange UM Integration Architecture in the Planning documentation.

1.2.6.11.4 E9-1-1 Support

E9-1-1 Support

Supportability > Server Software and Infrastructure Support > Voice Support >

Topic Last Modified: *2012-09-21*

Lync Server 2013 supports Enhanced 9-1-1 (E9-1-1) as part of an enterprise deployment. E9-1-1 is an emergency notification feature that associates the calling party's telephone number with a civic (that is, a street) address. E9-1-1 support is available only in the United States.

To support E9-1-1 as part of a Lync Server 2013 deployment, you must obtain E9-1-1 routing service from a certified emergency services provider or use an Emergency Location Identification Number (ELIN) gateway. The emergency services provider or carrier routes emergency calls that originate from Lync Server 2013 to the correct Public Safety Answering Point (PSAP), based on the location information contained within the call. For details about E9-1-1 support, see Planning for Emergency Services (E9-1-1) in the Planning documentation.

1.2.6.12 Virtualization Support

Virtualization Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-09-21*

Lync Server 2013 supports virtualization topologies that support all major workloads, including instant messaging (IM) and presence, conferencing, and Enterprise Voice. Virtualization is supported only on the Windows Server 2008 R2 operating system and Windows Server 2012 for all host and guest operating systems.

Lync Server 2013 supports virtualization of the following:

- **Servers in Front End pools.** If you virtualize a Front End Server, you can also virtualize some or all of the other server roles in the pool.
- **Standard Edition servers.** When deploying a virtualized Standard Edition server, the only server roles that can be deployed with it are Director and Edge Server, as well as Monitoring and Archiving, both of which run on the Standard Edition server.
- **Edge Servers for Front End pools and Standard Edition servers.**

Support includes both of the following:

- Microsoft Hyper-V technology
- VMWare

1.2.7 Additional Server Support and Requirements

Additional Server Support and Requirements

Microsoft Lync Server 2013 > Supportability >

Topic Last Modified: *2012-10-18*

In addition to the software support described in the other sections of this Supportability documentation, Lync Server 2013 has the following support limitations:

- Lync Server 2013 supports Domain Name System (DNS) and hardware load balancing for specific server roles. It also supports application load balancing for Mediation Servers, where appropriate. For details about when to use each, see the Planning documentation.
- Lync Server 2013 uses the Distribution List Expansion Protocol (DLX) to expand distribution lists. This protocol also specifies the web service method that is used to get the membership of a distribution list. Microsoft Exchange Server supports dynamic groups that do not have members statically assigned to them. Instead, they store queries that are evaluated when the group is expanded. DLX does not support dynamic distribution lists.
- The Enable User Wizard does not support automatic conversion of non-English characters to a SIP-compliant URI, so you must modify the SIP address manually.
- For servers running antivirus software, include all servers running Lync Server 2013 in the exception list in order to provide optimal performance and audio quality.
- If you use IPsec, we recommend disabling IPsec over the port ranges used for audio and video traffic. For details, see IPsec Exceptions in the Planning documentation.
- If your organization uses a Quality of Service (QoS) infrastructure, the media subsystem is designed to work within this existing infrastructure. For details about implementing QoS, see Managing Quality of Service (QoS) in the Operations documentation.
- Use of the operating system firewall is supported. Lync Server 2013 manages the firewall exceptions for the operating system firewall, except for Microsoft SQL Server database software. For details about SQL Server firewall requirements, see the SQL Server documentation.
- The external interfaces used to implement support for external user access must be on a separate subnet, *not* on the same network as the internal interfaces.
- The XMPP capability of Lync Server 2013 is tested and supported by Microsoft for instant messaging federation with Google Talk. For any other XMPP systems contact the third-party vendor to verify that they support federation with Lync Server 2013, and for any deployment or troubleshooting recommendations.
- Lync Server 2013 does not support two-factor authentication. However, if you deploy Lync Server 2013 in a network environment that already provides two-factor authentication (for example, a VPN with two-factor authentication), Lync Server 2013 works in that environment.
- Most internal servers require a certificate type defined as **Open Authentication** (OAuth). You are required to request and assign an OAuth certificate during the **Request, Install and Assign Certificates** phase of the Lync Server Deployment Wizard. The minimum size for an OAuth certificate key is 1024 bits. A warning may be displayed if you request a certificate with a key length less than 2048 bits in length. To avoid potential problems in the event that a key length of 2048 is enforced instead of warned, it is strongly recommended to always use a key length of 2048 for OAuth certificates.
- Lync Server 2013 and Microsoft Exchange Server 2010 Service Pack 1 (SP1) operate with support for Federal Information Processing Standard (FIPS) 140-2 algorithms if the Windows Server 2008 R2 operating systems are configured to use the FIPS 140-2 algorithms for system cryptography. To implement FIPS support, you must configure each server running Lync Server 2013 to support it. For details about FIPS-compliant algorithms and how to implement FIPS support, see Microsoft Knowledge Base article 811833, "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing security setting in Windows XP and in later versions of Windows at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=811833. For details about FIPS 140-2 support and limitations in Exchange 2010, see "Exchange 2010 SP1 and Support for FIPS Compliant Algorithms" at http://go.microsoft.com/fwlink/p/?linkId=205335.

Lync Server 2013 requires the installation of other software on specific components prior to or during deployment. This includes software that is available with the operating system, downloadable software, and software that is automatically installed during installation of Lync Server 2013. Following is a list of additional software that can be required:

- Windows Update
- Windows Identity Foundation
- Microsoft .NET 4.5 Framework
- Microsoft Visual C++ 2012 Redistributable

> **Note:**
> Microsoft Visual C++ 2012 Redistributable is automatically installed when you install Lync Server 2013. You should not install and use any other version.

- URL Rewrite Module version 2.0 Redistributable
- Windows Media Format Runtime
- Windows PowerShell version 3.0
- Microsoft Silverlight 4 browser plug-in (Silverlight 4.0.50524.0 or the latest version for Lync Server Control Panel)
- Active Directory Domain Services (AD DS) tools

Some of these software requirements only apply to specific server roles or components. For details about these software requirements, see Additional Software Requirements in the Planning documentation.

1.2.8 Client and Device Software and Infrastructure Support

Client and Device Software and Infrastructure Support

Microsoft Lync Server 2013 > Supportability >

Topic Last Modified: *2012-10-01*

Software support for clients and devices of a Lync Server 2013 deployment includes the supported operating systems, infrastructure software, and other additional software required to support client and device features.

- Lync Client Software Support

> **Note:**
> Lync Phone Edition works the same way with Lync Server 2013 as it does with Lync Server 2010. For details about software support for devices, see the following topics in the Lync Server 2010 TechNet Library:
> - Required Lync Server 2010 Components for Devices at http://go.microsoft.com/fwlink/p/?linkid=256488
> - Device System and Infrastructure Support at http://go.microsoft.com/fwlink/p/?linkid=256489

1.2.8.1 Lync Client Software Support

Lync Client Software Support

See Also

Microsoft Lync Server 2013 > Supportability > Client and Device Software and Infrastructure Support >

Topic Last Modified: *2013-03-07*

This section summarizes software support for Lync 2013 and the Online Meeting Add-in for Lync 2013.

Note:

The Online Meeting Add-in for Lync 2013, which supports meeting management from within the Outlook messaging and collaboration client, installs automatically with Lync 2013.

Software Requirements for Lync 2013 and the Online Meeting Add-in for Lync 2013

System component	Minimum requirement
Windows Operating system	Windows 8 Windows 7 operating system Windows Server 2008 R2 with latest service pack
Installation and updates	Administrator rights and permissions
Browser	Windows Internet Explorer 10 Internet browser Windows Internet Explorer 9 Internet browser Windows Internet Explorer 8 Internet browser Windows Internet Explorer 7 Internet browser Mozilla Firefox web browser **Note:** If you are using Lync with Microsoft Exchange Online and your organization has deployed an authenticating HTTP proxy, Internet Explorer 9 or Internet Explorer 8 is required.
Microsoft Office Integration	For the full set of integration features: • Outlook 2013 messaging and collaboration client • Outlook 2010 messaging and collaboration client
Microsoft Exchange Integration	For the full set of integration features: • Microsoft Exchange Server 2013 • Microsoft Exchange Server 2010

Macintosh Operating Systems

Lync 2013 is available only for Windows. However, Lync Server 2013 supports the following clients on computers that are running Mac OS 10.5.8 or latest service pack or release (Intel-based) operating systems. For details about supported features, see Client Comparison Tables.

- Microsoft Lync for Mac 2011 (see “Lync for Mac 2011 Deployment Guide” at http://go.microsoft.com/fwlink/p/?LinkId=268786)
- Microsoft Communicator for Mac 2011 (see “Communicator for Mac 2011 Deployment Guide” at http://go.microsoft.com/fwlink/p/?LinkId=268787)

Lync Web App Browsers

Lync Web App supports specific combinations of operating systems and browsers. For details, see Lync Web App Supported Platforms in the Planning documentation.

Microsoft Office Supportability

Lync Server 2013 clients support integration with various versions of Microsoft Office, as summarized in this section.

- Lync 2013 integration features are supported on Outlook 2013 and Microsoft Outlook 2010.
- Lync 2013 integration features are supported on Microsoft Exchange Server 2013 and Microsoft Exchange Server 2010.
- Certain Lync 2013 integration features are supported on Microsoft Office 2007 and Microsoft Office 2003 Service Pack 3 (SP3). For integration with Microsoft Office 2007 to work correctly, you may have to install an update to Microsoft Office 2007. For details about the Outlook update, see Microsoft Knowledge Base article 936864, "Description of the 2007 Office hotfix package" at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=936864.
- The Online Meeting Add-in for Lync 2013 is supported with Office 2013, Microsoft Office 2010, Microsoft Office 2007, and the Microsoft Office 2003 suites.

Using Mandatory Profiles

If users are planning to use Lync 2013 conferencing features, they should not use Active Directory Domain Services (AD DS) mandatory profiles to sign in to the Lync 2013 client. Because mandatory profiles are read-only user profiles, the public key infrastructure (PKI) keys that are required for Lync 2013 conferencing cannot be saved to the profile. For details, see Microsoft Knowledge Base article 2552221, “Lync 2010 conferencing feature fails when the user is signed in using a mandatory user profile,” at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=2552221.

⊟See Also

Concepts

Lync Client Hardware Support
Lync Client Video Requirements
Supported Clients from Previous Deployments

1.3 Planning

Planning

Microsoft Lync Server 2013 >

Topic Last Modified: *2012-10-16*

The planning phase is the time in which you decide what Lync Server 2013 features to deploy, and how to deploy them. The topics in this section describe how to plan for a successful Lync Server deployment.

- Planning Primer: Planning for Your Organization
- Determining Your Infrastructure Requirements
- Network Planning for Lync Server
- Capacity Planning
- Planning for High Availability and Disaster Recovery
- Planning for Manageability and Virtualization
- Planning for Front End Servers, Instant Messaging, and Presence
- Planning for Conferencing
- Planning for External User Access

- Planning for Enterprise Voice
- Planning for Monitoring
- Planning for Archiving
- Planning for Persistent Chat Server
- Planning for Exchange Server Integration
- Planning for Clients and Devices in Lync Server 2013
- Planning for Remote Call Control
- Planning for Mobility

1.3.1 Planning Primer: Planning for Your Organization

Planning Primer: Planning for Your Organization

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-24*

The topics in this section help you get started with planning your Lync Server deployment.

- Deciding How to Deploy Microsoft Lync provides guidelines for choosing between these basic deployment scenarios for Lync Server 2013.
- Beginning the Planning Process helps you understand how to get started planning an on-premises deployment and how the planning documentation works with Topology Builder.
- Topology Basics You Must Know Before Planning describes the basics of Lync Server topologies, including sites, server pools, and topologies that support high availability and disaster recovery.
- Initial Planning Decisions takes you through the questions you must answer to decide what workloads and features of Lync Server to deploy.
- Clients for Lync Server 2013 describes the different types of client software that you can deploy to your organization’s users, including computer-installed client software, web-based clients, and mobile devices.
- Reference Topologies shows three sample topologies that illustrate good topology design in three typical organization types, and explains the reasoning behind many of the decisions in designing those topologies.

1.3.1.1 Deciding How to Deploy Microsoft Lync

Deciding How to Deploy Microsoft Lync

Microsoft Lync Server 2013 > Planning > Planning Primer: Planning for Your Organization >

Topic Last Modified: *2012-10-03*

When planning for Lync, the first major decision is how to deploy Microsoft Lync: as Lync Server 2013 on premises, or Lync Online with Microsoft Office 365 in the cloud.

- **Lync Server 2013 on-premises** : This choice provides the complete Lync feature set and provides ultimate flexibility in configuring, customizing, and operating your deployment. All servers are installed onsite and maintained by your organization. An on-premises deployment provides the full range of Lync Server features.
- **Lync Online in the cloud** Lync Online is designed for organizations that want the cost and agility benefits of cloud-based instant messaging, presence, and meetings without sacrificing the business-class capabilities of Lync Server. With Lync Online, Microsoft deploys and maintains the required server infrastructure, and handles ongoing maintenance, patches, and upgrades. Some features available in an on-premises deployment are not available in

Lync Online.

Which type of deployment would be best for you depends on the workloads you want to deploy, and your organization’s geographical and business status.

Lync Server

An on-premises Lync Server deployment is best for the following scenarios:

- **Full Enterprise Voice Capabilities** If you plan to deploy a full Enterprise Voice solution to replace your PBX or which uses advanced calling features, an on-premises Lync Server deployment is required. On-premises supports direct connectivity with PBX systems and trunks, and advanced phone features such as response groups and call park. Lync Online does not currently support these features.
- **Media Quality Controls** If you want the full range of media quality assurance features, such as Call Admission Control (CAC) and Quality of Service (QoS) features, you will want an on-premises deployment .
- **Persistent Chat** If you need to deploy Persistent chat for your organization, you must choose an on-premises deployment.
- **3rd-Party Server Applications** Only on-premises deployments can work with trusted 3rd-party applications that use the Microsoft Unified Communications Managed API (UCMA).
- **Multi-National/Multi-Regional Companies Needing Regional Support** If you have datacenters in multiple countries or regions and need servers to be deployed and managed on a regional basis, an on-premises deployment is best, as it provides this type of regional management capabilities.
- **Complete control over policies, reports, and upgrades** With an on premises Lync Server deployment, you have access to the full set of server and client policies, Monitoring and other reports, and timing of upgrades. Lync Online provides a subset of policy setting and reports, and provides a limited, though significant, window for accepting upgrades.

Lync Online

If none of the factors in the preceding list are critical for you, you may want to choose Lync Online, for simpler deployment and manageability. Lync Online provides a robust IM, presence and conferencing feature set, and also enables voice and video calls over IP between users in your organization.

1.3.1.2 Beginning the Planning Process

Beginning the Planning Process

Microsoft Lync Server 2013 > Planning > Planning Primer: Planning for Your Organization >

Topic Last Modified: *2012-09-24*

While planning an on-premises unified communications deployment may seem intimidating, Lync Server provides two valuable tools to help you:

- **The Planning Tool** is a wizard that presents a series of questions about your organization, the Lync Server features that you want to enable, and your capacity planning needs. It then creates a recommended deployment topology based on your answers, and produces a Microsoft Visio diagram of this deployment.
- **Topology Builder** is an installation component of Lync Server. You use Topology Builder to create, adjust, and publish your planned topology. It also validates your topology before you begin server installations. When you install Lync Server on individual servers, the servers read the published topology as

part of the installation process, and the installation program deploys the server as directed in the topology.

Lync Server Planning Tool

The Planning Tool takes your answers to the questions in the tool and generates a topology based on Lync Server guidelines and best practices. It also provides several views of a deployment based on your answers. It shows both a global view of all your sites (that is, including both central sites and branch sites), and detailed views showing the servers and other components at each site.

Running the Planning Tool does not commit you to any specific deployment or initiate any processes. In fact, running the Planning Tool even before you have a firm plan in mind can be a very instructive way to understand the kinds of questions you need to think about in your planning process.

You can run the Planning Tool multiple times, answering questions differently, and compare the outcomes. If you have a design you are mostly satisfied with but that you need to make changes to, you can return to the Planning Tool, load the design, and make the changes. It takes about 15 minutes to complete the Planning Tool once.

After you are satisfied, you can use the Planning Tool to create a diagram of your planned deployment. You can use this diagram while creating the deployment in Topology Builder.

Note:

The Planning Tool included with this release of Lync Server 2013 is a prerelease version. Note that the capacity planning numbers in the Planning Tool are preliminary and are not supported for the final release.

Lync Server Topology Builder

Once you have decided on your deployment plan, you use Topology Builder to begin deploying. When finished, you use Topology Builder to validate the topology, and then, if it passes, you can publish the topology. When you publish the topology, Lync Server puts the topology into the Central Management store, which is created at this time if it does not already exist. When you install Lync Server on each server in your deployment, the server reads the topology from the Central Management store and installs itself to fit into its role in your deployment.

Alternatively, if you are very familiar with Lync Server and need less prescriptive guidance, you can skip the Planning Tool and use the wizards in Topology Builder for the initial design of your deployment and also for the validation and publishing steps.

Using Topology Builder to plan and publish a topology is a required step. You cannot bypass Topology Builder and install Lync Server individually on the servers in your deployment. Each server must read the topology from a validated, published topology in the Central Management store.

High-Level Planning Process

We recommend the following general process for using both the documentation and the Planning Tool to plan your Lync Server deployment.

1. If you are familiar with previous versions of Lync Server, read New Server Features to familiarize yourself with the new features and requirements in Lync Server 2013.
2. Read the other topics in this section of the documentation: Topology Basics You Must Know Before Planning, Reference Topologies, Initial Planning Decisions, and Clients for Lync Server 2013. Note the planning decisions

represented in Reference Topologies.

3. Now that you are more familiar with Lync Server features and the kinds of questions that must be answered, run the Planning Tool and view the resulting topology and its details. Make sure that the topology fits the unique requirements for your organization.
4. If there are particular workloads or features you are interested in or need to learn about, read the appropriate sections of Planning.
5. Run the Planning Tool again. You can start with the deployment you created in step 3 and modify the results, or start over from the beginning. If needed, run the Planning Tool a third time and repeat until you are satisfied with the output.
6. When you have finalized the topology plan, use Planning Tool to create and print a Visio diagram of your topology. You can use this printout while working with Topology Builder to input your topology.
7. Before you begin deployment, read Determining Your System Requirements and Determining Your Infrastructure Requirements to familiarize yourself with the prerequisites and necessary infrastructure for Lync Server. Additionally, be sure you have read all the sections of Planning that apply to the workloads and features that you plan to deploy.

Migrating from Previous Versions

If you are migrating to Lync Server from a previous version, see the Migration documentation for specific instructions for your migration and deployment.

1.3.1.3 Topology Basics You Must Know Before Planning

Topology Basics You Must Know Before Planning

Microsoft Lync Server 2013 > Planning > Planning Primer: Planning for Your Organization >

Topic Last Modified: *2012-09-25*

You do not have to be an expert on Lync Server to run the Planning Tool. In fact, running the Planning Tool multiple times, answering questions differently, and comparing the output is a good way to learn about Lync Server.

Before you learn about the various components in more depth, you should understand the following basic aspects of Lync Server 2013 topologies.

- Sites
- Server Roles
- High Availability and Disaster Recovery Support

1.3.1.3.1 Sites

Sites

Planning > Planning Primer: Planning for Your Organization > Topology Basics You Must Know Before Planning >

Topic Last Modified: *2012-10-16*

In Lync Server, you define *sites* on your network that contain Lync Server components. A site is a set of computers that is well-connected by a high-speed, low-latency network, such as a single local area network (LAN) or two networks connected by a high-speed fiber optic network. Note that Lync Server sites are a separate concept from Active

Directory Domain Services (AD DS) sites and Microsoft Exchange Server sites. Your Lync Server sites do not need to correspond to your Active Directory sites.

Site Types

Each site is either a *central site*, which contains at least one Front End pool or a Standard Edition server, or a *branch site*. Each branch site is associated with exactly one central site, and the users at the branch site get most of their Lync Server functionality from the servers at the associated central site.

Each branch site contains one of the following:

- A *Survivable Branch Appliance (SBA)*, which is an industry-standard blade server with a Lync Server Registrar and a Mediation Server running on Windows Server. The Survivable Branch Appliance also contains a public switched telephone network (PSTN) gateway. The Survivable Branch Appliance is designed for branch sites with between 25 and 1000 users.
- A *Survivable Branch Server (SBS)*, which is a server running Windows Server that meets specified hardware requirements, and that has Lync Server Registrar and Mediation Server software installed on it. It must connect to either a PSTN gateway or a SIP trunk to a telephone service provider. The Survivable Branch Server is designed for branch sites with between 1000 and 5000 users.
- A PSTN gateway, and, optionally, a *Mediation Server*. For details on this and other server roles, see Server Roles.

A branch office with a resilient wide area network (WAN) link to a central site can use the third option—a PSTN gateway, and, optionally, a Mediation Server. Branch office sites with less-resilient links should use a Survivable Branch Appliance or Survivable Branch Server, which provide resiliency in times of wide-area network failures. For example, in a site with a Survivable Branch Appliance or Survivable Branch Server deployed, users can still make and receive Enterprise Voice calls if the WAN connecting the branch site to the central site is down. For details about the Survivable Branch Appliance, Survivable Branch Server, and resiliency, see Planning for Enterprise Voice Resiliency in the Planning documentation.

Site Topologies

Your deployment must include at least one central site, and can include zero to many branch sites. Each branch site is affiliated with one central site. The central site provides the Lync Server services to the branch site that are not hosted locally at the branch site, such as presence and conferencing.

If you have multiple sites, you can pair together the Front End pools at different sites to enable disaster recovery abilities. For details, see High Availability and Disaster Recovery Support.

⊟See Also

Concepts

Server Roles
High Availability and Disaster Recovery Support

Other Resources

Planning for Enterprise Voice Resiliency

Server Roles

Planning > Planning Primer: Planning for Your Organization > Topology Basics You Must Know Before Planning >

Topic Last Modified: *2013-01-11*

Each server running Lync Server runs one or more *server roles*. A server role is a defined set of Lync Server functionalities provided by that server. You do not need to deploy all available server roles in your network. Install only the server roles that contain the functionality that you want.

Even if you are not familiar with server roles in Lync Server, the Planning Tool can guide you to the best solution for the servers that you need to deploy, based on the features that you want. This section provides a brief overview of the server roles and the general features that they provide:

- Standard Edition Server
- Front End Server and Back End Server
- Edge Server
- Mediation Server
- Director
- Persistent Chat Front End Server
- Persistent Chat Store (Persistent Chat Back End Server)
- Persistent Chat Compliance Store (Persistent Chat Compliance Back End Server)

For most server roles, for scalability and high availability you can deploy *pools* of multiple servers all running the same server role. Each server in a pool must run an identical server role or roles. For most types of pools in Lync Server, you must deploy a load balancer to spread traffic between the various servers in the pool. Lync Server supports both Domain Name System (DNS) load balancing and hardware load balancers.

Standard Edition Server

The Standard Edition server is designed for small organizations, and for pilot projects of large organizations. It enables many of the features of Lync Server, including the necessary databases, to run on a single server. This enables you to have Lync Server functionality for a lower cost, but does not provide a true high-availability solution.

Standard Edition server enables you to use instant messaging (IM), presence, conferencing, and Enterprise Voice, all running on one server.

For a high-availability solution, use Lync Server Enterprise Edition.

Front End Server and Back End Server

In Lync Server Enterprise Edition, the Front End Server is the core server role, and runs many basic Lync Server functions. The Front End Server, along with the Back End Servers, are the only server roles required to be in any Lync Server Enterprise Edition deployment.

A *Front End pool* is a set of Front End Servers, configured identically, that work together to provide services for a common group of users. A pool of multiple servers running the same role provides scalability and failover capability.

The Front End Server includes the following:

- User authentication and registration
- Presence information and contact card exchange
- Address book services and distribution list expansion
- IM functionality, including multiparty IM conferences
- Web conferencing, PSTN Dial-in conferencing and A/V conferencing (if deployed)
- Application hosting, for both applications included with Lync Server (for example, Conferencing Attendant and Response Group application), and third-party applications
- Optionally, Monitoring, to collect usage information in the form of call detail records (CDRs) and call error records (CERs). This information provides metrics about the quality of the media (audio and video) traversing your network for both Enterprise Voice calls and A/V conferences.
- Web components to supported web-based tasks such as web scheduler and join launcher.
- Optionally, Archiving, to archive IM communications and meeting content for compliance reasons. For details, see Planning for Archiving in the Planning documentation.
  In Lync Server 2010 and prior versions, Monitoring and Archiving were separate server roles, not collocated on Front End Server.
- Optionally, if Persistent chat is enabled, Persistent Chat Web Services for Chat Room Management and Persistent Chat Web Services for File Upload/Download.

Front End Pools are also the primary store for user and conference data. Information about each user is replicated among three Front End Servers in the pool, and backed up on the Back End Servers.

Additionally, one Front End pool in the deployment also runs the *Central Management Server*, which manages and deploys basic configuration data to all servers running Lync Server. The Central Management Server also provides Lync Server Management Shell and file transfer capabilities.

The Back End Servers are database servers running Microsoft SQL Server that provide the database services for the Front End pool. The Back End Servers serve as backup stores for the pool’s user and conference data, and are the primary stores for other databases such as the Response Group database. You can have a single Back End Server, but a solution that uses SQL Server mirroring is recommended for failover. Back End Servers do not run any Lync Server software.

Important:

We do not recommend collocating Lync Server databases with other databases. If you do so, availability and performance may be affected.

Information stored in the Back End Server databases includes presence information, users' Contacts lists, conferencing data, including persistent data about the state of all current conferences, and conference scheduling data.

Edge Server

Edge Server enables your users to communicate and collaborate with users outside the organization’s firewalls. These external users can include the organization’s own users who are currently working offsite, users from federated partner organizations, and outside users who have been invited to join conferences hosted on your Lync Server deployment. Edge Server also enables connectivity to public IM connectivity services, including Windows Live, AOL, Yahoo!, and Google Talk.

Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User

Subscription License (“PIC USL”) is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).

- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft’s ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

Deploying Edge Server also enables mobility services, which supports Lync functionality on mobile devices. Users can use supported Apple iOS, Android, Windows Phone, or Nokia mobile devices to perform activities such as sending and receiving instant messages, viewing contacts, and viewing presence. In addition, mobile devices support some Enterprise Voice features, such as click to join a conference, Call via Work, single number reach, voice mail, and missed calls. The mobility feature also supports *push notifications* for mobile devices that do not support applications running in the background. A push notification is a notification that is sent to a mobile device about an event that occurs while a mobile application is inactive.

Edge Servers also include a fully-integrated Extensible Messaging and Presence Protocol (XMPP) proxy, with an XMPP gateway included on Front End Servers. You can configure these XMPP components to enable your Lync Server 2013 users to add contacts from XMPP-based partners (such as Google Talk) for instant messaging and presence.

For details, see Planning for External User Access in the Planning documentation.

Mediation Server

Mediation Server is a necessary component for implementing Enterprise Voice and dial-in conferencing. Mediation Server translates signaling, and, in some configurations, media between your internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk. You can run Mediation Server collocated on the same server as Front End Server, or separated into a stand-alone Mediation Server pool.

For details, see Mediation Server Component in the Planning documentation.

Director

Directors can authenticate Lync Server user requests, but they do not home user accounts or provide presence or conferencing services. Directors are most useful to enhance security in deployments that enable external user access. The Director can authenticate requests before sending them on to internal servers. In the case of a denial-of-service attack, the attack ends with the Director and does not reach the Front End servers. For details, see Scenarios for the Director in the Planning documentation.

Persistent Chat Server Roles

Persistent chat enables users to participate in multiparty, topic-based conversations that persist over time. The Persistent Chat Front End Server runs the persistent chat service.

The Persistent Chat Back End Server stores the chat history data, and information about categories and chat rooms. The optional Persistent Chat Compliance Back End Server can store the chat content and compliance events for the purpose of compliance.

Servers running Lync Server Standard Edition can also run Persistent chat collocated on the same server. You cannot collocate the Persistent Chat Front End Server with Enterprise Edition Front End Server.

For details, see Planning for Persistent Chat Server.

⊟See Also

Concepts

Mediation Server Component

Other Resources

Planning for Archiving
Planning for External User Access
Scenarios for the Director
Planning for Persistent Chat Server

1.3.1.3.3 High Availability and Disaster Recovery Support

High Availability and Disaster Recovery Support

See Also

Planning > Planning Primer: Planning for Your Organization > Topology Basics You Must Know Before Planning >

Topic Last Modified: *2012-09-25*

Lync Server 2013 provides high availability by server redundancy via pooling. If a server running a certain server role fails, the other servers in the pool running the same role take the load of that server. This applies to Front End Servers, Edge Servers, Mediation Servers, and Directors. For details about server roles, see Server Roles.

Lync Server 2013 also provides disaster recovery measures by enabling pool pairing. If you deploy this topology, you will designate pairs of Front End pools, with each pool in a pair located in a separate data center, and in a separate geographical area. If one pool or site goes down, you can redirect the users of that pool to use the other pool in the pair, with minimal interruption of service.

Lync Server 2013 also supports Back End Server high availability. This is an optional topology in which you deploy two Back End Servers for a Front End pool, and set up synchronous SQL Server mirroring for all the Lync databases running on the Back End Servers.

For details about pool pairing and Back End Server mirroring, see Planning for High Availability and Disaster Recovery.

Concepts

Server Roles
Planning for High Availability and Disaster Recovery

1.3.1.4 Initial Planning Decisions

Initial Planning Decisions

Microsoft Lync Server 2013 > Planning > Planning Primer: Planning for Your Organization >

Topic Last Modified: *2012-10-01*

The first part of the planning process is deciding which Lync Server workloads and major features you want for your organization.

1. **Do you want an on-premises or online deployment?** Lync Server supports both deployment scenarios. For more information on making this decision, see Deciding How to Deploy Microsoft Lync, earlier in this section
2. **Do you want a physical or virtualized topology?** Lync Server supports all workloads and server roles in both physical and virtualized topologies. User capacity and scalability can differ between physical and virtual topologies. For more information, see Running Lync Server on Virtual Servers.
3. **Instant messaging *(IM)* and *presence* are always enabled.** In any Lync Server deployment, the instant messaging (IM) and presence workload is installed and enabled by default. IM enables your users to communicate with real-time text messages, and presence enables them to see the status of other users on the network. A user’s presence status provides information to help others decide whether they should try to contact the user, and by what means. For details, see Planning for Front End Servers, Instant Messaging, and Presence in the Planning documentation.
4. **Do you want to deploy any modes of conferencing?** Conferencing is another core feature of Lync Server. Several modes of conferencing are supported. You can choose to deploy all supported types of conferencing, or just some of them. *Web conferencing* enables users to see a file, such as a slide deck created with Microsoft PowerPoint presentation graphics program, that is being presented. *Application sharing* enables users to share all or part of their desktop with each other in real time. With *A/V conferencing*, users can add audio (and possibly video) to their conferences and peer-to-peer communications. *Dial-in conferencing* enables users to use standard PSTN phones to join the audio portion of conferences hosted at your organization. For details, see Planning for Conferencing in the Planning documentation.
   In Lync Server 2013, if you deploy Web conferencing, you must also plan for integration with Office Web Apps Server to enable Powerpoint sharing and viewing in meetings. For more information, see Configuring Integration with Office Web Apps Server and Lync Server 2013.
5. **If you deploy A/V conferencing, you should also monitor the audio quality of these conferences.** Many factors affect the audio and video quality of Lync Server A/V conferences. By using Monitoring, you can monitor the A/V quality of your calls and conferences. You can detect issues that affect media quality, and ensure that your users have the best possible media experience. For more information, see Planning for Monitoring.
6. **Do you want high availability for your IM, presence, and conferencing servers?** If you have only one server at a site providing IM, presence and conferencing features, your users’ productivity will be greatly affected if that server goes down. By deploying an Enterprise Edition *pool* of at least three servers for these functions, you make it possible for Lync Server to continue functioning with all of these features intact even if a server is unavailable. Another option for organizations with 5000 or fewer users who want high availability is to deploy two servers running Lync Server Standard Edition and pair these servers together. For more information, see Planning for High Availability and Disaster Recovery.
7. **Do you want disaster recovery options?** If you have two datacenters and want disaster recovery options to enable your users to continue to work if all or many servers at one datacenter go down, you can deploy your servers with disaster recovery in mind. For this deployment, you pair a pool of servers at one datacenter with a corresponding pool at another datacenter. If one

datacenter goes down, the other pool in the pair can service users in both pools with minimum interruption of services. For more information, see Planning for High Availability and Disaster Recovery.

8. **Do you want to enable your users to communicate and collaborate with external users?** Enabling communication and collaboration with external users can increase your return on investment in Lync Server. This enables your organization’s own users to benefit from Lync Server features even when they are working outside your organization’s firewalls. You can also federate with your partner or customer organizations that run Lync Server. By doing so, your users and federated partner users can easily send and receive IM messages, invite each other to meetings, and see each other’s presence. Additionally, your users can use an email message to invite specific outside users to conferences that they organize. For more information, see Planning for External User Access.
9. **Do you want to deploy Enterprise Voice?** *Enterprise Voice* is the voice over IP (VoIP) solution provided by Lync Server. It provides an attractive alternative to traditional PBX-based telephony. Enterprise Voice enables users to place calls from their computers or VoIP phones by clicking a contact in Outlook or Lync Server. They can place calls over the IP network from computer to computer, computer to telephone, or telephone to computer. Users benefit from having all of their communications options-voice, email, IM, and conferencing-available and integrated on their computers. For details, see Planning for Enterprise Voice in the Planning documentation.
10. **If you deploy Enterprise Voice, you should also monitor the audio quality of these calls.** We recommend you use Monitoring to ensure the audio quality of your Enterprise Voice calls, if you deploy Enterprise Voice. For more information, see Planning for Monitoring.
11. **Do you need to archive IM content or meeting content for compliance purposes?** If your organization has to archive IM content or meeting content for compliance purposes, you can deploy Archiving. For more information, see Planning for Archiving.
12. **Do you want to deploy Persistent chat?** If you want to enable your users to have real-time conversations that can persist over time, you can deploy Persistent chat. For more information, see Planning for Persistent Chat Server.
13. **Do you have Microsoft Exchange deployed?** If your organization uses Microsoft Exchange Server for its email services, you can enable several features which enhance the usefulness of both Lync Server and Microsoft Exchange Server. Some of these features, called Exchange Unified Messaging (UM), include enabling users to receive voice mail notices and listen to voice mail from Outlook or Outlook Web Access, to access their Microsoft Exchange mailboxes using a telephone, and to receive faxes in their Microsoft Exchange mailboxes. Additionally, if you have Exchange 2013 deployed, you can integrate the contact stores for users between the two systems, use Exchange to store higher-resolution contact photos, and integrate the archiving of emails and instant messages. For more information, see Planning for Exchange Server Integration.
14. **Do you have branch offices in your organization?** If your organization has branch offices, Lync Server supports a variety of ways to support them and ensure their resiliency for voice and other features. In particular, at a branch office that does not have a resilient WAN link to a data center, you can install a Survivable Branch Appliance or Survivable Branch Server to maintain Enterprise Voice support should the wide area network (WAN) link go down. For more information, see Planning for Branch-Site Voice Resiliency.

1.3.1.5 Clients for Lync Server 2013

Clients for Lync Server 2013

See Also

Microsoft Lync Server 2013 > Planning > Planning Primer: Planning for Your Organization >

Topic Last Modified: *2013-02-19*

Lync Server 2013 supports several types of client software that you can deploy to your organization's users, including computer-installed client software, web-based clients, and mobile devices. This topic outlines the clients that you can use. For a detailed comparison of the features provided by Lync Server 2013 clients, see Client Comparison Tables.

Lync 2013

Lync 2013 is the full-featured client for Lync Server. The Lync 2013 user interface has been fully redesigned and includes newly integrated features, such as Persistent Chat (Lync 2010 had a separate client for chat functionality), tabbed conversations, video preview, and multiparty video. For a summary of changes, see What's New for Clients.

Lync 2013 client setup is part of the Office setup program on the installation media.

Online Meeting Add-in for Lync 2013

The Online Meeting Add-in for Lync 2013 supports meeting management from within Microsoft Outlook messaging and collaboration client. The Online Meeting Add-in for Lync 2013 software installs automatically with Lync 2013.

Lync Web Scheduler

Lync Web Scheduler is a web-based meeting scheduling and management tool for users who don't have access to Microsoft Outlook, or who are on an operating system not based on Windows. With Lync Web Scheduler, users can create new meetings, modify existing meetings, and send invitations using their preferred email program.

Lync Web App

Lync Web App is the web-based conferencing client for Lync Server 2013 meetings. In this release, the addition of computer audio and video to Lync Web App provides a complete in-meeting experience for anyone who does not have a Lync client installed locally. Meeting participants have access to all collaboration and sharing features and presenter meeting controls.

If Lync 2013 is not installed on a user's computer and the user clicks a meeting link in a meeting request, Lync Web App opens. You can also configure the Meeting Join page to allow users to join meetings by using previous versions of clients; see Configuring the Meeting Join Page in the Deployment documentation.

Because of the enhancements to Lync Web App, an updated version of Microsoft Lync 2010 Attendee is not available for Lync Server 2013. Lync Web App is the client of choice for participants outside your organization. With Lync Web App, no local client installation is required, although audio, video, and sharing features require installation of a plug-in during first use.

Lync 2013 Basic

Lync 2013 Basic is a downloadable client for customers who have a licensed, on-premises Lync Server 2013 deployment and customers who subscribe to a Microsoft Office 365 plan that does not include the full Lync 2013 client. The Lync Basic client includes enhanced presence, contacts, instant messaging (IM), Lync meetings, and basic voice functionality. Features not supported in Lync Basic include multiparty video, OneNote integration, virtual desktop infrastructure (VDI) support, skill search, recording, Enterprise Voice features, and advanced call handling (for example, call forwarding and Team Call). For details, see Client Comparison Tables.

Lync Windows Store App

The Lync Windows Store app is a touch-optimized Lync app designed specifically for Windows 8 and Windows RT. Users can download the app through the Windows Store by searching for "Lync." For more information, see Client Comparison Tables, Lync Windows Store App Requirements, and Deploying Lync Windows Store App.

Lync 2013 for Mobile Devices

Lync 2013 mobile apps now include voice over IP (VoIP) and video over IP capabilities, in addition to contacts, presence, and IM features. Mobile users can choose to communicate with others through IM, voice calls, or video calls by using either Wi-Fi or their cellular data connection. With a single click of the meeting link in a calendar item, mobile users can join voice and video meetings. For more information about Lync 2013 mobile apps, see Planning for Mobile Clients.

Supported Clients from Previous Releases

Lync Server 2013 supports the following clients from previous server releases. You can make certain previous clients available to users when they join meetings. For details, see Configuring the Meeting Join Page in the Deployment documentation.

- **Lync 2010** Lync 2010 provides a full desktop experience, including IM, enhanced presence, voice, video, sharing, and telephony. However, none of the new features introduced in Lync Server 2013 will be available until the user’s client is upgraded to Lync 2013.
- **Lync 2010 Mobile** Lync Server 2013 supports all of the Microsoft Lync 2010 Mobile mobile apps. Microsoft Lync 2010 Mobile provides IM, enhanced presence, and telephony for users in your organization who are connecting from a smartphone or a phone running a Professional edition of Windows Mobile. You can instruct your users to install Microsoft Lync 2010 Mobile by directing them to the app marketplace for their mobile phone. For details, see “Planning for Mobile Clients” in the Lync Server 2010 documentation at http://go.microsoft.com/fwlink/p/?LinkID=235955.
- **Lync Phone Edition** Lync Phone Edition software for intelligent IP phones (for example, USB-attached phones) has not been updated for Lync Server 2013. Lync Phone Edition continues to be supported in for placing and receiving calls, enhanced presence, and client audio capabilities for conferences.
- **Lync 2010 Attendant** The Microsoft Lync 2010 Attendant integrated call-management program enables a receptionist to manage multiple conversations at the same time through rapid call handling, IM, and onscreen routing.

See Also

Concepts

Client Interoperability in Lync 2013

1.3.1.6 Reference Topologies

Reference Topologies

Microsoft Lync Server 2013 > Planning > Planning Primer: Planning for Your Organization >

Topic Last Modified: *2012-05-21*

The ideal Lync Server topology depends on your organization's size, the workloads you want to deploy, and your preferences for high availability versus cost of investment.

The following topics outline three reference topologies, including the reasoning behind many of the decisions that drive the requirements for each topology.

- Reference Topology For Small Organizations
- Reference Topology For Medium Organizations
- Reference Topology for Large Organizations With Multiple Data Centers

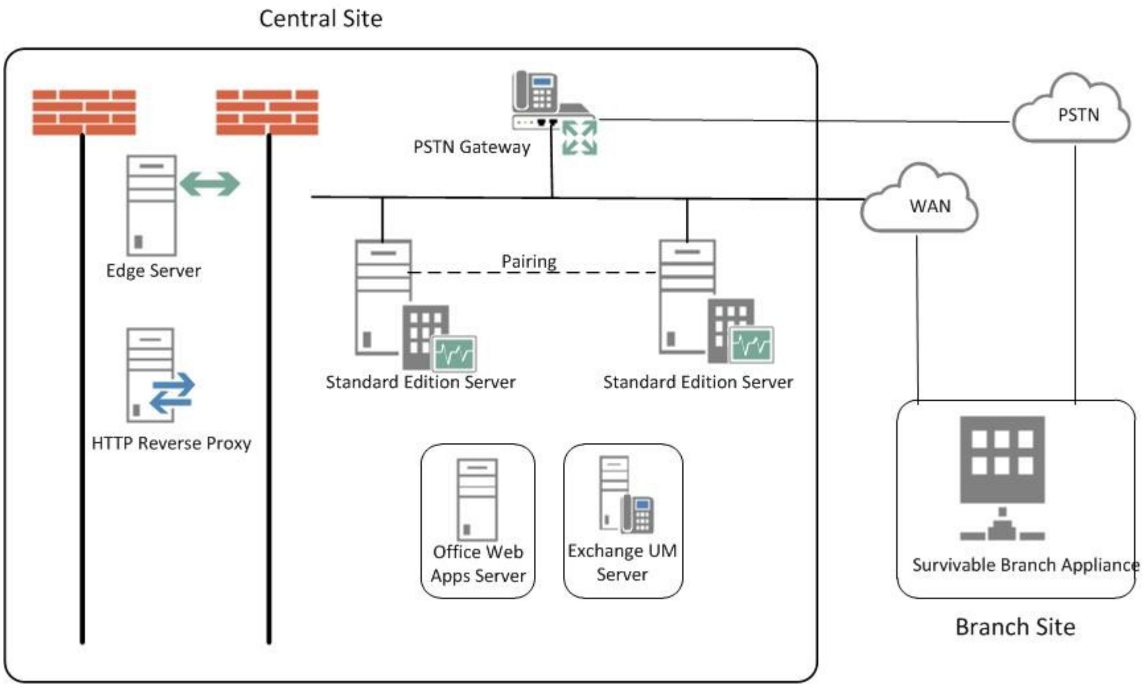
1.3.1.6.1 Reference Topology For Small Organizations

Reference Topology For Small Organizations

Planning > Planning Primer: Planning for Your Organization > Reference Topologies >

Topic Last Modified: *2013-03-12*

The reference topology for small organizations shows how you can deploy a robust, highly available solution by deploying only three servers running Lync Server.



- **Pair of Standard Edition Servers Deployed** This organization has 4,000 users at their central site. The organization has deployed two Standard Edition servers and paired them together to enable high availability and disaster recovery. Each server homes 2,000 users, but information about all users is synchronized between the two servers. If one goes down, an administrator can fail over those users to be served by the other server, with a minimum of disruption to users. For more information about high availability and disaster recovery features in Lync Server 2013, see Planning for High Availability and Disaster Recovery.

- **Edge Server deployment is recommended.** Although deploying an Edge Server is not required for internal IM, presence and conferencing, we recommend it even for small deployments. You can maximize your Lync Server investment by deploying an Edge Server to provide service to users currently outside your organization's firewalls. The benefits include the following:
  - Your organization's own users can use Lync Server functionality, if they are working from home or are out on the road.
  - Your users can invite outside users to participate in meetings.
  - If you have a partner, vendor or customer organization that also uses Lync Server, you can form a *federated relationship* with that organization. Your Lync Server deployment would then recognize users from that federated organization, leading to better collaboration.
  - Your users can exchange instant messages with users of public IM services, including any or all of the following: Windows Live, AOL, Yahoo!, and Google Talk. A separate license might be required for public IM connectivity with these services.

Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

- **Branch site survivability.** This organization is running a pilot program of the Enterprise Voice feature of Lync Server. Some users are using Lync Server as their sole voice solution. Some of these Voice pilot users are located at the branch site. The branch site does not have a reliable wide area network (WAN) link to the central site, so a Survivable Branch Appliance is deployed there. With this deployed, if the WAN link goes down, users at the branch site can still make and receive calls (both calls within the organization and PSTN calls), have voice mail functionality, and communicate with two-party instant messaging (IM). Users can also be authenticated when the WAN link is unavailable as well.
- **Exchange UM deployment.** This reference topology includes an Exchange Unified Messaging (UM) Server, which runs Microsoft Exchange Server, not Lync Server.
  For details about Exchange UM, see Planning for Exchange Unified Messaging

Integration and Hosted Exchange Unified Messaging Integration in the Planning documentation.
- **Office Web Apps Server.** We recommend deploying an Office Web Apps Server or Office Web Apps Server farm in every organization that uses web conferencing. Office Web Apps Server makes it possible for PowerPoint slides to be presented in web conferences. For more information, see Configuring Integration with Office Web Apps Server and Lync Server 2013.

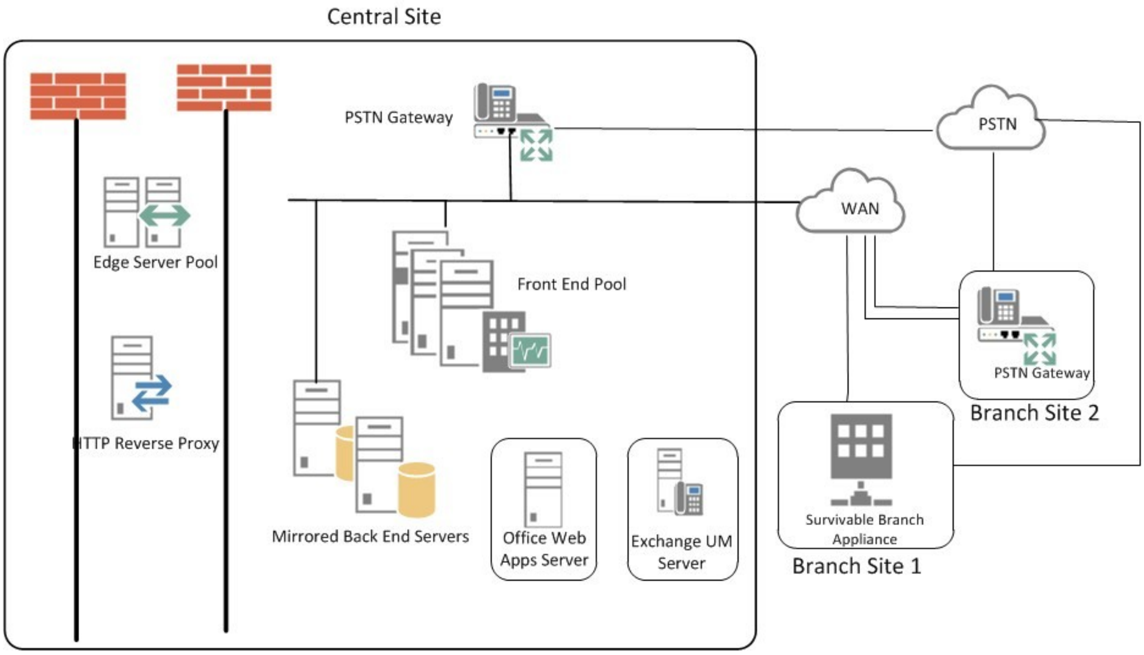
1.3.1.6.2 Reference Topology For Medium Organizations

Reference Topology For Medium Organizations

Planning > Planning Primer: Planning for Your Organization > Reference Topologies >

Topic Last Modified: *2013-01-11*

The reference topology with high availability and a single data center is designed for a small-to-medium size organization with one central site. The exact topology in the following diagram is for an organization of 20,000 users.



- **Accommodate more users by adding more Front End Servers.** The exact topology in this diagram has three Front End Servers to provide support for 20,000 users. If you have a single central site and more users, you can simply add more Front End Servers to the pool. The maximum number of users per pool is 80,000, with twelve Front End Servers.
However, the single site topology can support even more users by adding another Front End pool to the site.
- **Disaster Recovery could be added.** For this organization, high availability for their Lync Server services is a necessary feature, but disaster recovery is not. The pool of Front End Servers they have deployed provides high availability. If they wanted to add disaster recovery ability, they could consider establishing another datacenter and adding another Front End pool there, and pairing it with the Front End pool in their current datacenter. Then, if there was a disaster affecting their primary pool, the administrators could fail over users to the backup pool.

- **Back End Servers are mirrored** To provide more high availability for basic user features, the organization has deployed a mirrored pair of Back End Servers for each Front End pool. This is a new topology option for Lync Server 2013, and is optional. You could choose to deploy a single Back End Server instead.
- **Monitoring Server database options.** This organization has deployed Monitoring to ensure the quality of Enterprise Voice calls and A/V conferences. Monitoring is deployed on every Front End Server, and the Monitoring database is collocated with the Back End Servers. We also support topologies in which the Monitoring database is located on a separate server.
- **Edge Server high availability** In this example organization with 20,000 users, just one Edge Server would be sufficient for performance. However, there is a pool of two Edge Servers deployed to provide high availability.
- **Branch site deployment options.** The organization in this topology has Enterprise Voice deployed as their voice solution. Branch Site 1 does not have a resilient wide area network (WAN) link to the central site, so it has a Survivable Branch Appliance deployed to maintain many Lync Server features in case the WAN link to the central site goes down. Branch Site 2 however has a resilient WAN link, so only a public switched telephone network (PSTN) gateway is needed. The PSTN gateway deployed there supports media bypass, so no Mediation Server is needed at Branch Site 2. For details about deciding what to deploy at a branch site, see Planning for Branch-Site Voice Resiliency in the Planning documentation.
- **DNS load balancing.** The Front End pool andEdge Server pool, have DNS load balancing for SIP traffic deployed. This eliminates the need for hardware load balancers for the Edge Servers, and significantly lessens the setup and maintenance of the hardware load balancers for the other pools, as the hardware load balancers are needed only for HTTP traffic. For details about DNS load balancing, see DNS Load Balancing in the Planning documentation.
- **Exchange UM deployment.** This reference topology includes an Exchange Unified Messaging (UM) Server, which runs Microsoft Exchange Server, not Lync Server.
  For details about Exchange UM, see Planning for Exchange Unified Messaging Integration and Hosted Exchange Unified Messaging Integration in the Planning documentation.
- **Office Web Apps Server.** We recommend deploying an Office Web Apps Server or Office Web Apps Server farm in every organization that uses web conferencing. Office Web Apps Server makes it possible for Powerpoint slides to be presented in web conferences. For more information, see Configuring Integration with Office Web Apps Server and Lync Server 2013.
- **Edge Servers are recommended.** Although deploying an Edge Server is not required, we recommend it for any size of deployment. You can maximize your Lync Server investment by deploying an Edge Server to provide service to users currently outside your organization's firewalls. The benefits include the following:
  - Your organization's own users can use Lync Server functionality, if they are working from home or are out on the road.
  - Your users can invite outside users to participate in meetings.
  - If you have a partner, vendor or customer organization that also uses Lync Server, you can form a *federated relationship* with that organization. Your Lync Server deployment would then recognize users from that federated organization, leading to better collaboration.
  - Your users can exchange instant messages with users of public IM services, including any or all of the following: Windows Live, AOL, Yahoo!, and Google Talk. A separate license might be required for public IM connectivity with these services.

◆**Important:**
- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License

> ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
>
> - The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
> - More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

- **Directors could be added.** If this organization wanted to help to increase security against denial of service attacks, it could also deploy a pool of Directors. A Director is a separate, optional server role in Lync Server that does not home user accounts, or provide presence or conferencing services. It serves as an internal next hop server to which an Edge Server routes inbound SIP traffic destined for internal servers. The Director pre-authenticates inbound requests and redirects them to the user's home pool or server. Pre-authentication at the Director allows for dropping of requests from user accounts unknown to the deployment. A Director helps insulate Front End Servers from malicious traffic such as denial-of-service (DoS) attacks. If the network is flooded with invalid external traffic in such an attack, the traffic ends at the Director.
- **System Center Operations Manager is recommended.** We recommend that you monitor the health of your Lync Server deployment to help ensure service availability for end-users. You can monitor Lync with the System Center Operations Manager Management Pack for Lync that is available as a free download from Microsoft. With the Lync Management Pack, you can proactively get real-time alerts when issues occur, run synthetic transactions to test end-to-end Lync functionality, get reports for service availability, and so on. This helps you to proactively respond to issues with your deployment before end-users experience them.

1.3.1.6.3 Reference Topology for Large Organizations With Multiple Data Centers

Reference Topology for Large Organizations With Multiple Data Centers

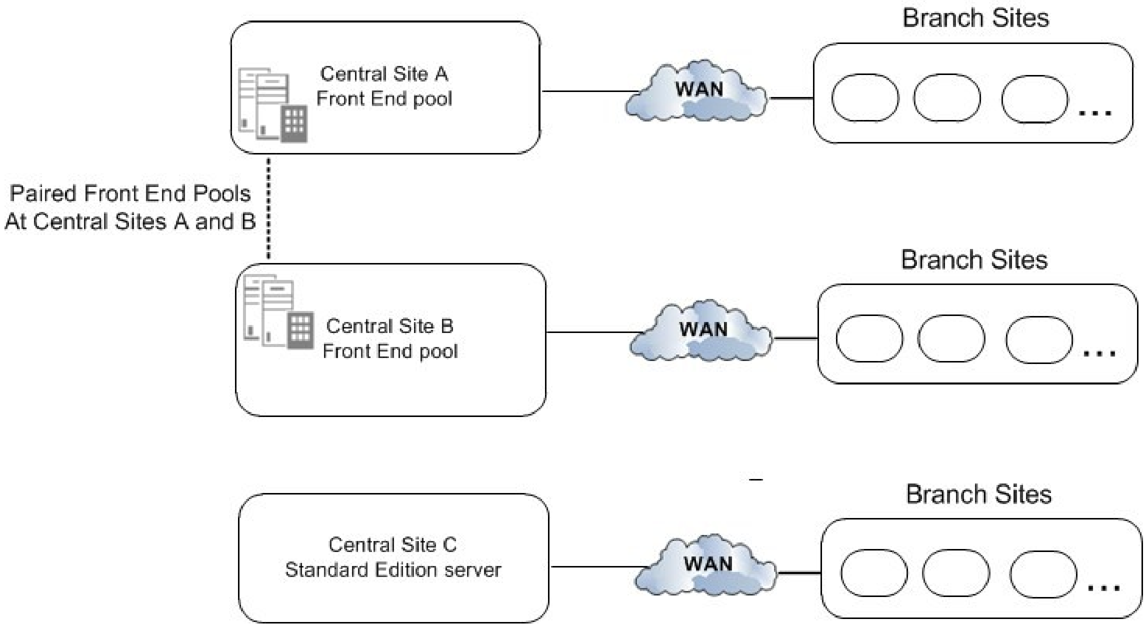
Planning > Planning Primer: Planning for Your Organization > Reference Topologies >

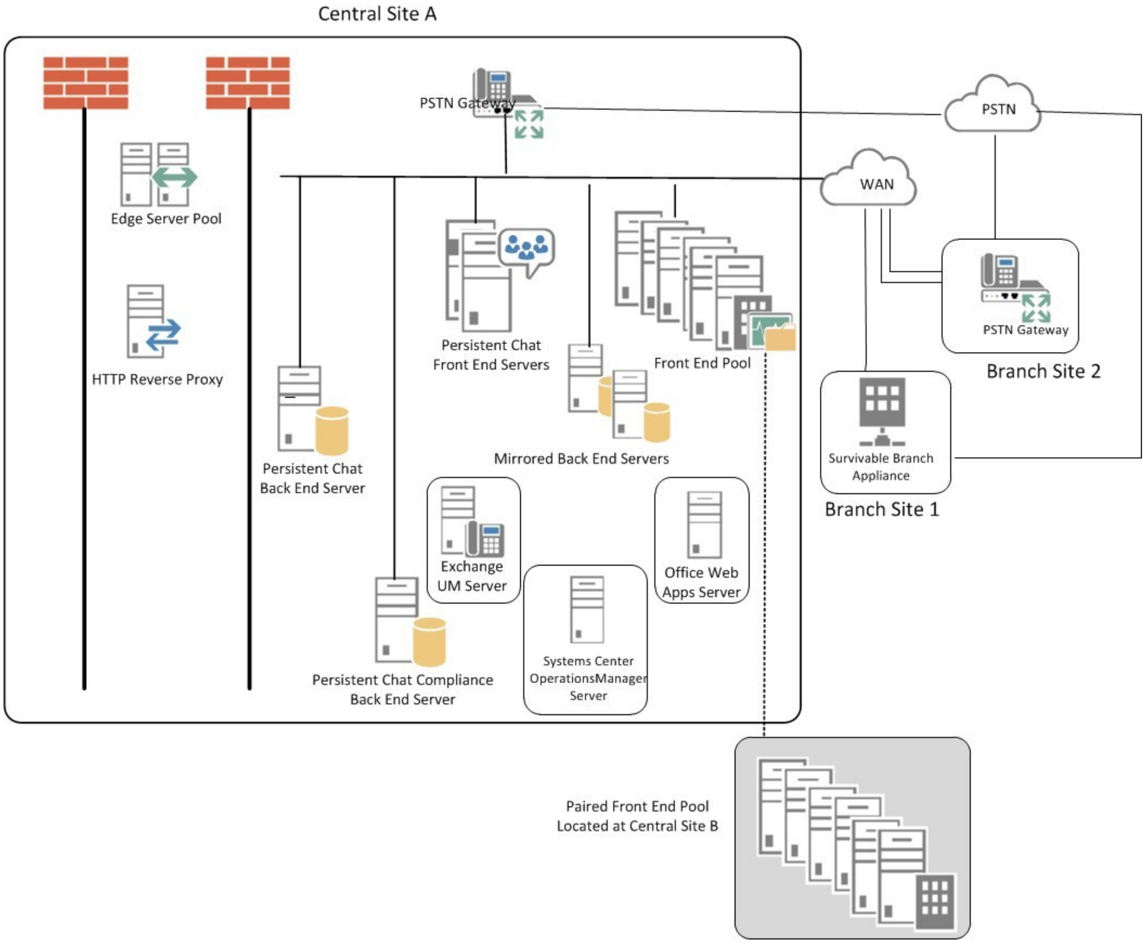
Topic Last Modified: *2012-10-22*

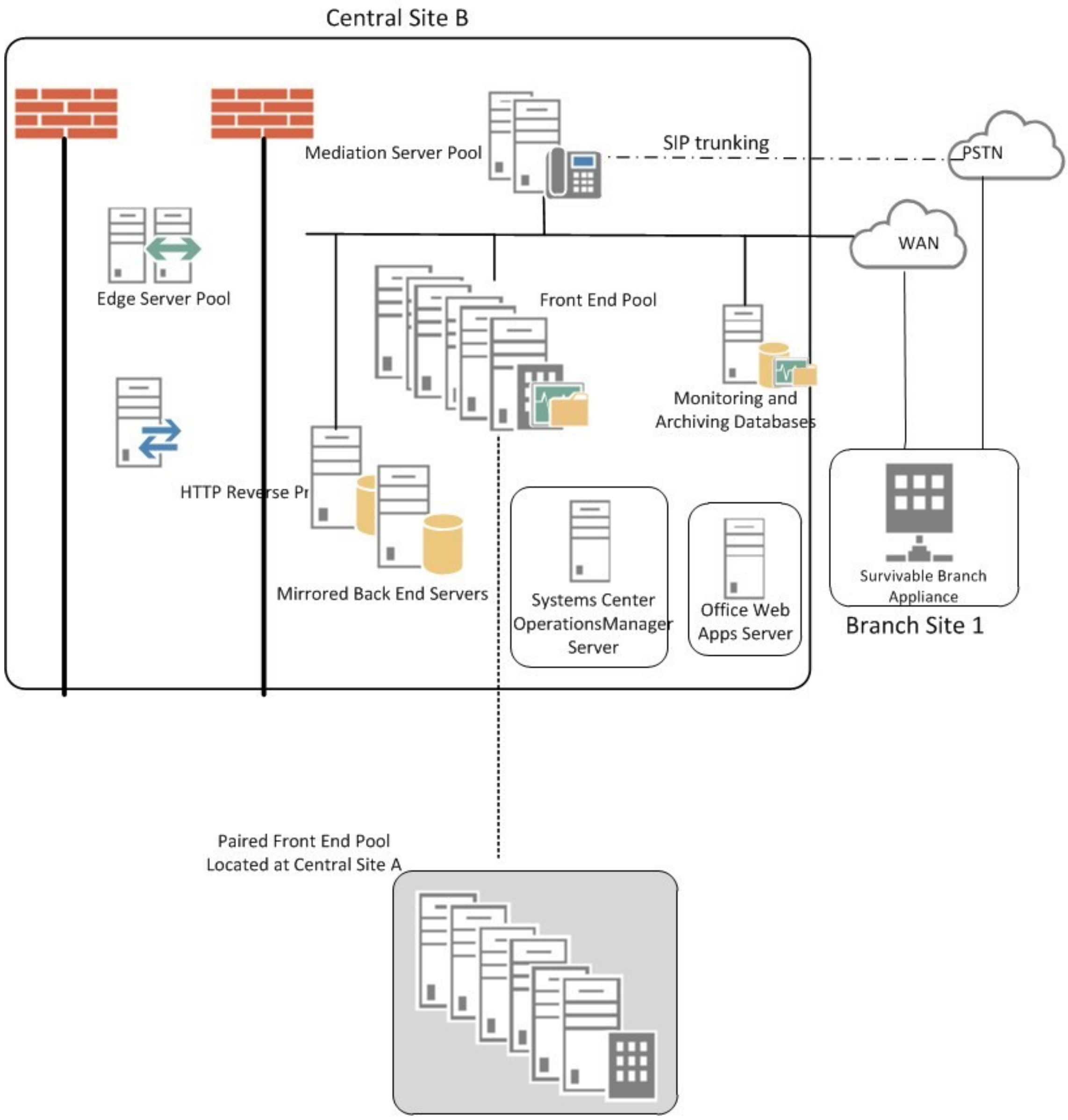
The reference topology for a large organization with multiple data centers support is for any size of organization with more than one central site. The exact topology in the following diagram is for an organization of 50,000 users, with 20,000 users at Central Site A, 20,000 at Central Site B. and a total of 10,000 at Central Site C and branch sites. The type of topology shown in this diagram can accommodate organizations with any number of users.

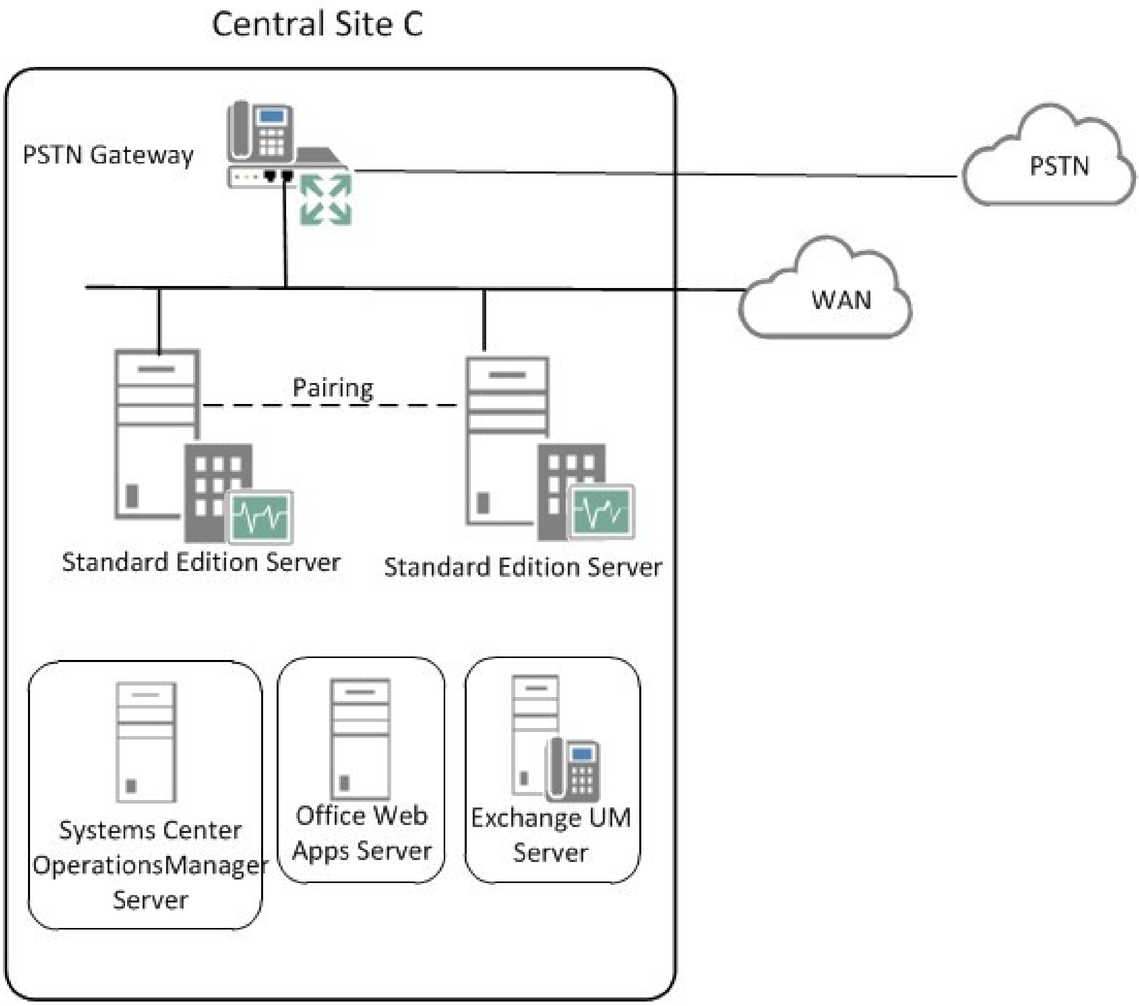
In addition to the high availability provided by pools of Front End Servers, this topology adds disaster recovery support. The Front End pools at Central Sites A and B are paired together. If one of these pools goes down, the administrator can shift the services for the affected users to the paired pool at the unaffected site.

This topology is shown in multiple diagrams, with an overview first followed by detailed views of the central sites.




Central Site A
PSTN Gateway
PSTN
WAN
Edge Server Pool
HTTP Reverse Proxy
Persistent Chat Front End Servers
Front End Pool
Persistent Chat Back End Server
Mirrored Back End Servers
Exchange UM Server
Office Web Apps Server
Systems Center OperationsManager Server
Persistent Chat Compliance Back End Server
PSTN Gateway
Branch Site 2
Survivable Branch Appliance
Branch Site 1
Paired Front End Pool Located at Central Site B


Central Site B
Mediation Server Pool
SIP trunking
PSTN
WAN
Edge Server Pool
Front End Pool
Monitoring and
Archiving Databases
HTTP Reverse Pr
Mirrored Back End Servers
Systems Center
OperationsManager
Server
Office Web
Apps Server
Survivable Branch
Appliance
Branch Site 1
Paired Front End Pool
Located at Central Site A



- **Front End pools Are Paired to Enable Disaster Recovery.** The Front End pools at Site A and Site B are paired with each other, to provide disaster recovery support. If the pool at one site fails, the administrator can fail over the users from that site to the paired Front End pool at the other site, with a minimum of service interruption for users. Each of these two Front End pools has six servers, which is enough for all 40,000 users in both pools in case of failover. For more information, see Planning for High Availability and Disaster Recovery.
- **Back End Servers are mirrored** To provide more high availability for basic user features, the organization has deployed a mirrored pair of Back End Servers for each Front End pool. This is an optional topology, and you could choose to deploy a single Back End Server instead.
- **Using Standard Edition server at a branch site.** This organization considers Site C as a branch site because it has only 600 employees. However, the users there have many A/V conferences among themselves. If it was deployed in Lync Server as a branch site, the media for these conferences would run across the wide area network (WAN) to and from a central site that has a Front End Server deployed. To avoid this potential bandwidth load, they have installed a pair of Standard Edition servers at this site, which will host these conferences. And because Standard Edition servers are installed there, Lync Server by definition considers it a central site, and it is treated as such in Topology Builder and the Planning Tool.
  Just one Standard Edition server would be enough for performance here, but

the organization has deployed two and paired them together to provide high availability in case one server goes down.
Although Site C is considered a central site, you do not have to deploy Edge Servers there. In this example, Site C will use the Edge Servers deployed at Site A.

- **Monitoring and Archiving** This organization has deployed both Monitoring and Archiving. When you deploy Monitoring or Archiving, it runs on every Front End Server. The databases for these features can be collocated with the Back End Database, or located on a separate server. This organization has located these databases on a server separate from the Back End Servers, in Central Site B. The databases here receive Monitoring and Archiving data from the Front End Servers in all sites.
- **Branch site deployment options.** This organization actually has over 50 branch sites, only three of which are shown in the detailed diagrams. Branch Sites 1 and 3 do not have a resilient WAN link to the central site, so they have Survivable Branch Appliances deployed to provide telephone service in case the WAN link to the central site goes down. Branch Site 2 however has a resilient WAN link, so you need only a public switched telephone network (PSTN) gateway. The PSTN gateway deployed there supports media bypass, so no Mediation Server is needed at Branch Site B. For details about deciding what to install at a branch site, see Planning for Enterprise Voice Resiliency in the Planning documentation.
- **SIP trunking and Mediation Server.** Notice that at Central Site B, Mediation Server is not collocated with the Front End Servers. This is because stand-alone Mediation Server is recommended for sites that use SIP trunking. In most other instances, we recommend you collocate Mediation Server with Front End Server. For details about Mediation Server topologies, see Components and Topologies for Mediation Server in the Planning documentation.
- **Persistent Chat is Deployed.** This organization has deployed the servers necessary to enable Persistent Chat. It has deployed multiple Persistent Chat Front End Servers to both handle the load for the number of users in the pool, and to provide high availability. It has also deployed Compliance for Persistent Chat, and located the Persistent Chat Store and the Persistent Chat Compliance Store on separate servers. These stores could be collocated, and can even be collocated with the Back End Server, but this organization has chosen to separate them to provide better performance.
- **DNS load balancing.** The Front End pool and Edge Server pool,. This eliminates the need for hardware load balancers for the internal interface of the Edge Servers, and significantly decreases the amount of time you have to spend on the setup and maintenance of the hardware load balancers for the other pools, as the hardware load balancers are needed only for HTTP traffic. For details about DNS load balancing, see DNS Load Balancing in the Planning documentation.
- **Exchange UM deployment.** Lync Server works with both *on-premises* deployments of Exchange Unified Messaging (UM) and *hosted* Exchange UM. Central Site A includes an Exchange Unified Messaging (UM) Server, which runs Microsoft Exchange Server, not Lync Server. The Exchange UM functionality for Lync Server runs on the Front End pool.
Central Site B uses hosted Exchange, so the Exchange UM Server functionality is also hosted.
For details about Exchange UM, see Planning for Exchange Unified Messaging Integration and Hosted Exchange Unified Messaging Integration in the Planning documentation.
- **Office Web Apps Server.** We recommend deploying an Office Web Apps Server or Office Web Apps Server farm in every organization that uses web conferencing. You could deploy a single Office Web Apps Server farm in one site which serves traffic from all sites, or deploy it in each site. Office Web Apps Server makes it possible for Powerpoint slides to be presented in web conferences. For more information, see Configuring Integration with Office

Web Apps Server and Lync Server 2013.

- **Directors could be added.** If this organization wanted to increase security against denial of service attacks, it could also deploy a pool of Directors. A Director is a separate, optional server role in Lync Server that does not home user accounts, or provide presence or conferencing services. It serves as an internal next hop server to which an Edge Server routes inbound SIP traffic destined for internal servers. The Director pre-authenticates inbound requests and redirects them to the user's home pool or server. Pre-authentication at the Director allows for dropping of requests from user accounts unknown to the deployment. A Director helps insulate Front End Servers from malicious traffic such as denial-of-service (DoS) attacks. If the network is flooded with invalid external traffic in such an attack, the traffic ends at the Director.
- **System Center Operations Manager is deployed.** We recommend that you monitor the health of your Lync Server deployment to ensure service availability for end-users. You can monitor Lync with the System Center Operations Manager Management Pack for Lync that is available as a free download from Microsoft. With the Lync Management Pack, you can proactively get real-time alerts when issues occur, run synthetic transactions to test end-to-end Lync functionality, get reports for service availability, and so on. This helps you to proactively respond to issues with your deployment before end-users experience them.
  This organization has deployed a System Center Operations Manager server in each central site.

1.3.2 Determining Your Infrastructure Requirements

Determining Your Infrastructure Requirements

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-10*

You need to identify and understand the infrastructure requirements for your deployment, so you can plan how to meet those requirements before you deploy Lync Server.

- Determining Your System Requirements
- Active Directory Infrastructure Requirements
- Certificate Infrastructure Requirements
- Internet Information Services (IIS) Requirements

1.3.2.1 Determining Your System Requirements

Determining Your System Requirements

See Also

Microsoft Lync Server 2013 > Planning > Determining Your Infrastructure Requirements >

Topic Last Modified: *2012-09-14*

All servers running Lync Server must meet certain minimum system requirements. System requirements for Lync Server include the server hardware, the operating system to be installed on each server, and related software requirements, such as the Windows updates and other software that must be installed on the servers.

◆**Important:**
Lync Server is available only in a 64-bit edition, which requires 64-bit hardware and a 64-bit edition of Windows Server. The exception is the Microsoft Lync Server 2013, Planning Tool, which is available in a 32-bit edition.

- Server Hardware Platforms
- Server and Tools Operating System Support
- Database Software Support
- Additional Software Requirements

⊟See Also

Other Resources

Client and Device Hardware Support
Supportability

1.3.2.1.1 Server Hardware Platforms

Server Hardware Platforms

Microsoft Lync Server 2013 > Supportability > Supported Hardware >

Topic Last Modified: *2013-01-07*

Lync Server 2013 server roles and computers running Lync Server administrative tools require 64-bit hardware.

The specific hardware used for Lync Server 2013 deployment can vary, depending on size and usage requirements. This section describes the recommended hardware. Although these are recommendations, not requirements, using hardware that does not meet these recommendations may result in significant performance issues and other issues.

Recommended Hardware Platform

For best performance, we recommend that you run Lync Server on servers with hardware that meets the requirements in the following table. If you use less powerful hardware, you may experience functionality problems or poor performance. Note that these hardware requirements are higher than those of previous versions of Lync Server, primarily because in Lync Server 2013, all Front End Servers run SQL Server.

Recommended Hardware for Front End Servers, Back End Servers, Standard Edition Servers, and Persistent Chat Store and Persistent Chat Compliance Store (Back End Server Roles for Persistent Chat Server)

Hardware component	Recommended
CPU	64-bit dual processor, hex-core, 2.26 gigahertz (GHz) or higher Intel Itanium processors are not supported for Lync Server server roles.
Memory	32 gigabytes (GB)
Disk	• 8 or more 10,000 RPM hard disk drives with at least 72 GB free disk space. Two of the disks should use RAID 1, and six should use RAID 10. - OR - • Solid state drives (SSDs) which provide performance similar to 8 10,000-RPM mechanical disk drives.
Network	• 1 dual-port network adapter, 1 Gbps or higher (2 recommended, which requires teaming with a single MAC address and

	single IP address)

Recommended Hardware for Edge Servers, Standalone Mediation Servers, and Directors

Hardware component	Recommended
CPU	• 64-bit dual processor, quad-core, 2.0 gigahertz (GHz) or higher - OR - • 64-bit 4-way processor, dual-core, 2.0 GHz or higher Intel Itanium processors are not supported for Lync Server server roles.
Memory	16 gigabytes (GB)
Disk	• 4 or more 10,000 RPM hard disk drives with at least 72 GB free disk space - OR - • Solid state drives (SSDs) which provide performance similar to 4 10,000-RPM mechanical disk drives.
Network	• 1 dual-port network adapter, 1 Gbps or higher (2 recommended, which requires teaming with a single MAC address and single IP address)

1.3.2.1.2 Server and Tools Operating System Support

Server and Tools Operating System Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-10-22*

All server roles support the same Windows Server operating systems. The required operating system support for other server roles, such as database servers, depends on what software you install on those servers.

Lync Server 2013 administrative tools are installed by default on the server running Lync Server 2013, but you can install administrative tools separately on other computers running Windows operating systems. For example, you can use a client computer running Windows 7 with Service Pack 1 (SP1) as an administrative console for planning purposes.

◆**Important:**
Lync Server 2013 is available only in 64-bit, which requires 64-bit hardware and 64-bit editions of Windows Server. This means that all server roles and computers running Lync Server 2013 administrative tools run a 64-bit edition operating system.

Operating Systems for Server Roles

Lync Server 2013 supports the 64-bit editions of the following operating systems:

- The Windows Server 2008 R2 with Service Pack 1 (SP1) Standard operating system (required) or latest service pack (recommended)
- The Windows Server 2008 R2 with SP1 Enterprise operating system (required) or latest service pack (recommended)

- The Windows Server 2008 R2 with SP1 Datacenter operating system (required) or latest service pack (recommended)
- The Windows Server 2012 Standard operating system
- The Windows Server 2012 Datacenter operating system

Lync Server 2013 is not supported on the following:

- The Server Core installation option of Windows Server 2008 R2 or Windows Server 2012
- The Windows Web Server 2008 R2 operating system or the Windows Web Server 2012 operating system
- Windows Server 2008 R2 HPC Edition or Windows Server 2012 HPC Edition

Operating Systems for Other Servers

Operating system support for servers other than those on which you deploy Lync Server 2013 server roles depends on the software that you plan to install on those servers. For details about requirements for Back End Servers and other database servers, see Database Software Support in the Supportability documentation. For details about requirements for reverse proxy servers (for Edge deployment), see Internet Information Services (IIS) Support in the Supportability documentation. For details about other software requirements, including infrastructure and virtualization support, see the other topics in the Server Software and Infrastructure Support section of the Supportability documentation.

Additional Operating Systems for Administrative Tools

Lync Server 2013 supports installation of the administrative tools, which includes the Topology Builder, on computers running any of the 64-bit editions of the operating systems supported for deployment of server roles (as described in the previous section). Additionally, you can install administrative tools on the 64-bit editions of the following operating systems:

- The Windows 7 operating system with SP1 operating system (required) or latest service pack (recommended)
- The Windows 8 operating or latest service pack (recommended)

1.3.2.1.3 Database Software Support

Database Software Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2013-03-12*

The following list contains the database management systems for the back-end database, the Archiving database, the Monitoring database, the Persistent Chat database, and the Persistent Chat compliance database that are supported by Lync Server 2013:

- **Back-end database of a Front End pool, Archiving database, Monitoring database, persistent chat database, and persistent chat compliance database**
  - Microsoft SQL Server 2008 R2 Enterprise database software (64-bit edition). Additionally running the latest service pack is recommended.
  - Microsoft SQL Server 2008 R2 Standard (64-bit edition). Additionally running the latest service pack is recommended.
  - Microsoft SQL Server 2012 Enterprise (64-bit edition). Additionally running the latest service pack is recommended.
  - Microsoft SQL Server 2012 Standard (64-bit edition). Additionally running the

latest service pack is recommended.

- **Standard Edition server database and local configuration store databases**
  - Microsoft SQL Server 2012 Express (64-bit edition)

Note:
Microsoft SQL Server 2012 Express (64-bit edition) is automatically installed by Lync Server 2013 on each Standard Edition server and each Lync Server 2013 server on which the local configuration store is deployed.

Important:

- Lync Server 2013 does not support the 32-bit edition of SQL Server. You must use the 64-bit edition.
- SQL Server Web edition and SQL Server Workgroup edition are not supported. You cannot use them with Lync Server 2013.
- Lync Server 2013 does support native database mirroring.
- To use the Monitoring Server role, you should install SQL Server Reporting Services.

In a Front End pool, the back-end database can be a single SQL Server computer.

Important:
If you collocate Lync Server databases with other databases, we highly recommend assessing all factors that might affect availability and performance, as well as ensuring that, if one node fails, the remaining node can handle the load. To verify failover capabilities, we recommend testing all failover scenarios.

SQL Clustering Topologies

SQL clustering topologies are not supported for new Lync Server 2013 deployments. For Back End Server high availability, SQL mirroring is the recommended and supported option.

If you are upgrading from a previous version of Lync Server and you have deployed an Enterprise Edition Front End pool that uses SQL clustering in that existing Lync Server topology, we recommend that you implement SQL Mirroring as a replacement for the existing SQL clustering deployment. However, continuing to use the existing SQL cluster with Lync Server 2013 is supported, but not recommended.

1.3.2.1.4 Additional Software Requirements

Additional Software Requirements

See Also

Planning > Determining Your Infrastructure Requirements > Determining Your System Requirements >

Topic Last Modified: *2012-12-08*

In addition to the hardware and operating system requirements for server platforms, Lync Server 2013 requires the installation of additional software on the servers that you deploy.

Note:
For details about the platform requirements for servers running Lync Server, see Server Hardware Platforms and Server and Tools Operating System Support. For details about system requirements for client computers and devices, see Planning for Clients and Devices in Lync Server 2013 in the Planning documentation. For details about software

requirements for administrative tools, see Administrative Tools Software Requirements.

Additional Software Necessary for All Internal Server Roles

On all internal server roles, you must also make sure that Windows PowerShell command-line interface 3.0 and Microsoft .NET Framework 4.5, are installed.

Important:

Edge Servers and Edge pools have different requirements from servers deployed on the internal network. The requirements for the Edge Servers and Edge pools are listed later in this topic under **Additional Software for Edge Servers**.

Additionally, Microsoft .NET Framework 4.5 is required on any computer where you will run the Lync Server administrative tools or Microsoft Lync Server 2013, Planning Tool.

Windows PowerShell 3.0

Each server running Lync Server 2013 must have the correct release of Windows PowerShell 3.0 installed. For details, see Installing Windows PowerShell 3.0.

Microsoft .NET Framework 4.5

Lync Server requires Microsoft .NET Framework 4.5. For Lync Server 2013, you must manually install the 64-bit edition of Microsoft .NET Framework 4.5 on the server prior to installing Lync Server 2013. To manually install it, download the Microsoft .NET 4.5 Framework from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?LinkId=268529

Installing Microsoft .NET Framework 4.5 on Servers Running Windows Server 2012

When you install Microsoft .NET Framework 4.5 on servers that will run Lync Server 2013 and Windows Server 2012, you must perform one additional step. After .NET Framework 4.5 is installed, use Server Manager to install HTTP Activation.

To Install .NET 4.5 HTTP Activation on Windows Server 2012

1. From the **Start** menu, click **Programs**, then click **Administrative Tools**, then click **Server Manager**.
2. In Server Manager, under **Features Summary**, choose **Add Features**.
3. Expand **.NET Framework 4.5**.
4. Select **WCF Activation** if it isn't already selected. Then select **HTTP Activation**.
5. Click **Next** and follow the prompts to finish the installation.

Windows Identity Foundation

Windows Identity Foundation in Lync Server 2013 requires the installation of Windows Identity Foundation in order to support server to server authentication scenarios. Windows Server 2008 R2 and Windows Server 2012 require different procedures to install the Windows Identify Foundation. Select your server operating system from the following list:

- Windows Server 2008 R2   For Windows Server 2008 R2, you check to see if it has already been installed on your computer. To do this, go to **Add/Remove Programs**, **View Installed Updates**, and look under **Windows** for the entry **Windows Identity Foundation (KB974405)**. For details about installing Windows Identity Foundation, see http://go.microsoft.com/fwlink/p/?linkId=204657.
- Windows Server 2012   For Windows Server 2012, you use **Server Manager** to install the Windows Identity Foundation. In the Server Manager **Add Roles and Features Wizard**, select **Features**. Select **Windows Identity Foundation**

3.5 from the list. Click **Next**, then click **Install**.

Additional Software for All Front End Servers and Standard Edition Servers

All Front End Servers and Standard Edition servers must also run Internet Information Services (IIS) with certain modules. Additionally, all Front End Servers and Standard Edition servers where conferencing, Call Park application, Announcement, or Response Groups are deployed must run Windows Media Format Runtime.

Internet Information Services (IIS)

Front End Servers and Standard Edition servers must run Internet Information Services (IIS), with the following modules:

- Static Content
- Default Document
- HTTP Errors
- ASP.NET
- .NET Extensibility
- Internet Server API (ISAPI) Extensions
- ISAPI Filters
- HTTP Logging
- Logging Tools
- Tracing
- Windows Authentication
- Request Filtering
- Static Content Compression
- Dynamic Content Compression
- IIS Management Console
- IIS Management Scripts and Tools
- Anonymous Authentication (this is installed by default when IIS is installed.)
- Client Certificate Mapping Authentication

Windows Desktop Experience

Windows Desktop Experience All Front End Servers and Standard Edition servers where conferencing will be deployed must have the Windows Media Format Runtime installed, which, except for Windows Server 2012 is installed as part of the Windows desktop experience. Windows Server 2012 requires Microsoft Media Foundation. The Windows Media Format Runtime is required to run the Windows Media Audio (.wma) files that the Call Park, Announcement, and Response Group applications play for announcements and music.

We recommend that you install Windows desktop experience before you install Lync Server 2013. If Lync Server 2013 does not find this software on the server, it will prompt you to install it, and then you must restart the server to complete installation.

Additional Software for Front End Servers and Standard Edition Servers Running on Windows Server 2012

Front End Servers require .NET 3.5, which is not installed by default on Windows Server 2012. To install it, put your Windows Server 2012 installation media in Drive D and type the following:

```
Add-WindowsFeature RSAT-ADDS, Web-Server, Web-Static-Content, Web-Default-Doc, We
```

For details about installing .NET 3.5 on servers running Windows Server 2012, see "Microsoft .NET Framework 3.5 Deployment Considerations" at http://go.microsoft.com/fwlink/p/?linkid=275032.

Additional Software for Directors

Directors must run Internet Information Services (IIS), with the following modules:

- Static Content
- Default Document
- HTTP Errors
- ASP.NET
- .NET Extensibility
- Internet Server API (ISAPI) Extensions
- ISAPI Filters
- HTTP Logging
- Logging Tools
- Tracing
- Windows Authentication
- Request Filtering
- Static Content Compression
- IIS Management Console
- IIS Management Scripts and Tools
- Anonymous Authentication (This is installed by default when IIS is installed.)
- Client Certificate Mapping Authentication

Additional Software for Persistent Chat Front End Servers

Persistent Chat Front End Servers must run Message Queuing (also known as MSMQ), which is a component of Windows Server.

Additional Software for Edge Servers

Edge Servers require the following software:

- Each server running Lync Server 2013 must have the correct release of Windows PowerShell 3.0 installed. For details, see Installing Windows PowerShell 3.0.
- Lync Server requires Microsoft .NET Framework 4.5. For Lync Server 2013 installed on Windows Server 2008 R2, you must manually install the 64-bit edition of Microsoft .NET Framework 4.5 on the server prior to installing Lync Server 2013. To manually install it, download the Microsoft .NET 4.5 Framework from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?LinkId=268529
- **Windows Identity Foundation** in Lync Server 2013 requires the installation of Windows Identity Foundation in order to support server to server authentication scenarios. Windows Server 2008 R2 and Windows Server 2012 require different procedures to install the Windows Identify Foundation. Select your server operating system from the following list:
  - Windows Server 2008 R2   For Windows Server 2008 R2, you check to see if it has already been installed on your computer. To do this, go to **Add/Remove Programs**, **View Installed Updates**, and look under **Windows** for the entry **Windows Identity Foundation (KB974405)**. For details about installing Windows Identity Foundation, see http://go.microsoft.com/fwlink/p/?linkId=204657.

- Windows Server 2012   For Windows Server 2012, you use **Server Manager** to install the Windows Identity Foundation. In the Server Manager **Add Roles and Features Wizard**, select **Features**. Select **Windows Identity Foundation 3.5** from the list. Click **Next**, then click **Install**.

Do Not Install Layered Socket Providers on Media Servers

Do not install any Microsoft Internet Security and Acceleration (ISA) Server client software, or any other Winsock Layered Service Providers (LSP) software, on any Front End Servers or stand-alone Mediation Servers. Installing this software could cause poor media traffic performance.

⊟See Also

Concepts

Administrative Tools Software Requirements

1.3.2.2 Active Directory Domain Services Requirements, Support, and Topologies

Active Directory Domain Services Requirements, Support, and Topologies

Microsoft Lync Server 2013 > Planning > Determining Your Infrastructure Requirements >

Topic Last Modified: *2012-10-05*

Prior to Lync Server 2010, Lync Server relied on Active Directory Domain Services (AD DS) to store all the global settings and groups necessary to deploy and manage Lync Server. Now much of this information is stored in the Central Management store instead of AD DS. However, user object schema extensions, including Lync Server 2013, Lync Server 2010, and Office Communications Server 2007 R2 schema extensions, are still stored in AD DS.

- Active Directory Domain Services Support
- Supported Active Directory Topologies
- Active Directory Infrastructure Requirements

1.3.2.2.1 Active Directory Domain Services Support

Active Directory Domain Services Support

Planning > Determining Your Infrastructure Requirements > Active Directory Domain Services Requirements, Support, and Topologies >

Topic Last Modified: *2012-12-04*

Lync Server 2013 uses the Central Management store to store configuration data for servers and services, instead of relying on Active Directory Domain Services (AD DS) for this information, as in the past. Lync Server 2013 still stores the following in AD DS:

- **Schema extensions**
  - User object extensions
  - Extensions for Lync Server 2010 and Office Communications Server 2007 R2 classes to maintain backward compatibility with previous supported versions
- **Data** (stored in Lync Server 2013 extended schema and in existing classes)
  - User SIP URI and other user settings
  - Contact objects for applications (for example, the Response Group

application and the Conferencing Attendant application)
- Data published for backward compatibility
- A service control point (SCP) for the Central Management store
- Kerberos Authentication Account (an optional computer object)

This section describes the AD DS support requirements for Lync Server 2013. For details about topology support, see Supported Active Directory Topologies in the Supportability documentation.

Supported Domain Controller Operating Systems

Lync Server 2013 supports domain controllers running the following operating systems:

- Windows Server 2012 operating system
- Windows Server 2008 R2 operating system
- Windows Server 2008 operating system
- Windows Server 2008 Enterprise 32-Bit
- The 32-bit or 64-bit versions of the Window Server 2003 R2 operating system
- The 32-bit or 64-bit versions of the Windows Server 2003 operating system

Forest and Domain Functional Level

You must raise all domains in which you deploy Lync Server 2013 to a domain functional level of Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or at least Windows Server 2003.

All forests in which you deploy Lync Server 2013 must be raised to a forest functional level of Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or at least Windows Server 2003.

Support for Read-Only Domain Controllers

Lync Server 2013 supports Active Directory Domain Services (AD DS) deployments that include read-only domain controllers or read-only global catalog servers, as long as there are writable domain controllers available.

Domain Names

Lync Server does not support single-labeled domains. For example, a forest with a root domain named **contoso.local** is supported, but a root domain named **local** is not supported. For details, see Microsoft Knowledge Base article 300684, "Information about configuring Windows for domains with single-label DNS names," at http://go.microsoft.com/fwlink/p/?linkId=143752.

Note:

Lync Server does not support renaming domains. If you need to rename a domain where Lync Server is deployed, you need to first uninstall Lync Server, then rename the domain, and then reinstall Lync Server.

Locked Down AD DS Environments

In a locked-down AD DS environment, Users and Computer objects are often placed in specific organizational units (OUs) with permissions inheritance disabled to help secure administrative delegation and to enable use of Group Policy objects (GPOs) to enforce security policies. Lync Server 2013 can be deployed in a locked-down Active Directory environment. For details about what is required to deploy Lync Server in a locked-down environment, see Preparing a Locked-Down Active Directory Domain Services in the Deployment documentation.

1.3.2.2.2 Supported Active Directory Topologies

Supported Active Directory Topologies

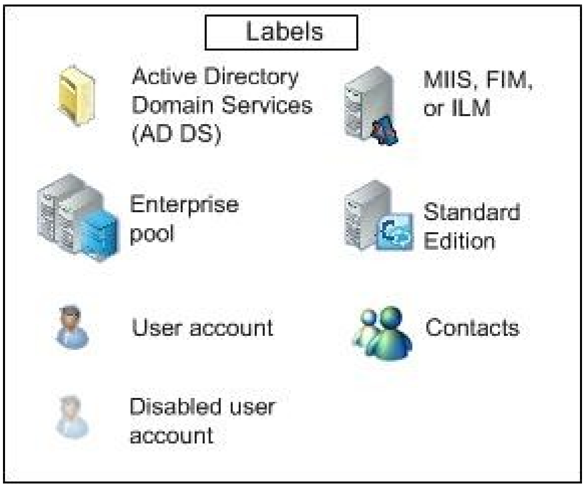
Planning > Determining Your Infrastructure Requirements > Active Directory Domain Services Requirements, Support, and Topologies >

Topic Last Modified: *2012-06-14*

Lync Server 2013 supports the same Active Directory Domain Services (AD DS) topologies as Microsoft Lync Server 2010 and Microsoft Office Communications Server 2007 R2. The following topologies are supported:

- Single forest with single domain
- Single forest with a single tree and multiple domains
- Single forest with multiple trees and disjoint namespaces
- Multiple forests in a central forest topology
- Multiple forests in a resource forest topology

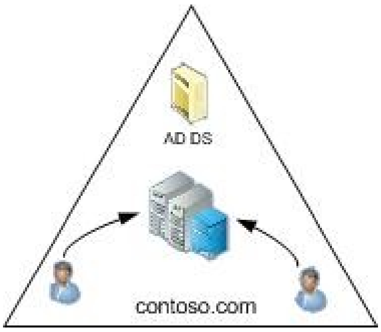
The following figure identifies the icons used in the illustrations in this section.



Single Forest, Single Domain

The simplest Active Directory topology supported by Lync Server, a single domain forest, is a common topology.

The following figure illustrates a Lync Server deployment in a single domain Active Directory topology.

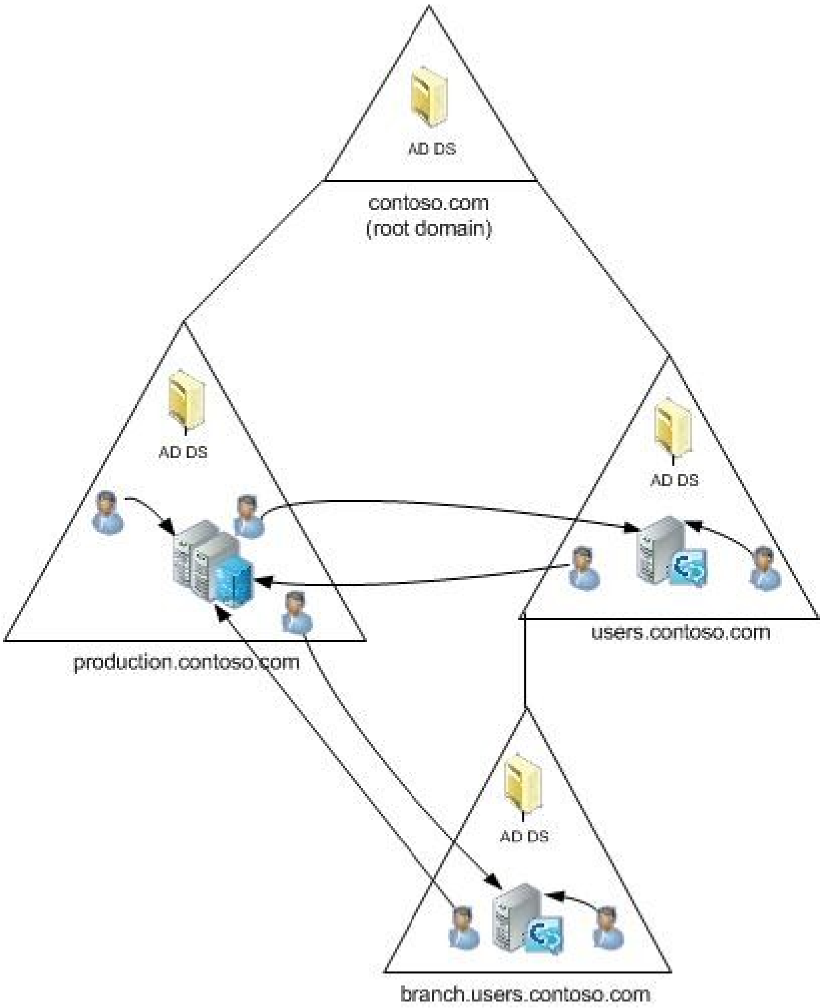


Single Forest, Multiple Domains

Another Active Directory topology supported by Lync Server is a single forest that consists of a root domain and one or more child domains. In this type of Active Directory topology, the domain where you create users can be different from the domain where you deploy Lync Server. However, if you deploy a Front End pool, you must deploy all the Front End Servers in the pool within a single domain. Lync Server support for Windows universal administrator groups enables cross-domain administration.

The following figure illustrates a deployment in a single forest with multiple domains. In this figure, a user icon shows the domain where the user account is homed, and the arrow points to the domain where the Lync Server pool resides. User accounts include the following:

- User accounts within the same domain as the Lync Server pool
- User accounts in a different domain from the Lync Server pool
- User accounts in a child domain of the domain with the Lync Server pool

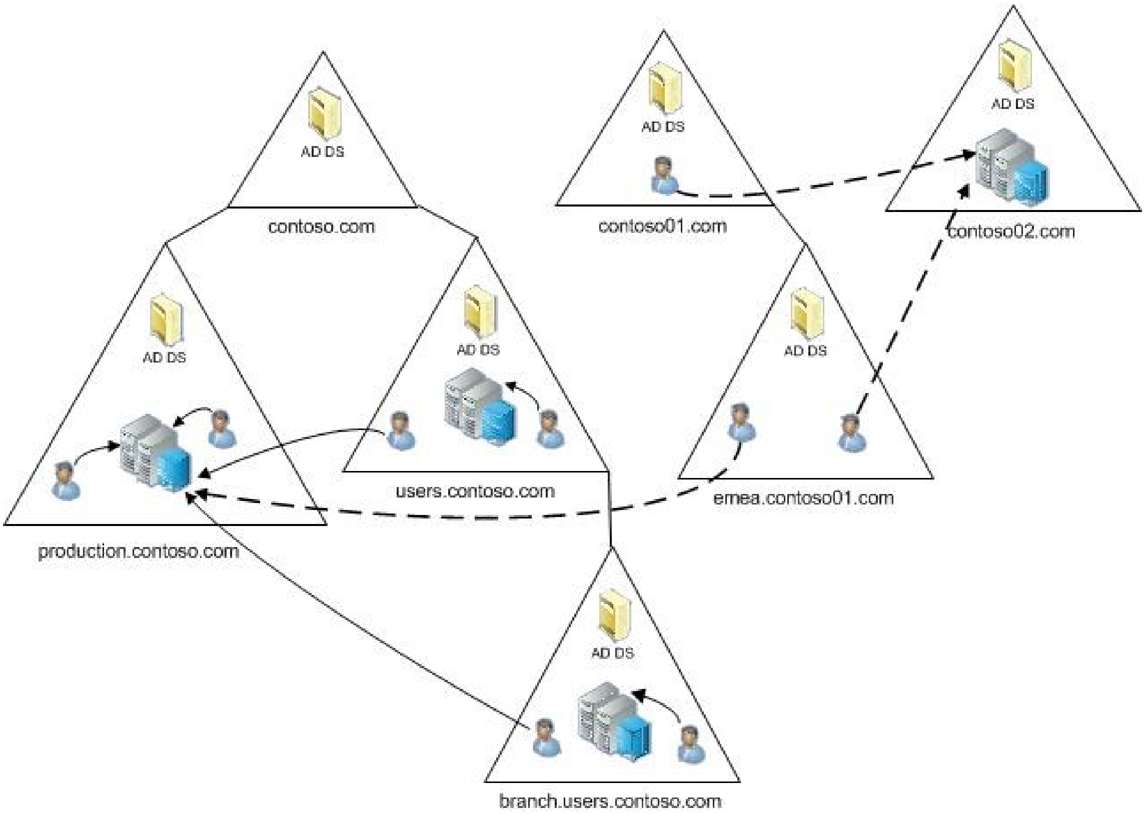


Single Forest, Multiple Trees

A multiple-tree forest topology consists of two or more domains that define independent tree structures and separate Active Directory namespaces.

The following figure illustrates a single forest with multiple trees. In this figure, a user icon shows the domain where the user account is homed, a solid line points to a Lync Server pool that resides in the same or a different domain, and a dashed line points to Lync Server pool that resides in a different tree. User accounts include the following:

- User accounts within the same domain as the Lync Server pool
- User accounts in a different domain from (but the same tree as) the Lync Server pool
- User accounts in a different tree from the Lync Server pool



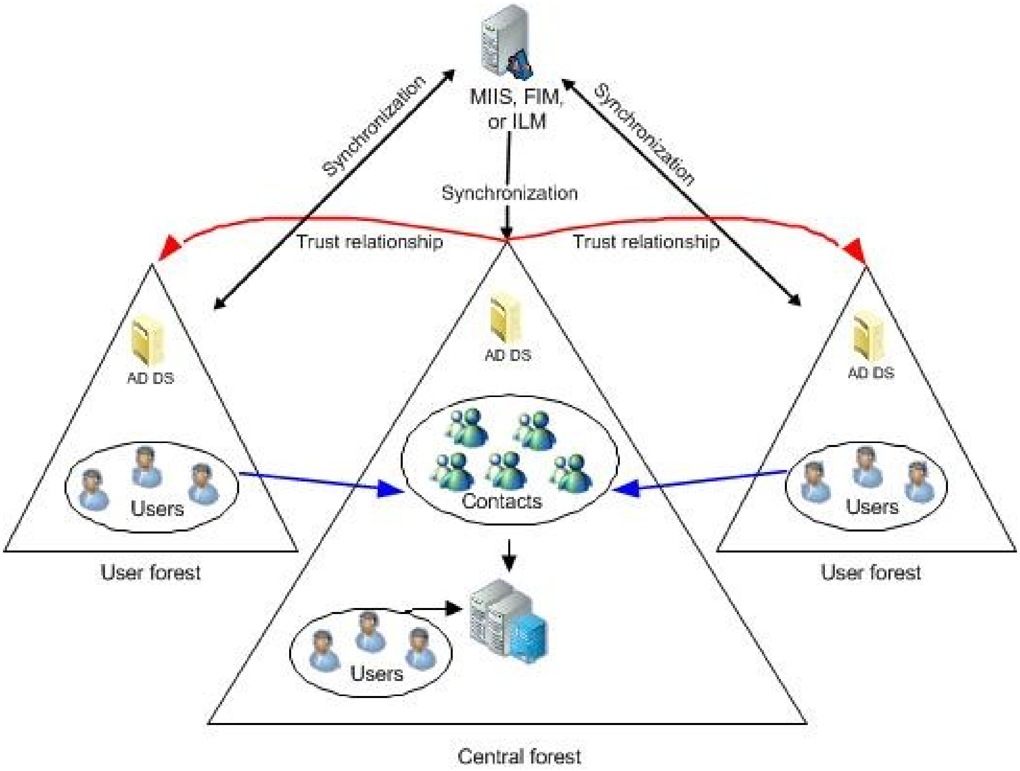
Multiple Forests, Central Forest

Lync Server supports multiple forests that are configured in a central forest topology. Central forest topologies use contact objects in the central forest to represent users in the other forests. The central forest also hosts user accounts for any users in this forest. A directory synchronization product, such as Microsoft Identity Integration Server (MIIS), Microsoft Forefront Identity Manager (FIM) 2010, or Microsoft Identity Lifecycle Manager (ILM) 2007 Feature Pack 1 (FP1), manages the life cycle of user accounts within the organization: When a new user account is created in one of the forests or a user account is deleted from a forest, the directory synchronization product synchronizes the corresponding contact in the central forest.

A central forest has the following advantages:

- Servers running Lync Server are centralized within a single forest.
- Users can search for and communicate with other users in any forest.
- Users can view presence of other users in any forest.
- The directory synchronization product automates the addition and deletion of contact objects in the central forest as user accounts are created or removed.

The following figure illustrates a central forest topology. In this figure, there are two-way trust relationships between the domain that hosts Lync Server, which is in the central forest, and each user-only domain, which is in a separate forest. The schema in the separate user forests does not need to be extended.



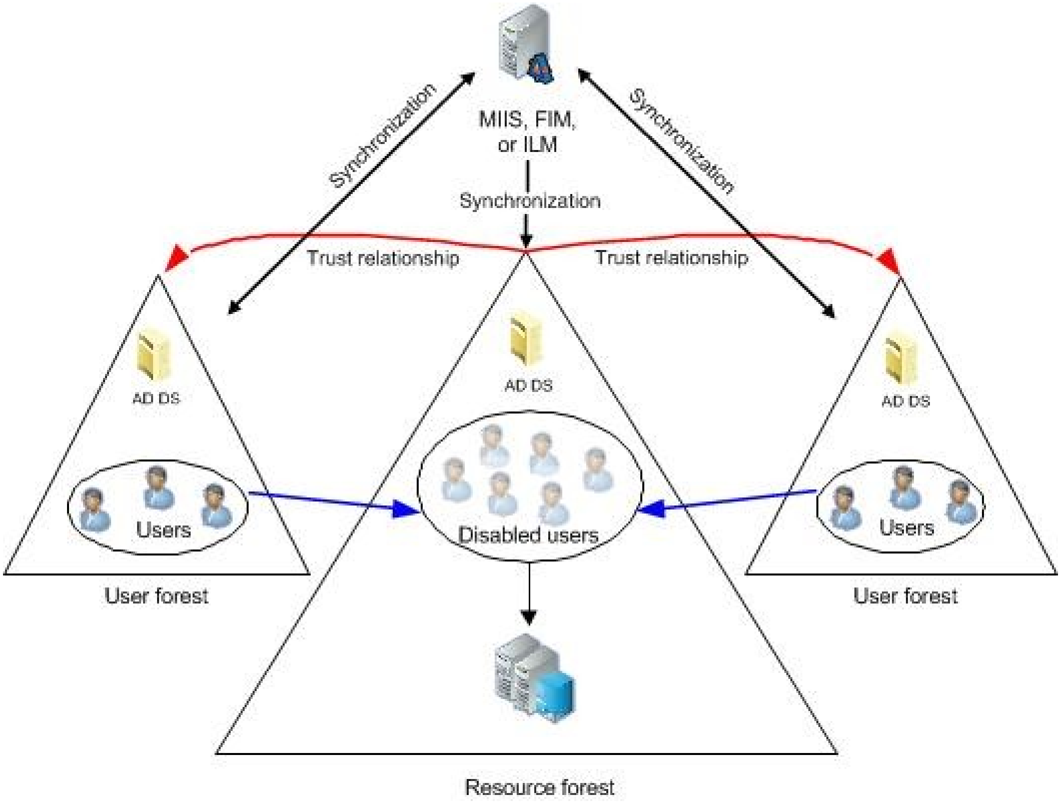
Multiple Forests, Resource Forest

In a resource forest topology, one forest is dedicated to running server applications, such as Microsoft Exchange Server and Lync Server. The resource forest hosts the server applications and a synchronized representation of the active user object, but it does not contain logon-enabled user accounts. The resource forest acts as a shared services environment for the other forests where user objects reside. The user forests have a forest-level trust relationship with the resource forest. When you deploy Lync Server in this type of topology, you create one disabled user object in the resource forest for every user account in the user forests. If Microsoft Exchange is already deployed in the resource forest, the disabled user accounts might already exist. A directory synchronization product, such as MIIS, Microsoft Forefront Identity Manager (FIM) 2010, or Microsoft Identity Lifecycle Manager (ILM) 2007 Feature Pack 1 (FP1), manages the life cycle of user accounts. When a new user account is created in one of the user forests or a user account is deleted from a forest, the directory synchronization product synchronizes the corresponding user representation in the resource forest.

This topology can be used to provide a shared infrastructure for services in organizations that manage multiple forests or to separate the administration of Active Directory objects from other administration. Companies that need to isolate Active Directory administration for security reasons often choose this topology.

This topology provides the benefit of limiting the need to extend the Active Directory schema to a single forest (that is, the resource forest).

The following diagram illustrates a resource forest topology.



1.3.2.2.3 Active Directory Infrastructure Requirements

Active Directory Infrastructure Requirements

[Planning](#) > [Determining Your Infrastructure Requirements](#) > [Active Directory Domain Services Requirements, Support, and Topologies](#) >

Topic Last Modified: *2012-11-27*

Before you start the process of preparing Active Directory Domain Services (AD DS) for Lync Server 2013, make sure that your Active Directory infrastructure meets the following prerequisites:

- All domain controllers (which include all global catalog servers) in the forest where you deploy Lync Server run one of the following operating systems:
  - Windows Server 2012 operating system
  - Windows Server 2008 R2 operating system
  - Windows Server 2008 operating system
  - Windows Server 2008 Enterprise 32-Bit
  - 32-bit or 64-bit versions of the Windows Server 2003 R2 operating system
  - 32-bit or 64-bit versions of the Windows Server 2003 operating system
- All domains in which you deploy Lync Server are raised to a domain functional level of Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or at least Windows Server 2003.
- The forest in which you deploy Lync Server is raised to a forest functional level of Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or at least Windows Server 2003.

Note:

To change your domain or forest functional level, see "Raising domain and forest functional levels" in the TechNet Library at http://go.microsoft.com/fwlink/p/?LinkId=263775.

- A global catalog is deployed in every domain where you deploy Lync Server computers or users.

Lync Server 2013 supports the universal groups in the Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003 operating systems. Members of universal groups can include other groups and accounts from any domain in the domain tree or forest and can be assigned permissions in any domain in the domain tree or forest. Universal group support, combined with administrator delegation, simplifies the management of a Lync Server deployment. For example, it is not necessary to add one domain to another to enable an administrator to manage both.

1.3.2.3 Certificate Infrastructure Requirements

Certificate Infrastructure Requirements

Microsoft Lync Server 2013 > Planning > Determining Your Infrastructure Requirements >

Topic Last Modified: *2013-01-11*

Lync Server 2013 requires a public key infrastructure (PKI) to support TLS and mutual TLS (MTLS) connections.

Lync Server uses certificates for the following purposes:

- TLS connections between client and server
- MTLS connections between servers
- Federation using automatic DNS discovery of partners
- Remote user access for instant messaging (IM)
- External user access to audio/video (A/V) sessions, application sharing, and conferencing
- Mobile requests using automatic discovery of Web Services

For Lync Server, the following common requirements apply:

- All server certificates must support server authorization (Server EKU).
- All server certificates must contain a CRL Distribution Point (CDP).
- All certificates must be signed using the RSA Sha1 signing algorithm

Important:
The RSA Sha1 signing algorithm is currently the only signing method recognized by Lync Server. Configuring your PKI to use a different signing algorithm may cause difficult to troubleshoot certificate failures in certificates on Lync Server role servers.

- Auto-enrollment is supported for internal servers running Lync Server.
- Auto-enrollment is not supported for Lync Server Edge Servers.
- When you submit a web-based certificate request to a Windows Server 2003 CA, you must submit it from a computer running either Windows Server 2003 with SP2 or Windows XP.
  Note that although KB922706 provides support for resolving issues with enrolling web certificates against a Windows Server 2003 Certificate Services web enrollment, it does not make it possible to use Windows Server 2008, Windows Vista, or Windows 7 to request a certificate from a Windows Server 2003 CA.
- Key lengths of 1024, 2048, and 4096 are supported. Key lengths of 2048 and greater are recommended.
- The default hash algorithm is RSA. The ECDH_P256, ECDH_P384, and

ECDH_P521 hash algorithms are also supported.

- Certificate Requirements for Internal Servers
- Certificate Requirements for External User Access
- Certificate Requirements for Persistent Chat Server
- Certificate Requirements for Mobility

1.3.2.3.1 Certificate Requirements for Internal Servers

Certificate Requirements for Internal Servers

See Also

Planning > Determining Your Infrastructure Requirements > Certificate Infrastructure Requirements >

Topic Last Modified: *2012-09-19*

Internal servers that are running Lync Server and that require certificates include Standard Edition server, Enterprise Edition Front End Server, Mediation Server, and Director. The following table shows the certificate requirements for these servers. You can use the Lync Server certificate wizard to request these certificates.

Tip:

Wildcard certificates are supported for the subject alternative names associated with the simple URLs on the Front End pool, Front End Server, or Director. For details about wildcard certificate support, see Wildcard Certificate Support.

Although an internal enterprise certification authority (CA) is recommended for internal servers, you can also use a public CA. For a list of public CAs that provide certificates that comply with specific requirements for unified communications (UC) certificates and have partnered with Microsoft to ensure they work with the Lync Server Certificate Wizard, see article Microsoft Knowledge Base 929395, "Unified Communications Certificate Partners for Exchange Server and for Communications Server," at http://go.microsoft.com/fwlink/p/?linkId=202834.

Communication with other applications and servers, such as Exchange 2013, requires a certificate that is supported by the other applications and products. For the 2013 release, Lync Server 2013 and other Microsoft server products, including Exchange 2013 and SharePoint Server, support the Open Authorization (OAuth) protocol for server-to-server authentication and authorization. For details, see Managing Server-to-Server Authentication (Oauth) and Partner Applications in the Deployment documentation or the Operations documentation.

For connections from clients running Windows 7 operating system, Windows Server 2008 operating system, Windows Server 2008 R2 operating system, Windows Vista operating system, and Microsoft Office Communicator 2007 Phone Edition, Lync Server 2013 includes support for (but does not require) certificates signed using the SHA-256 cryptographic hash function. To support external access using SHA-256, the external certificate is issued by a public CA using SHA-256.

The following tables show certificate requirements by server role for Front End pools and Standard Edition servers. All these are standard web server certificates, private key, non-exportable.

Note that server enhanced key usage (EKU) is automatically configured when you use the certificate wizard to request certificates.

Certificates for Standard Edition Server

Certificate	Subject	Subject alternative name	Example	Comments

	name/ Common name			
Default	Fully qualified domain name (FQDN) of the pool	FQDN of the pool and the FQDN of the server If you have multiple SIP domains and have enabled automatic client configuration, the certificate wizard detects and adds each supported SIP domain FQDNs. If this pool is the auto-logon server for clients and strict Domain Name System (DNS) matching is required in group policy, you also need entries for sip.sipdomain (for each SIP domain you have).	SN=se01.contoso.com; SAN=se01.contoso.com If this pool is the auto-logon server for clients and strict DNS matching is required in group policy, you also need SAN=sip.contoso.com; SAN=sip.fabrikam.com	On Standard Edition server, the server FQDN is the same as the pool FQDN. The wizard detects any SIP domains you specified during setup and automatically adds them to the subject alternative name. You can also use this certificate for Server-to-Server Authentication.

Web internal	FQDN of the server	Each of the following:
		• Internal web FQDN (which is the same as the FQDN of the server)
		• Meet simple URLs
		• Dial-in simple URL
		• Admin simple URL
		• Or, a wildcard entry for the simple URLs
			SN=se01.contoso.com; SAN=se01.contoso.com; SAN=meet.contoso.com; SAN=meet.fabrikam.com; SAN=dialin.contoso.com; SAN=admin.contoso.com
			Using a wildcard certificate:
			SN=se01.contoso.com; SAN=se01.contoso.com; SAN=*.contoso.com
				Internal web FQDN cannot be overwritten in Topology Builder.
				If you have multiple Meet simple URLs, you must include all of them as subject alternative names.
				Wildcard entries are supported for the simple URL entries.

Web external	FQDN of the server	Each of the following: • External web FQDN • Dial-in simple URL • Admin simple URL	SN=se01.contoso.com; SAN=webcon01.contoso.com ; SAN=meet.contoso.com;	If you have multiple Meet simple URLs, you must include all of them as subject

		- Or, a wildcard entry for the simple URLs	SAN=meet.fabrikam.com;
			SAN=dialin.contoso.com
			Using a wildcard certificate:
			SN=se01.contoso.com;
			SAN=webcon01.contoso.com;
			SAN=*.contoso.com
				alternative names.
				Wildcard entries are supported for the simple URL entries.

Certificates for Front End Server in a Front End Pool

Certificate	Subject name/ Common name	Subject alternative name	Example	Comments

Default	FQDN of the pool	FQDN of the pool and FQDN of the server.
		If you have multiple SIP domains and have enabled automatic client configuration, the certificate wizard detects and adds each supported SIP domain FQDNs.
		If this pool is the auto-logon server for clients and strict DNS matching is required in group policy, you also need entries for sip.sipdomain (for each SIP domain you have).
			SN=eepool.contoso.com;
			SAN=eepool.contoso.com;
			SAN=ee01.contoso.com
			If this pool is the auto-logon server for clients and strict DNS matching is required in group policy, you also need SAN=sip.contoso.com;
			SAN=sip.fabrikam.com
				The wizard detects any SIP domains you specified during setup and automatically adds them to the subject alternative name.
				You can also use this certificate for Server-to-Server Authentication.

Web Internal	FQDN of the server	Each of the following:
		- Internal web FQDN (which is the same as the FQDN of the server)
		- Meet simple URLs
		- Dial-in simple URL
		- Admin simple URL
		- Or, a wildcard entry for the simple URLs
			SN=ee01.contoso.com;
			SAN=ee01.contoso.com;
			SAN=meet.contoso.com;
			SAN=meet.fabrikam.com;
			SAN=dialin.contoso.com;
			SAN=admin.contoso.com
			Using a wildcard certificate:
				Internal web FQDN cannot be overwritten in Topology Builder.
				If you have multiple Meet simple URLs, you must include all of them as subject alternative names.

			SN=ee01.contoso.com;
			SAN=ee01.contoso.com;
			SAN=*.contoso.com
				Wildcard entries are supported for the simple URL entries.

Web external	FQDN of the server	Each of the following:
		• External web FQDN
		• Dial-in simple URL
		• Admin simple URL
		• Or, a wildcard entry for the simple URLs
			SN=ee01.contoso.com;
			SAN=webcon01.contoso.com;
			SAN=meet.contoso.com;
			SAN=meet.fabrikam.com;
			SAN=dialin.contoso.com
			Using a wildcard certificate:
			SN=ee01.contoso.com;
			SAN=webcon01.contoso.com;
			SAN=*.contoso.com
				If you have multiple Meet simple URLs, you must include all of them as subject alternative names.
				Wildcard entries are supported for the simple URL entries.

Certificates for Director

Certificate	Subject name/ Common name	Subject alternative name	Example

Default	FQDN of the Director pool	FQDN of the Director, FQDN of the Director pool
		If this pool is the auto-logon server for clients and strict DNS matching is required in group policy, you also need entries for sip.sipdomain (for each SIP domain you have).
			SN=dir-pool.contoso.com;
			SAN=dir-pool.contoso.com;
			SAN=dir01.contoso.com
			If this Director pool is the auto-logon server for clients and strict DNS matching is required in group policy, you also need SAN=sip.contoso.com;
			SAN=sip.fabrikam.com

Web Internal	FQDN of the server	Each of the following:
		• Internal web FQDN (which is the same as the FQDN of the
			SN=dir01.contoso.com;
			SAN=dir01.contoso.com;

		server)
		- Meet simple URLs
		- Dial-in simple URL
		- Admin simple URL
		- Or, a wildcard entry for the simple URLs
			SAN=meet.contoso.com;
			SAN=meet.fabrikam.com;
			SAN=dialin.contoso.com;
			SAN=admin.contoso.com
			
			SN=dir01.contoso.com;
			SAN=dir01.contoso.com
			SAN=*.contoso.com

Web external	FQDN of the server	Each of the following:
		- External web FQDN
		- Dial-in simple URL
		- Admin simple URL
		- Or, a wildcard entry for the simple URLs
			The Director external web FQDN must be different from the Front End pool or Front End Server.
			
			SN=dir01.contoso.com;
			SAN=directorwebcon01.contoso.com
			SAN=meet.contoso.com;
			SAN=meet.fabrikam.com;
			SAN=dialin.contoso.com
			
			SN=dir01.contoso.com;
			SAN=directorwebcon01.contoso.com
			SAN=*.contoso.com

If you have a stand-alone Mediation Server pool, the Mediation Servers in it each need the certificates listed in the following table. If you collocate Mediation Server with the Front End Servers, the certificates listed in the "Certificates for Front End Server in Front End Pool" table earlier in this topic are sufficient.

Certificates for Stand-alone Mediation Server

Certificate	Subject name/ Common name	Subject alternative name	Example

Default	FQDN of the pool	FQDN of the pool
		
		FQDN of pool member server
			SN=medsvr-pool.contoso.net;
			SAN=medsvr-pool.contoso.net;
			SAN=medsvr01.contoso.net

Certificates for Survivable Branch Appliance

Certificate	Subject name/	Subject alternative	Example

	Common name	name	

Default	FQDN of the appliance	SIP.<sipdomain> (need one entry per SIP domain)	SN=sba01.contoso.net;
			SAN=sip.contoso.com;
			SAN=sip.fabrikam.com

Concepts

Wildcard Certificate Support

1.3.2.3.2 Certificate Requirements for External User Access

Certificate Requirements for External User Access

See Also

Planning > Determining Your Infrastructure Requirements > Certificate Infrastructure Requirements >

Topic Last Modified: *2012-09-08*

Microsoft Lync Server 2013 communications software supports the use of a single public certificate for access and web conferencing Edge external interfaces, plus the A/V Authentication service. The Edge internal interface typically uses a private certificate issued by an internal certification authority (CA), but can also use a public certificate, provided that it is from a trusted public CA. The reverse proxy in your deployment uses a public certificate and encrypts the communication from the reverse proxy to clients and the reverse proxy to internal servers by using HTTP (that is, Transport Layer Security over HTTP).

Following are the requirements for the public certificate used for access and web conferencing Edge external interfaces, and the A/V authentication service:

- The certificate must be issued by an approved public CA that supports subject alternative name. For details, see Microsoft Knowledge Base article 929395, "Unified Communications Certificate Partners for Exchange Server and for Communications Server," at http://go.microsoft.com/fwlink/p/?linkId=202834.
- If the certificate will be used on an Edge pool, it must be created as exportable, with the same certificate used on each Edge Server in the Edge pool. The exportable private key requirement is for the purposes of the A/V Authentication service, which must use the same private key across all Edge Servers in the pool.
- If you want to maximize the uptime for your Audio/Video services, review the certificate requirements for implementing a decoupled A/V Edge service certificate (that is, a separate A/V Edge service certificate from the other External Edge certificate purposes). For details, see Changes in Lync Server 2013 That Affect Edge Server Planning, Plan for Edge Server Certificates and Staging AV and OAuth Certificates Using -Roll in Set-CsCertificate.
- The subject name of the certificate is the Access Edge service external interface fully qualified domain name (FQDN) or hardware load balancer VIP (for example, access.contoso.com).

  Note:

  For Lync Server 2013, this is no longer a requirement, but it is still recommended for compatibility with Office Communications Server.

- The subject alternative name list contains the FQDNs of the following:
  - The Access Edge service external interface or hardware load balancer VIP (for example, sip.contoso.com).

    Note:

Even though the certificate subject name is equal to the access Edge FQDN, the subject alternative name must also contain the access Edge FQDN because Transport Layer Security (TLS) ignores the subject name and uses the subject alternative name entries for validation.

- The web conferencing Edge external interface or hardware load balancer VIP (for example, webcon.contoso.com).
- If you are using client auto-configuration or federation, also include any SIP domain FQDNs used within your company (for example, sip.contoso.com, sip.fabrikam.com).
- The A/V Edge service does not use the subject name or the subject alternative names entries.

Note:

The order of the FQDNs in the subject alternative names list does not matter.

If you are deploying multiple, load-balanced Edge Servers at a site, the A/V authentication service certificate that is installed on each Edge Server must be from the same CA and must use the same private key. Note that the certificate's private key must be exportable, regardless of whether it is used on one Edge Server or many Edge Servers. It must also be exportable if you request the certificate from any computer other than the Edge Server. Because the A/V authentication service does not use the subject name or subject alternative name, you can reuse the access Edge certificate as long as the subject name and subject alternative name requirements are met for the access Edge and the web conferencing Edge and the certificate’s private key is exportable.

Requirements for the private (or public) certificate used for the Edge internal interface are as follows:

- The certificate can be issued by an internal CA or an approved public certificate CA.
- The subject name of the certificate is typically the Edge internal interface FQDN or hardware load balancer VIP (for example, lsedge.contoso.com). However, you can use a wildcard certificate on the Edge internal.
- No subject alternative name list is required.

The reverse proxy in your deployment services requests for:

- External user access to meeting content for meetings
- External user access to expand and display members of distribution groups
- External user access to downloadable files from the Address Book Service
- External user access to the Lync Web App client
- External user access to the Dial-in Conferencing Settings web page
- External user access to the Location Information Service
- External device access to the Device Update Service and obtain updates

The reverse proxy publishes the internal server Web Components URLs. The Web Components URLs are defined on the Director, Front End Server or Front End pool as the **External web services** in Topology Builder.

Wildcard entries are supported in the subject alternative name field of the certificate assigned to the reverse proxy. For details about how to configure the certificate request for the reverse proxy, see Request and Configure a Certificate for Your Reverse HTTP Proxy.

Concepts

Wildcard Certificate Support

1.3.2.3.3 Certificate Requirements for Persistent Chat Server

Certificate Requirements for Persistent Chat Server

Planning > Determining Your Infrastructure Requirements > Certificate Infrastructure Requirements >

Topic Last Modified: *2012-10-03*

To install Persistent Chat Server, you must have a certificate issued by the same CA as the one used by Lync Server 2013 internal servers for each server running the Persistent Chat Web Services for File Upload/Download. Make sure that you have the required certificate(s) before you start the Persistent Chat installation, especially if you are using an external CA.

1.3.2.3.4 Certificate Requirements for Mobility

Certificate Requirements for Mobility

Planning > Determining Your Infrastructure Requirements > Certificate Infrastructure Requirements >

Topic Last Modified: *2012-06-24*

If you deploy the mobility feature and support automatic discovery for mobile clients, you need to include certain subject alternative name entries on certificates to support secure connections from the mobile clients.

You need to include subject alternative name entries for automatic discovery on the following certificates:

- Director pool
- Front End pool
- Reverse proxy

This section describes the subject alternative name entries that are required on your certificates for automatic discovery.

Note:

Reissuing certificates by using an internal certificate authority is typically a simple process, but adding multiple subject alternative name entries to public certificates used by the reverse proxy can be expensive. If you have many SIP domains, making the addition of subject alternative names very expensive, you can configure the reverse proxy to use HTTP for the initial Autodiscover Service request, instead of using HTTPS (the default configuration). For details, see Technical Requirements for Mobility.

Director Pool Certificate Requirements

Description	Subject alternative name entry
Internal Autodiscover Service URL	SAN=lyncdiscoverinternal.<sipdomain>
External Autodiscover Service URL	SAN=lyncdiscover.<sipdomain>

Note:

Alternatively, you can use SAN=*.<sipdomain>

Front End Pool Certificate Requirements

Description	Subject alternative name entry

Internal Autodiscover Service URL	SAN=lyncdiscoverinternal.<sipdomain>
External Autodiscover Service URL	SAN=lyncdiscover.<sipdomain>

Note:

Alternatively, you can use SAN=*.<sipdomain>

Reverse Proxy (Public CA) Certificate Requirements

Description	Subject alternative name entry
External Autodiscover Service URL	SAN=lyncdiscover.<sipdomain>

Note:

You assign this SAN to the certificate assigned to the SSL Listener on the reverse proxy.

Note:

Your reverse proxy listener will have subject alternative names for your external Web Services URL(s) (for example, SAN=lyncwebextpool01.contoso.com, and dirwebexternal.contoso.com if you have deployed the optional Director).

1.3.2.4 Internet Information Services (IIS) Requirements

Internet Information Services (IIS) Requirements

Microsoft Lync Server 2013 > Planning > Determining Your Infrastructure Requirements >

Topic Last Modified: *2012-06-19*

Several Lync Server 2013 components require Internet Information Services (IIS). This topic describes the specific IIS features required to support Lync Server. The topics in this section describe the requirements of specific components for IIS.

When the Web Server (IIS) role is enabled on Windows Server 2008, various role services are installed by default. The following table describes the additional role services that must be installed when the Web Server (IIS) role is enabled on Windows Server 2008.

Role service	Feature
Common HTTP Features	HTTP Redirection
Application Development	ASP.NET
Application Development	.NET Extensibility
Application Development	ISAPI Extensions
Application Development	ISAPI Filters
Health and Diagnostics	Logging Tools
Health and Diagnostics	Tracing
Security	Basic Authentication
Security	Windows Authentication
Management Tools	IIS Management Scripts and Tools
Management Tools	IIS 6 Management Compatibility

Security Note:

If you are using IIS 7.0 on a Windows Server 2008 operating system, Lync Server Setup disables kernel mode authentication in IIS.

- IIS Requirements for Front End Pools and Standard Edition Servers

1.3.2.4.1 IIS Requirements for Front End Pools and Standard Edition Servers

IIS Requirements for Front End Pools and Standard Edition Servers

Planning > Determining Your Infrastructure Requirements > Internet Information Services (IIS) Requirements >

Topic Last Modified: *2012-06-19*

For Standard Edition servers and Front End Servers, and Directors, the Lync Server 2013 installer creates virtual directories in Internet Information Services (IIS) for the following purposes:

- To enable users to download files from the Address Book Service
- To enable clients to obtain updates
- To enable conferencing
- To enable users to download meeting content
- To enable users to expand distribution groups
- To enable phone conferencing
- To enable response group features

In addition, the cumulative update for Lync Server 2010: November 2011 installer creates virtual directories in IIS for the following purposes:

- On Front End Servers or Standard Edition servers to support mobility functionality, such as instant messaging (IM) and presence, on mobile devices
- On Front End Servers or Standard Edition servers and on Directors to enable mobile devices to automatically discover mobility resources

Note:

If you are deploying mobility, we recommend that you use IIS 7.5. The Lync Server Mobility Service installer sets some ASP.NET flags to improve performance. IIS 7.5 is installed by default on Windows Server 2008 R2, and the Mobility Service installer automatically changes the ASP.NET settings. If you use IIS 7.0 on Windows Server 2008, you need to manually change these settings.

Lync Server requires the following IIS modules to be installed:

Important:

If your organization requires that you locate IIS and all Web Services on a drive other than the system drive, you can change the installation location path for the Lync Server files in the Setup dialog box. If you install the Setup files to this path, including OCSCore.msi, the rest of the Lync Server files will be deployed to this drive as well. For details about how to relocate the INETPUB deployed by Windows Server Manager when installing IIS, see http://go.microsoft.com/fwlink/p/?linkId=216888.

- Static Content
- Default Document
- HTTP Errors
- ASP.NET
- .NET Extensibility
- Internet Server API (ISAPI) Extensions
- ISAPI Filters

- HTTP Logging
- Logging Tools
- Tracing
- Windows Authentication
- Request Filtering
- Static Content Compression
- Dynamic Content Compression
- IIS Management Console
- IIS Management Scripts and Tools
- Anonymous Authentication (installed by default when IIS is installed)
- Client Certificate Mapping Authentication

The following table lists the URIs for the virtual directories for internal access and the file system resources to which they refer.

Virtual Directories for Internal Access

Feature	**Virtual directory URI**	**Refers to**
Address Book Server	https://*<Internal FQDN>*/ABS/int/Handler	Location of Address Book Server download files for internal users.
Autodiscover Service	https://*<Internal FQDN>*/Autodiscover	Location of the Lync Server Autodiscover Service that locates mobility resources for internal mobile device users.
Client updates	http://*<Internal FQDN>*/AutoUpdate/Int	Location of update files for internal computer-based clients.
Conf	http://*<Internal FQDN>*/Conf/Int	Location of conferencing resources for internal users.
Device updates	http://*<Internal FQDN>*/DeviceUpdateFiles_Int	Location of unified communications (UC) device update files for internal UC devices.
Meeting	http://*<Internal FQDN>*/etc/place/null	Location of meeting content for internal users.
Mobility Service	https://*<Internal FQDN>*/Mcx	Location of Mobility Service resources for internal mobile device users.
Group Expansion and Address Book Web Query service	http://*<Internal FQDN>*/GroupExpansion/int/service.asmx	Location of the Web service that enables group expansion for internal users. Also, the location of the Address Book Web Query service that provides global address list information to internal Lync Mobile Microsoft Lync 2010 Mobile clients.
Phone Conferencing	http://*<Internal FQDN>*/PhoneConferencing/Int	Location of phone conferencing data for internal users.
Device updates	http://*<Internal FQDN>*/	Location of the Device

	RequestHandler	Update Web service Request Handler that enables internal UC devices to upload logs and check for updates.
Response Group application	http://*<Internal FQDN>*/RgsConfig http://*<Internal FQDN>*/RgsClients	Location of Response Group Configuration Tool.

Note:
For Front End pools in a consolidated configuration, you must deploy IIS before you can add servers to the pool.

Security Note:
You must use the IIS administrative snap-in to assign the certificate used by the IIS web component server.

1.3.3 Network Planning for Lync Server

Network Planning for Lync Server

See Also

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-10*

You can use the topics in this section to ensure that your network is ready for Lync Server.

- Network Infrastructure Requirements
- Planning for and Configuring IPv6
- Load Balancing Requirements
- Domain Name System (DNS) Requirements
- Port Requirements
- Network Bandwidth Requirements for Media Traffic
- Managing Quality of Service (QoS)

See Also

Other Resources

Determining Your Infrastructure Requirements

1.3.3.1 Network Infrastructure Requirements

Network Infrastructure Requirements

Microsoft Lync Server 2013 > Planning > Network Planning for Lync Server >

Topic Last Modified: *2012-10-18*

The network adapter card of each server in the Lync Server 2013 topology must support at least 1 gigabit per second (Gbps). In general, you should connect all server roles within the Lync Server topology using a low latency and high bandwidth local area network (LAN). The size of the LAN is dependent on the size of the topology:

- In Standard Edition topologies, servers should be in a network that supports 1

Gbps Ethernet or equivalent.
- In Front End pool topologies, most servers should be in a network that supports more than 1 Gbps, especially when supporting audio/video (A/V) conferencing and application sharing.

For public switched telephone network (PSTN) integration, you can integrate by using either T1/E1 lines or SIP trunking.

Audio/Video Network Requirements

Network requirements for audio/video (A/V) in a Lync Server deployment include the following:

- If you are deploying a single Edge Server or an Edge pool using DNS load balancing, you can configure the external firewall as a NAT. You cannot configure the internal firewall as a NAT. For details about these requirements, see Determine External A/V Firewall and Port Requirements in the Planning documentation.

Important:

If you have an Edge pool and are using a hardware load balancer, you must use public IP addresses on each of the Edge Servers and you cannot use NAT for the servers or the pool at your NAT device (for example, the firewall, or other infrastructure device that would NAT inbound or outbound traffic). For details, see Port Summary - Scaled Consolidated Edge with Hardware Load Balancers in the Planning for External User Access documentation.

- If your organization uses a Quality of Service (QoS) infrastructure, the media subsystem is designed to work within this existing infrastructure.
- If you use Internet Protocol security (IPsec), we recommend disabling IPsec over the port ranges used for A/V traffic. For details, see IPsec Exceptions in the Planning documentation.

To ensure optimal media quality, do the following:

- Provision your network links to support throughput of 65 kilobits per second (Kbps) per audio stream and 500 Kbps per video stream, if enabled, during peak usage periods. A bidirectional audio or video session consists of two streams.
- To cope with unexpected spikes in traffic above this level and increased usage over time, Lync Server media endpoints can adapt to varying network conditions and support loads of three times the throughput (see previous paragraph) for audio and video while still retaining acceptable quality. However, do not assume that this adaptability will support an under-provisioned network. In an under-provisioned network, the ability of the Lync Server media endpoints to dynamically deal with varying network conditions (for example, temporary high packet loss) is reduced.
- For network links where provisioning is extremely costly and difficult, you may need to consider provisioning for a lower volume of traffic. In this scenario, let the elasticity of the Lync Server media endpoints absorb the difference between the traffic volume and the peak traffic level, at the cost of some reduction in the voice quality. Also, there is a decrease in the headroom otherwise available to absorb sudden peaks in traffic.
- For links that cannot be correctly provisioned in the short term (for example, a site with very poor WAN links), consider disabling video for certain users.
- Provision your network to ensure a maximum end-to-end delay (latency) of 150 milliseconds (ms) under peak load. Latency is the one network impairment that Lync Server media components cannot reduce, and it is important to find and eliminate the weak points.
- For servers running antivirus software, include all servers running Lync Server in the exception list in order to provide optimal performance and audio quality.

Conferencing Network Requirements

The bandwidth that is used to download conference content from the Internet Information Services (IIS) server depends on the size of the content that is uploaded.

1.3.3.2 Planning for and Configuring IPv6

Planning for and Configuring IPv6

[Microsoft Lync Server 2013](#) > [Planning](#) > [Network Planning for Lync Server](#) >

Topic Last Modified: *2012-06-14*

Lync Server 2013 includes support for IP version 6 (IPv6) addresses, along with continued support of IP version 4 (IPv4) addresses. IPv4 addresses are 32-bit addresses that allow a computer to communicate over the Internet. Due to the increasing number of devices worldwide, the available IPv4 addresses have run out. Because of this, many new devices are moving to using IPv6 addresses. IPv6 addresses perform the same function as IPv4 addresses (with some additional features), but instead of using only 32-bits, IPv6 addresses use 128-bits. This provides not only a new set of addresses, but also a much larger number of them. A typical IPv4 address looks something like this: 192.0.2.235, whereas an IPv6 address looks like this: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. The change in formatting and functionality for devices that use IPv6 addresses requires several deployment and configuration considerations in your Lync Server 2013 installation.

In This Section

- [Overview of IP Address Types for Lync Server 2013](#)
- [Technical Requirements for IPv6](#)
- [Migration and Coexistence Considerations for IPv6](#)
- [Configure IP Address Types](#)

1.3.3.2.1 Overview of IP Address Types for Lync Server 2013

Overview of IP Address Types for Lync Server 2013

[Planning](#) > [Network Planning for Lync Server](#) > [Planning for and Configuring IPv6](#) >

Topic Last Modified: *2013-01-29*

You have three options when configuring IP addresses in Lync Server 2013. You can configure Lync Server 2013 to support only IP version 4 (IPv4), only IP version 6 (IPv6), or a combination of both (known as a *dual stack*). There are several issues to consider with each type of configuration:

- **IPv4 only** IPv6 was created because the world is running out of IPv4 addresses. Ultimately, IPv6 will be fully supported worldwide, but at this time, many companies and devices that your enterprise might need to communicate with do not yet support IPv6, and may not for some time. An IPv4-only configuration will help to ensure that your Lync Server implementation can communicate with most existing devices.
- **IPv6 only** Conversely, a full IPv6 implementation, at this time, will exclude communication with many existing devices.
- **Dual Stack** Dual stack is a network where both IPv4 and IPv6 addresses are

enabled. This configuration is supported in Lync Server 2013 because in most cases the transition from full-IPv4 to full-IPv6 will take several years.

The following sections outline the compatibility among these three configurations for various Lync Server features.

Note:

Client or server configuration with IPv6 only is supported only for lab or validation purposes. IPv6 only configuration is not supported in the production deployment.

Client Registration

Client endpoint network	Server network
IPv4	IPv4
IPv4	Dual stack
Dual stack	IPv4
Dual stack	Dual stack
Dual stack	IPv6
IPv6	Dual stack
IPv6	IPv6

Peer-to-Peer Client

Peer-to-peer communications include audio, audio/video, application sharing, and file transfer. After both clients have successfully registered, the following combinations are supported.

Client endpoint 1	Client endpoint 2
IPv4	IPv4
IPv4	Dual stack
Dual stack	Dual stack
IPv6	Dual stack
IPv6	IPv6

Conferencing

Conferencing includes audio/video, application sharing, and data collaboration (whiteboarding and file sharing).

Client endpoint network	Server network
IPv4	IPv4
IPv4	Dual stack
Dual stack	IPv4
Dual stack	Dual stack

Dual stack	IPv6
IPv6	Dual stack
IPv6	IPv6

Mediation Server/PSTN

Lync Server 2013 does not support media bypass for public switched telephone network (PSTN) calls if the traffic is through an IPv6 interface. If media bypass is required, we recommend that the PSTN gateway is configured to IPv4.

Primary interface*	PSTN interface (on Mediation Server)	PSTN gateway setting
IPv4	Dual stack	IPv4
Dual stack	Dual stack	IPv4
Dual stack	Dual stack	IPv6

* The primary interface is the interface that communicates with the Lync Server components.

Remote User Peer-to-Peer Communications

Peer-to-peer communications with remote users include instant messaging, audio/video, application sharing, and file transfer.

Remote user network	Edge server (External edge)
IPv4	IPv4
Dual stack	IPv4
Dual stack	Dual stack
IPv6	Dual stack
IPv6	IPv6

Front End Pool and Edge Pool Configuration

The following table shows the support matrix between the Front End Server pool and the internal Edge Server pool.

Front End Pool and Edge Pool (Internal Edge) Matrix

	Edge Pool: IPv4	Edge Pool: Dual Stack	Edge Pool: IPv6
Front End Pool: IPv4	Yes	Yes	No
Front End Pool: Dual Stack	Yes	Yes	No

Front End Pool: IPv6	No	No	Yes*

* Use this combination only in a lab environment.

The following table is a matrix of the supported combinations of internal and external edge interfaces.

Edge Pool (Internal Edge) and Edge pool (External Edge) Matrix

	Edge Pool (External Edge) : IPv4	**Edge Pool (External Edge): Dual Stack**	**Edge Pool (External Edge): IPv6**
Edge Pool (Internal Edge): IPv4	Yes	Yes	No
Edge Pool (Internal Edge): Dual Stack	No	Yes	No
Edge Pool (Internal Edge): IPv6	No	No	Yes*

* Use this combination only in a lab environment.

Advanced Enterprise Voice Support for IPv6

Deployments that include call admission control (CAC), Enhanced 9-1-1 (E9-1-1), or media bypass must be configured as IPv4 only or as a dual-stacked implementation.

Note:
In a dual-stacked deployment, even if a Lync client connects to a Lync Server by using IPv6, Lync will make a best effort to map an appropriate IPv4 address to support E9-1-1.

Location Information service with IPv6 addresses is not supported.

Exchange Unified Messaging (UM) does not support IPv6. For Exchange UM, be sure that DNS resolution does not return an IPv6 address. Using IPv6 may cause failure when calls are sent to voice mail.

Other Lync Server 2013 Feature Support for IPv6

In addition to the features and components mentioned previously, Lync Server 2013 supports IPv6 for the following features:

- **Persistent Chat**
  You configure IPv6 for Persistent Chat by using Topology Builder. For details about configuring Persistent Chat, see the Deploying Persistent Chat Server documentation.
- **Quality of Experience (QoE) and call detail recording (CDR) reports**
  Monitoring reports include the IP address as it is stored in the Monitoring Server database, whether of type IPv4 or IPv6.

1.3.3.2.2 Technical Requirements for IPv6

Technical Requirements for IPv6

See Also

Planning > Network Planning for Lync Server > Planning for and Configuring IPv6 >

Topic Last Modified: *2012-10-30*

If you plan to configure Lync Server 2013 for IPv6, keep the following requirements in mind:

- To use IPv6 addresses with Lync Server, you need to create domain name system (DNS) records for records that must be discovered and resolved to an IPv6 address. IPv6 DNS uses host AAAA (quad-A) records. If you use both IPv4 and IPv6 in your deployment, it is best to configure and maintain both host A records for IPv4 and host AAAA records for IPv6. Even when you fully transition your deployment to IPv6, you may still require IPv4 DNS host records for external users who still use IPv4.
  You can deploy IPv6 DNS host records before you start using IPv6. If the client or server doesn't use IPv6, the record will not be referenced. Transitional technologies will make the decision about which record to use, based on transition technology configuration and policies.
- Each IPv6 address has a scope. The three scopes that you can use for IPv6 addressing are IPv6 global addresses (similar to public IPv4 addresses), IPv6 unique local addresses (similar to the private IPv4 address ranges), and IPv6 link-local addresses (similar to automatic private IP addresses in Windows Server for IPv4). All the servers within a pool should have IPv6 addresses with the same scope.

◆**Important:**
IPv6 is a complex topic and requires careful planning with your networking team and your Internet provider to help ensure that the addresses that you assign at the Windows Server level and at the Lync Server 2013 level work as expected. See the links at the end of this topic for additional resources on IPv6 addressing and planning.

Other Resources

IP Version 6 Addressing Architecture
IPv6 Global Unicast Address Format
Unique Local IPv6 Unicast Addresses

1.3.3.2.3 Migration and Coexistence Considerations for IPv6

Migration and Coexistence Considerations for IPv6

Planning > Network Planning for Lync Server > Planning for and Configuring IPv6 >

Topic Last Modified: *2012-06-14*

IP version 6 (IPv6) is not supported on Lync Server 2010 or Office Communications Server. For piloting purposes, you can test Lync Server 2010 and Lync Server 2013 dual-stack coexistence. We recommend that all pools for a given central site are upgraded to Lync Server 2013 before you enable IPv6 (dual-stack network) for any of the pools. If you need to configure a pool for IPv6 only, we recommend that you set up an IPv6-only pool in your lab environment for testing.

The following scenarios are supported during migration and coexistence:

- Lync Server 2013, Lync Server 2010, and Office Communications Server 2007 R2 pools in IPv4 mode, coexisting with Lync Server 2013 in dual-stack mode.

- Lync Server 2013 pool in IPv6-only mode, if the IPv6-only pool is siloed.

1.3.3.2.4 Configure IP Address Types

Configure IP Address Types

Planning > Network Planning for Lync Server > Planning for and Configuring IPv6 >

Topic Last Modified: *2012-06-13*

You deploy IP address types by using topology settings that you configure in Topology Builder. This section describes how to deploy IP address types on Front End Servers, Mediation Servers, and Edge Servers.

In This Section

- Deploy IP Address Types on a Front End Server
- Deploy IP Address Types on a Mediation Server
- Deploy IP Address Types on an Edge Server

1.3.3.2.4.1 Deploy IP Address Types on a Front End Server

Deploy IP Address Types on a Front End Server

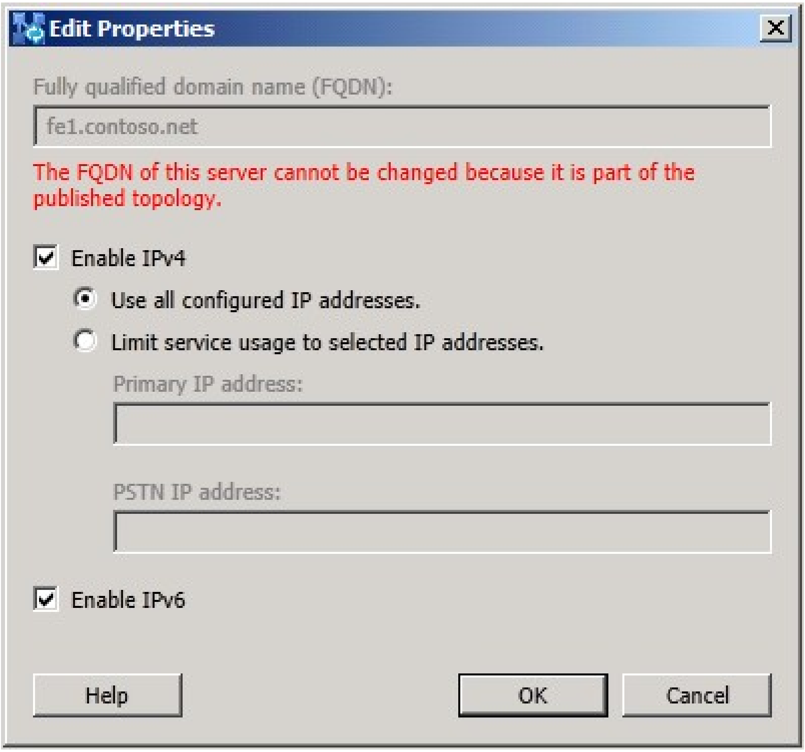
Network Planning for Lync Server > Planning for and Configuring IPv6 > Configure IP Address Types >

Topic Last Modified: *2012-06-14*

Using Topology Builder, perform the steps in the following procedure to deploy IP address types on a Front End Server.

⊟To deploy IP address types on a Front End Server

1. Under **Enterprise Edition Front End pools**, right-click the server within a pool, and then select **Edit Properties**. (Alternatively, select the server, and then click **Edit Properties** from the **Action** menu.)
2. In the **Edit Properties** dialog box, select the IP address type that you want to configure. For a dual-stack configuration, select **Enable IPv4** and **Enable IPv6**, as shown in the following figure.



Edit Properties

Fully qualified domain name (FQDN):

fe1.contoso.net

The FQDN of this server cannot be changed because it is part of the published topology.

☑ Enable IPv4

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

Primary IP address:

PSTN IP address:

☑ Enable IPv6

- **Use all configured IP addresses**. Select this option if you want to allow any IP address defined on the computer to be used.

> **Note:**
> This is the recommended option for IP version 6 (IPv6) configurations.

- **Limit service usage to selected IP addresses**. Select this option to specify a specific address to use on the new server. If you select this option, you must enter a value for **Primary IP address**.
- **Primary IP address**. Enter an IP address that the server will use for all communications except public switched telephone network (PSTN). The IP address entered must match the format of the select address type.
- **PSTN IP address**. Define a PSTN IP address when a Mediation Server is collocated on the Front End Server. This address must match the format of the selected address type.

1.3.3.2.4.2 Deploy IP Address Types on a Mediation Server

Deploy IP Address Types on a Mediation Server

Network Planning for Lync Server > Planning for and Configuring IPv6 > Configure IP Address Types >

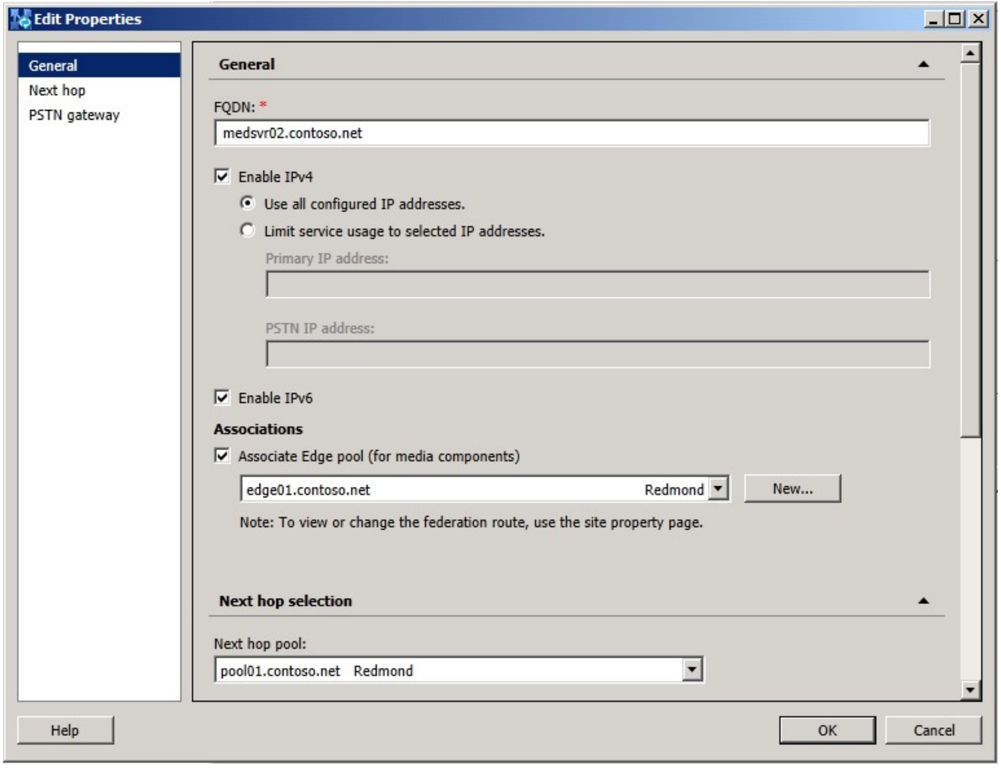
Topic Last Modified: *2012-06-14*

Using Topology Builder, perform the steps in the following procedure to deploy IP address types on a Mediation Server.

⊟To deploy IP address types on a Mediation Server

- In Topology Builder, under **Mediation pools**, right-click the server within a pool, and then select **Edit Properties**. (Alternatively, select the server, and then click **Edit Properties** from the **Action** menu.)

- In the **Edit Properties** dialog box, select the IP address type that you want to configure. For a dual-stack configuration, select **Enable IPv4** and **Enable IPv6**, as shown in the following figure.



General

FQDN: * medsvr02.contoso.net

☑ Enable IPv4

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

Primary IP address:

PSTN IP address:

☑ Enable IPv6

Associations

☑ Associate Edge pool (for media components)

edge01.contoso.net Redmond

Note: To view or change the federation route, use the site property page.

Next hop selection

Next hop pool: pool01.contoso.net Redmond

- **Use all configured IP addresses**. Select this option if you want to allow any IP address defined on the computer to be used.

Note:
This is the recommended option for IP version 6 (IPv6) configurations.

- **Limit service usage to selected IP addresses**. Select this option to specify a specific address to use on the new server. If you select this option, you must enter a value for Primary IP address.
- **Primary IP address**. Enter an IP address that the server will use for all communications except public switched telephone network (PSTN). The IP address entered must match the format of the select address type.
- **PSTN IP address**. Define a PSTN IP address when a Mediation Server is collocated on the Front End Server. This address must match the format of the selected address type.

1.3.3.2.4.3 Deploy IP Address Types on an Edge Server

Deploy IP Address Types on an Edge Server

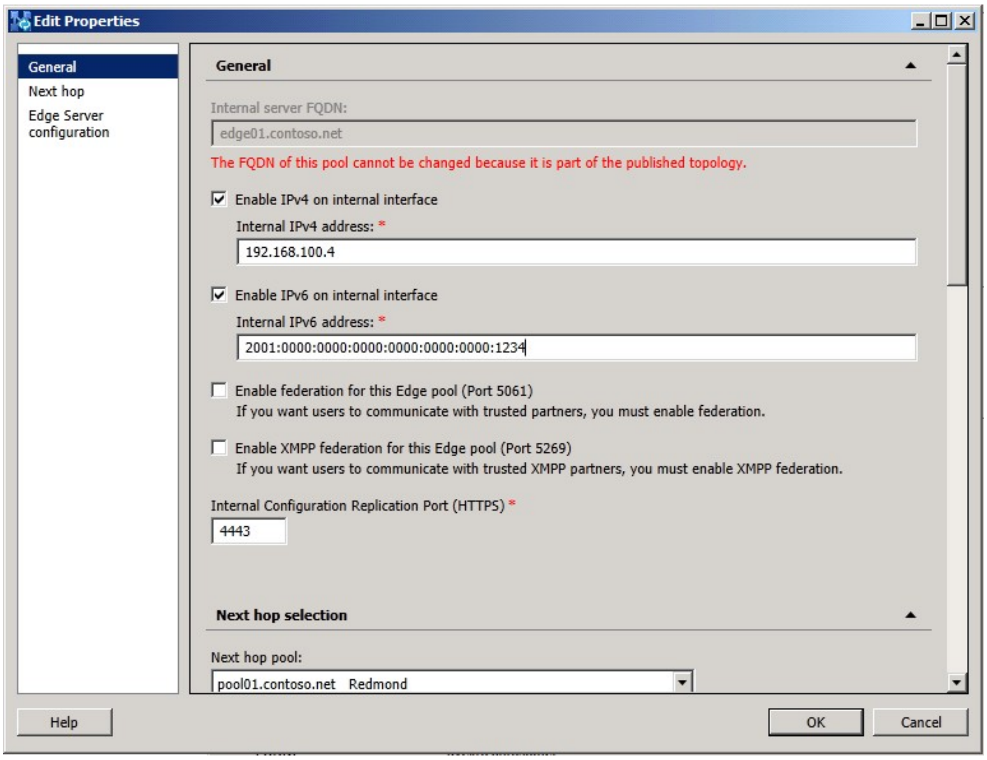
Network Planning for Lync Server > Planning for and Configuring IPv6 > Configure IP Address Types >

Topic Last Modified: *2012-06-14*

Using Topology Builder, perform the steps in the following procedure to deploy IP address types on an Edge Server.

⊟To deploy IP address types on an Edge Server

1. In Topology Builder, under **Edge pools**, right-click the server within a pool, and then select **Edit Properties**. (Alternatively, select the server, and then click **Edit Properties** from the **Action** menu.)
2. In the **Edit Properties** window, select the IP address configuration that you want to support. The following figures show a dual stack configuration for the internal interface and the external interface.



General

Internal server FQDN:

edge01.contoso.net

The FQDN of this pool cannot be changed because it is part of the published topology.

☑ Enable IPv4 on internal interface

Internal IPv4 address: *

192.168.100.4

☑ Enable IPv6 on internal interface

Internal IPv6 address: *

2001:0000:0000:0000:0000:0000:0000:1234

☐ Enable federation for this Edge pool (Port 5061)
If you want users to communicate with trusted partners, you must enable federation.

☐ Enable XMPP federation for this Edge pool (Port 5269)
If you want users to communicate with trusted XMPP partners, you must enable XMPP federation.

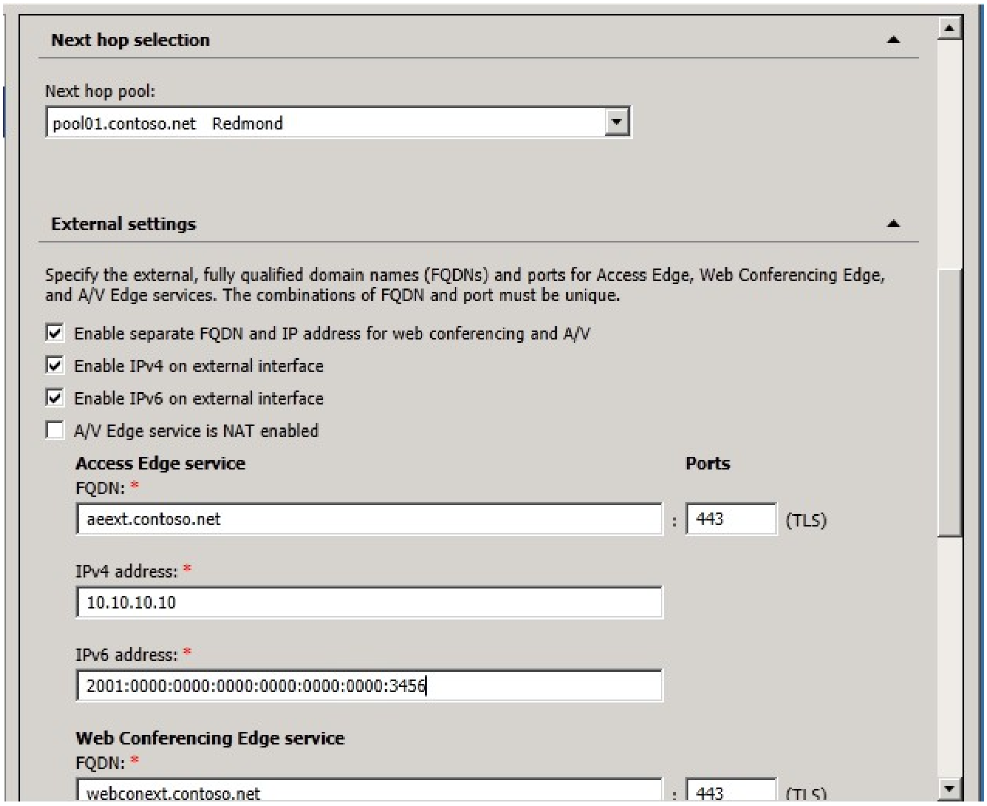
Internal Configuration Replication Port (HTTPS) *

4443

Next hop selection

Next hop pool:

pool01.contoso.net Redmond



Next hop selection

Next hop pool:
pool01.contoso.net Redmond

External settings

Specify the external, fully qualified domain names (FQDNs) and ports for Access Edge, Web Conferencing Edge, and A/V Edge services. The combinations of FQDN and port must be unique.

☑ Enable separate FQDN and IP address for web conferencing and A/V
☑ Enable IPv4 on external interface
☑ Enable IPv6 on external interface
☐ A/V Edge service is NAT enabled

Access Edge service — Ports
FQDN: *
aeext.contoso.net : 443 (TLS)

IPv4 address: *
10.10.10.10

IPv6 address: *
2001:0000:0000:0000:0000:0000:0000:3456

Web Conferencing Edge service
FQDN: *
webconext.contoso.net : 443 (TLS)

3. For each address type that you select, you must supply appropriate internal and external addresses.

1.3.3.3 Load Balancing Requirements

Load Balancing Requirements

Microsoft Lync Server 2013 > Planning > Network Planning for Lync Server >

Topic Last Modified: *2012-10-05*

If you have Front End pools, Director pools, or Edge Server pools, you need to deploy load balancing for these pools. Load balancing distributes the traffic among the servers in a pool.

Lync Server 2013 supports two types of load balancing solutions for client-to-server traffic: Domain Name System (DNS) load balancing and hardware load balancing. DNS load balancing offers several advantages including simpler administration, more efficient troubleshooting, and the ability to isolate much of your Lync Server traffic from any potential hardware load balancer problems.

Decide which load balancing solution is appropriate for each pool in your deployment, keeping in mind the following restrictions:

- The internal Edge interface and external Edge interface must use the same type of load balancing. You cannot use DNS load balancing on one interface and hardware load balancing on the other.
- Some types of traffic require a hardware load balancer. For example, HTTP traffic requires a hardware load balancer instead of DNS load balancing. DNS load balancing does not work with client-to-server web traffic.

For more details about choosing a hardware load balancer solution, see Hardware Load

Balancer Requirements.

If you choose to use DNS load balancing for a pool but still need to implement hardware load balancers for traffic such as HTTP traffic, the administration of the hardware load balancers is greatly simplified. For example, configuring the hardware load balancer will be simpler as it will only manage the HTTP and HTTPS traffic, while all other protocols will be managed by DNS load balancing. For details, see DNS Load Balancing.

For server-to-server traffic, Lync Server 2013 uses topology-aware load balancing. Servers read the published topology in the Central Management store to obtain the FQDNs of servers in the topology, and automatically distribute the traffic among the servers. Administrators do not need to set up or manage this type of load balancing.

If you use DNS load balancing and you need to block traffic to a specific computer, it is not sufficient to just remove the IP address entries from the Pool FQDN. You must remove the DNS entry for the computer as well.

1.3.3.3.1 Hardware Load Balancer Requirements

Hardware Load Balancer Requirements

Planning > Network Planning for Lync Server > Load Balancing Requirements >

Topic Last Modified: *2012-10-22*

The Lync Server 2013 scaled consolidated Edge topology is optimized for DNS load balancing for new deployments federating primarily with other organizations using Lync Server. If high availability is required for any of the following scenarios, a hardware load balancer must be used on Edge Server pools for the following:

- Federation with organizations using Office Communications Server 2007 R2 or Office Communications Server 2007
- Exchange UM for remote users using Exchange UM prior to Exchange 2010 with SP1
- Connectivity to public IM users

> **Important:**
>
> Using DNS load balancing on one interface and hardware load balancing on the other is not supported. You must use hardware load balancing for both interfaces or DNS load balancing for both.

> **Note:**
>
> If you are using a hardware load balancer, the load balancer deployed for connections with the internal network must be configured to load balance only the traffic to servers running the Access Edge service and the A/V Edge service. It cannot load balance the traffic to the internal Web Conferencing Edge service or the internal XMPP Proxy service.

> **Note:**
>
> The direct server return (DSR) NAT is not supported with Lync Server 2013.

To determine whether your hardware load balancer supports the necessary features required by Lync Server 2013, see "Lync Server 2010 Load Balancer Partners" at http://go.microsoft.com/fwlink/p/?linkId=202452.

Hardware Load Balancer Requirements

for Edge Servers Running the A/V Edge Service

Following are the hardware load balancer requirements for Edge Servers running the A/V Edge service:

- Turn off TCP nagling for both internal and external ports 443. Nagling is the process of combining several small packets into a single, larger packet for more efficient transmission.
- Turn off TCP nagling for external port range 50,000 – 59,999.
- Do not use NAT on the internal or external firewall.
- The edge internal interface must be on a different network than the Edge Server external interface and routing between them must be disabled.
- The external interface of the Edge Server running the A/V Edge Service must use publically routable IP addresses and no NAT or port translation on any of the edge external IP addresses.

Hardware Load Balancer Requirements

Cookie-based affinity requirements are greatly reduced in Lync Server 2013 for Web services. If you are deploying Lync Server 2013 and will not retain any Lync Server 2010 Front End Servers or Front End pools, you do not need cookie-based persistence. However, if you will temporarily or permanently retain any Lync Server 2010 Front End Servers or Front End pools, you still use cookie-based persistence as it is deployed and configured for Lync Server 2010.

Note:

If you decide to use cookie-based affinity even though your deployment does not require it, there is no negative impact to doing so.

For deployments that **will not use** cookie-based affinity:

- On the reverse proxy publishing rule for port 4443, set **Forward host header** to True. This will ensure that the original URL is forwarded.

For deployments that **will use** cookie-based affinity:

- On the reverse proxy publishing rule for port 4443, set **Forward host header** to True. This will ensure that the original URL is forwarded.
- Hardware load balancer cookie MUST NOT be marked httpOnly
- Hardware load balancer cookie MUST NOT have an expiration time
- Hardware load balancer cookie MUST be named **MS-WSMAN** (This is the value that the Web services expect, and cannot be changed)
- Hardware load balancer cookie MUST be set in every HTTP response for which the incoming HTTP request did not have a cookie, regardless of whether a previous HTTP response on that same TCP connection had already obtained a cookie. If the load balancer optimizes cookie insert to only occur once per TCP connection, that optimization MUST NOT be used

Note:

Typical hardware load balancer configurations use source-address affinity and a 20 min. TCP session lifetime, which is fine for Lync Server and Lync 2013 clients because session state is maintained through client usage and/or and application interaction.

If you are deploying mobile devices, your hardware load balancer must be able to load balance individual request within a TCP session (in effect, you must be able to load balance an individual request based on the target IP address).

Warning:

F5 hardware load balancers have a feature called OneConnect that ensures each request within a TCP connection is individually load balanced. If you are deploying mobile devices, ensure your hardware load balancer vendor supports the same functionality. The latest Apple iOS mobile apps require Transport Layer Security (TLS) version 1.2. F5 provides specific settings for this.
For details on third party hardware load balancers, see http://go.microsoft.com/fwlink/p/?linkId=230700

Following are the hardware load balancer requirements for Director and Front End pool Web Services:

- For internal Web Services VIPs, set Source_addr persistence (internal port 80, 443) on the hardware load balancer. For Lync Server 2013, Source_addr persistence means that multiple connections coming from a single IP address are always sent to one server to maintain session state.
- Use TCP idle timeout of 1800 seconds.
- On the firewall between the reverse proxy and the next hop pool’s hardware load balancer, create a rule to allow https: traffic on port 4443, from the reverse proxy to the hardware load balancer. The hardware load balancer must be configured to listen on ports 80, 443, and 4443.

Summary of Hardware Load Balancer Affinity Requirements

Client/user location	External web services FQDN affinity requirements	Internal web services FQDN affinity requirements
Lync Web App (internal and external users) Mobile device (internal and external users)	No affinity	Source address affinity
Lync Web App (external users only) Mobile device (internal and external users)	No affinity	Source address affinity
Lync Web App (internal users only) Mobile device (not deployed)	No affinity	Source address affinity

Port Monitoring for Hardware Load Balancers

You define port monitoring on the hardware load balancers to determine when specific services are no longer available due to hardware or communications failure. For example, if the Front End Server service (RTCSRV) stops because the Front End Server or Front End pool fails, the HLB monitoring should also stop receiving traffic on the Web Services. You implement port monitoring on the HLB to monitor the following:

Front End Server User Pool – HLB Internal Interface

Virtual IP/Port	Node Port	Node Machine/ Monitor	Persistence Profile	Notes

<pool>web-int_mco_443_vs 443	443	Front End 5061	Source	HTTPS
<pool>web-int_mco_80_vs 80	80	Front End 5061	Source	HTTP

Front End Server User Pool – HLB External Interface

Virtual IP/Port	Node Port	Node Machine/ Monitor	Persistence Profile	Notes
<pool>web_mco_443_vs 443	4443	Front End 5061	None	HTTPS
<pool>web_mco_80_vs 80	8080	Front End 5061	None	HTTP

1.3.3.4 Domain Name System (DNS) Requirements

Domain Name System (DNS) Requirements

Microsoft Lync Server 2013 > Planning > Network Planning for Lync Server >

Topic Last Modified: *2012-06-18*

To deploy Lync Server, you must create Domain Name System (DNS) records that enable the discovery of clients and servers, and, optionally, support for automatic client sign-in if your organization wants to support it.

Lync Server uses DNS in the following ways:

- To discover internal servers or pools for server-to-server communications.
- To allow clients to discover the Front End pool or Standard Edition server used for various SIP transactions.
- To allow unified communications (UC) devices that are not logged on to discover the Front End pool or Standard Edition server running Device Update Web Service, obtain updates, and send logs.
- To allow external servers and clients to connect to Edge Servers or the HTTP reverse proxy for instant messaging (IM) or conferencing.
- To allow external UC devices to connect to Device Update Web service through Edge Servers or the HTTP reverse proxy and obtain updates.
- To allow mobile clients to automatically discover Web Services resources without requiring users to manually enter URLs in device settings.
- Determine DNS Requirements
- DNS Requirements for Front End Pools
- DNS Requirements for Standard Edition Servers
- DNS Requirements for Simple URLs
- DNS Requirements for Automatic Client Sign-In
- DNS Requirements for Mobility

- DNS Load Balancing

1.3.3.4.1 Determine DNS Requirements

Determine DNS Requirements

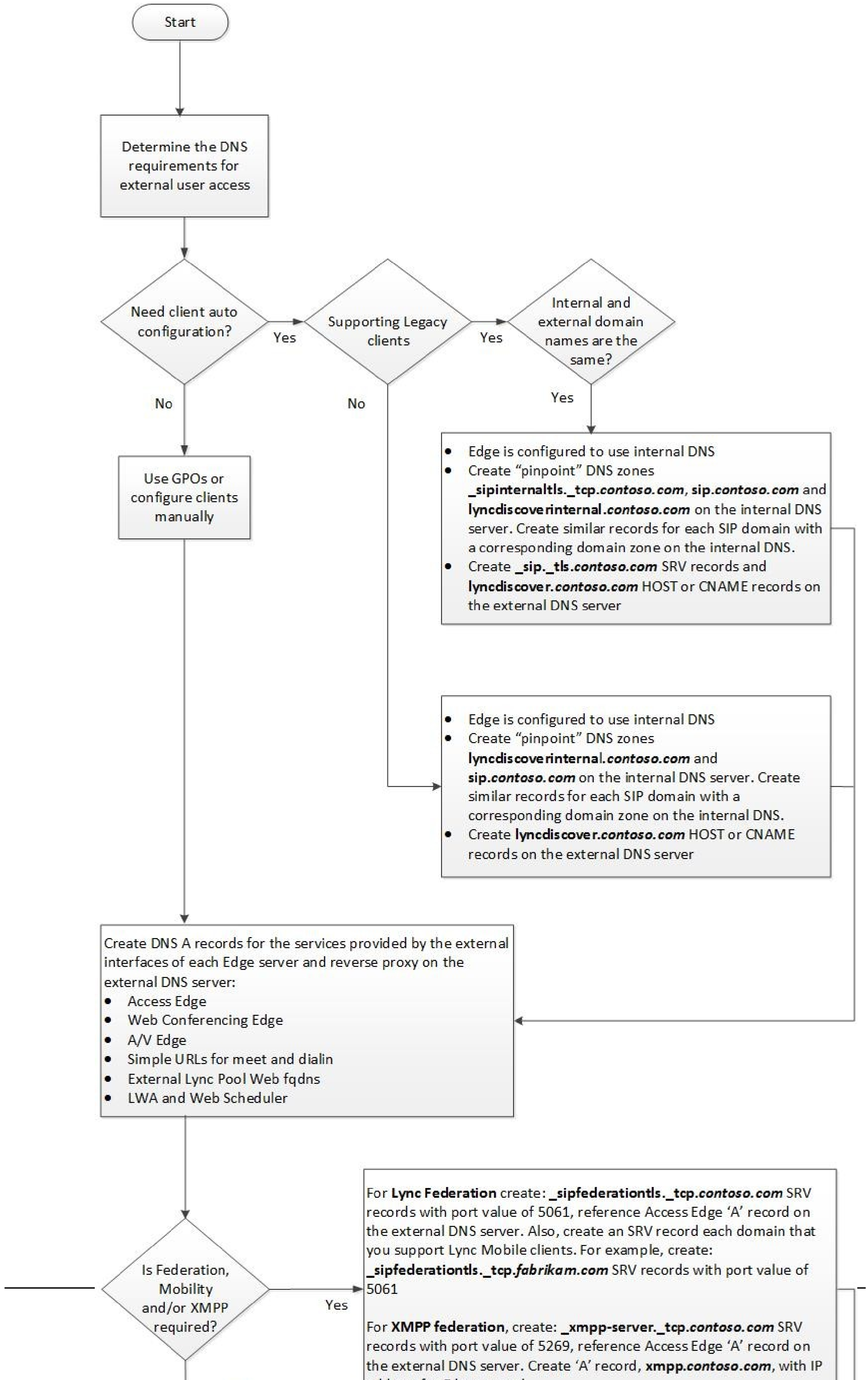
Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2013-02-22*

Use the following flow chart to determine Domain Name System (DNS) requirements. Changes for the Cumulative Updates for Lync Server 2013: February 2013 are noted where they apply.

Important:

Microsoft Lync Server 2013 supports the use of IPv6 addressing. To use IPv6 addresses, you must also provide support for IPv6 DNS and configure DNS host AAAA (known as “quad-A”) records. In deployments where both IPv4 and IPv6 are being used, it is best to configure and maintain both host A records for IPv4 and host AAAA for IPv6. Even if your deployment has transitioned fully to IPv6, IPv4 DNS host records may still be required when external users are still using IPv4.



Start
Need client auto configuration?
Yes
No
Supporting Legacy clients
Yes
No
Internal and external domain names are the same?
Yes
Is Federation, Mobility and/or XMPP required?
Yes

Determine the DNS requirements for external user access

Use GPOs or configure clients manually

- Edge is configured to use internal DNS
- Create "pinpoint" DNS zones **_sipinternaltls._tcp.*contoso.com***, **sip.*contoso.com*** and **lyncdiscoverinternal.*contoso.com*** on the internal DNS server. Create similar records for each SIP domain with a corresponding domain zone on the internal DNS.
- Create **_sip._tls.*contoso.com*** SRV records and **lyncdiscover.*contoso.com*** HOST or CNAME records on the external DNS server

- Edge is configured to use internal DNS
- Create "pinpoint" DNS zones **lyncdiscoverinternal.*contoso.com*** and **sip.*contoso.com*** on the internal DNS server. Create similar records for each SIP domain with a corresponding domain zone on the internal DNS.
- Create **lyncdiscover.*contoso.com*** HOST or CNAME records on the external DNS server

Create DNS A records for the services provided by the external interfaces of each Edge server and reverse proxy on the external DNS server:

- Access Edge
- Web Conferencing Edge
- A/V Edge
- Simple URLs for meet and dialin
- External Lync Pool Web fqdns
- LWA and Web Scheduler

For **Lync Federation** create: **_sipfederationtls._tcp.*contoso.com*** SRV records with port value of 5061, reference Access Edge 'A' record on the external DNS server. Also, create an SRV record each domain that you support Lync Mobile clients. For example, create: **_sipfederationtls._tcp.*fabrikam.com*** SRV records with port value of 5061

For **XMPP federation**, create: **_xmpp-server._tcp.*contoso.com*** SRV records with port value of 5269, reference Access Edge 'A' record on the external DNS server. Create 'A' record, **xmpp.*contoso.com***, with IP

Important:

By default the computer name of a computer that is not joined to a domain is a host name, not a fully qualified domain name (FQDN). Topology Builder uses FQDNs, not host names. So, you must configure a DNS suffix on the name of the computer to be deployed as an Edge Server that is not joined to a domain. **Use only standard characters** (including A–Z, a–z, 0–9, and hyphens) when assigning FQDNs of your Lync Servers, Edge Servers, and pools. Do not use Unicode characters or underscores. Nonstandard characters in an FQDN are often not supported by external DNS and public CAs (that is, when the FQDN must be assigned to the SN in the certificate). For additional details, see Configure DNS Host Records

How Lync Clients Locate Services

Microsoft Lync 2010, Lync 2013, and Lync Mobile are similar in how the client finds and accesses services in Lync Server 2013. The notable exception is the Lync Windows Store app that uses a different service location process. This section details two scenarios of how the clients locate services, first the traditional method using a series of SRV and A host records, second using only the Autodiscover service records. Cumulative updates to the desktop clients change the DNS location process from Lync Server 2010 For all clients, the DNS query process continues until a successful query is returned, or the list of possible DNS records is exhausted, and the final error is returned to the client.

For all clients **except** for the Lync Windows Store app During DNS lookup, SRV records are queried and returned to the client in the following order:

1. lyncdiscoverinternal.<*domain*>   A (host) record for the Autodiscover service on the internal Web services
2. lyncdiscover.<*domain*>   A (host) record for the Autodiscover service on the external Web services
3. _sipinternaltls._tcp.<*domain*>   SRV (service locator) record for internal TLS connections
4. _sipinternal._tcp.<*domain*>   SRV (service locator) record for internal TCP connections (performed only if TCP is allowed)
5. _sip._tls.<*domain*>   SRV (service locator) record for external TLS connections
6. sipinternal.<*domain*>   A (host) record for the Front End pool or Director, resolvable only on the internal network
7. sip.<*domain*>   A (host) record for the Front End pool or Director on the internal network, or the Access Edge service when the client is external
8. sipexternal.<*domain*>   A (host) record for the Access Edge service when the client is external

The Lync Windows Store app changes the process completely because it uses two records:

1. lyncdiscoverinternal.<*domain*>   A (host) record for the Autodiscover service on the internal Web services
2. lyncdiscover.<*domain*>   A (host) record for the Autodiscover service on the external Web services

There is no fallback to the other record types.

The difference between the methods used for newer clients as compared to older clients is that the Autodiscover service is becoming the preferred method to locate all services.

When a connection is successful, the Autodiscover Service returns all the Web Services URLs for the user's home pool, including the Mobility Service (known as Mcx by the virtual directory created for the service in IIS), Microsoft Lync Web App and Web scheduler URLs. However, both the internal Mobility Service URL and the external Mobility Service URL is associated with the external Web Services FQDN. Therefore, regardless of whether a mobile device is internal or external to the network, the device always connects to the Mobility Service externally through the reverse proxy.

If the Cumulative Updates for Lync Server 2013: February 2013 has been installed, the Autodiscover Service also returns references to Internal/UCWA, External/UCWA and UCWA. These entries refer to the Unified Communications Web API (UCWA) web component. Currently, only the entry UCWA is used and provides a reference to a URL for the web component. UCWA is used by Lync 2013 Mobile clients instead of the Mcx Mobility Service used by the Lync 2010 Mobile clients.

Note:

When creating SRV records, it is important to remember that they must point to a DNS A and AAAA (if you are using IPv6 addressing) record in the same domain in which the DNS SRV record is created. For example, if the SRV record is in contoso.com, the A and AAAA (if you are using IPv6 addressing) record it points to cannot be in fabrikam.com.

Tip:

The default configuration is to direct all mobile client traffic through the external site. You can modify settings to return only the internal URL, if this is more preferable for your requirements. With this configuration, users can use Lync mobile applications on their mobile devices only when they are inside the corporate network. To define this configuration, you use the **Set-CsMcxConfiguration** cmdlet.

Note:

Although mobile applications can also connect to other Lync Server 2013 services, such as Address Book Service, internal mobile application web requests go to the external web FQDN only for the Mobility Service. Other service requests, such as Address Book requests, do not require this configuration.

Mobile devices support manual discovery of services. In this case, each user must configure the mobile device settings with the full internal and external Autodiscover Service URIs, including the protocol and path, as follows:

- https://*<ExtPoolFQDN>*/Autodiscover/autodiscoverservice.svc/Root for external access
- https://*<IntPoolFQDN>*/AutoDiscover/AutoDiscover.svc/Root for internal access

We recommend that you use automatic discovery, rather than manual discovery. However, manual settings can be useful for troubleshooting mobile device connectivity issues.

Configuring Split-Brain DNS with Lync Server

Split-brain DNS is known by a number of names, for example, split DNS or split-horizon DNS. Simply, it describes a DNS configuration where there are two DNS zones with the same namespace – but one DNS zone services internal-only requests, and the other DNS zone services external-only requests. However, many of the DNS SRV and A records contained in the internal DNS will not be contained in the external DNS, and the reverse is also true. In cases where the same DNS record exists in both the internal and external DNS (for example, www.contoso.com), the IP address returned will be different based on where (internal or external) the query was initiated.

Important:

Currently, Split-Brain DNS is not supported for the mobility, or more specifically, the LyncDiscover and LyncDiscoverInternal DNS records. LyncDiscover must be defined on an external DNS server and LyncDiscoverInternal must be defined on an internal DNS server.

For the purposes of these topics, the term split-brain DNS will be used.

If you are configuring split-brain DNS, the following internal and external zone contain a summary of the types of DNS records required in each zone. For details, see Scenarios for External User Access.

Internal DNS:

- Contains a DNS zone called contoso.com for which it is authoritative
- The internal contoso.com zone contains:
  - DNS A and AAAA (if you are using IPv6 addressing) and SRV records for internal Lync Server 2013 client autoconfiguration (optional)
  - DNS A and AAAA (if you are using IPv6 addressing) or CNAME records for automatic discovery of Lync Server 2013 Web Services (optional)
  - DNS A and AAAA (if you are using IPv6 addressing) records for Front End pool name, Director or Director pool name, and all internal servers running Lync Server 2013 in the corporate network
  - DNS A and AAAA (if you are using IPv6 addressing) records for the Edge internal interface of each Lync Server 2013, Edge Server in the perimeter network
  - DNS A and AAAA (if you are using IPv6 addressing) records for the internal interface of each reverse proxy server in the perimeter network (optional for management of reverse proxy)
  - All Lync Server 2013 Edge Server internal edge interfaces in the perimeter network use the internal DNS zone for resolving queries to contoso.com
  - All servers running Lync Server 2013 and clients running Lync 2013 in the corporate network point to the internal DNS servers for resolving queries to contoso.com, or use of HOSTS file on each Edge server and list A and AAAA (if you are using IPv6 addressing) records for next hop server, specifically the Director or Director VIP, Front End pool VIP, or Standard Edition server

External DNS:

- Contains a DNS zone called contoso.com for which it is authoritative
- The external contoso.com zone contains:
  - DNS A and AAAA (if you are using IPv6 addressing) and SRV records for Lync Server 2013 client autoconfiguration (optional)
  - DNS A and AAAA (if you are using IPv6 addressing) or CNAME records for automatic discovery of Lync Server 2013 Web Services for use with mobility
  - DNS A and AAAA (if you are using IPv6 addressing) and SRV records for the Edge external interface of each Lync Server 2013, Edge Server or hardware load balancer virtual IP (VIP) in the perimeter network
  - DNS A and AAAA (if you are using IPv6 addressing) records for the external interface of the reverse proxy server or VIP for a pool of reverse proxy servers in the perimeter network

Automatic Configuration without Split-Brain DNS

Using split-brain DNS, a Lync Server 2013 user that signs in internally can take advantage of automatic configuration if the internal DNS zone contains a _sipinternaltls._tcp SRV record for each SIP domain in use. However, if you do not use split-brain DNS, internal automatic configuration of clients running Lync will not work unless one of the workarounds described in later in this section is implemented. This is because Lync Server 2013 requires the user's SIP URI to match the domain of the Front End pool designated for automatic configuration. This was also the case with earlier versions of Communicator.

For example, if you have two SIP domains in use, the following DNS service (SRV) records would be required:

- If a user signs in as bob@contoso.com the following SRV record will work for automatic configuration because the user's SIP domain (contoso.com) matches the domain of automatic configuration Front End pool):

_sipinternaltls._tcp.contoso.com. 86400 IN SRV 0 0 5061 pool01.contoso.com

- If a user signs in as alice@fabrikam.com the following DNS SRV record will work for automatic configuration of the second SIP domain.
  _sipinternaltls._tcp.fabrikam.com. 86400 IN SRV 0 0 5061 pool01.fabrikam.com

For comparison, if a user signs in as tim@litwareinc.com the following DNS SRV record will not work for automatic configuration, because the client's SIP domain (litwareinc.com) does not match the domain that the pool is in (fabrikam.com):

_sipinternaltls._tcp.litwareinc.com. 86400 IN SRV 0 0 5061 pool01.fabrikam.com

If automatic configuration is required for clients running Lync, select one of the following options:

- **Group Policy Objects** Use Group Policy objects (GPOs) to populate the correct server values.

  Note:
  This option does not enable automatic configuration, but it does automate the process of manual configuration, so if this approach is used, the SRV records associated with automatic configuration are not required.

- **Matching internal zone** Create a zone in the internal DNS that matches the external DNS zone (for example, contoso.com) and create DNS A and AAAA (if you are using IPv6 addressing) records corresponding to the Lync Server 2013 pool used for automatic configuration. For example, if a user is homed on pool01.contoso.net but signs into Lync as bob@contoso.com, create an internal DNS zone called contoso.com and inside it, create a DNS A and AAAA (if IPv6 addressing is used) record for pool01.contoso.com.
- **Pin-point internal zone** If you are creating an entire zone in the internal DNS is not an option, you can create pin-point (that is, dedicated) zones that correspond to the SRV records that are required for automatic configuration, and populate those zones using dnscmd.exe. Dnscmd.exe is required because the DNS user interface does not support creation of pin-point zones. For example, if the SIP domain is contoso.com and you have a Front End pool called pool01 that contains two Front End Servers, you need the following pin-point zones and A records in your internal DNS:

```
dnscmd . /zoneadd _sipinternaltls._tcp.contoso.com. /dsprimary
dnscmd . /recordadd _sipinternaltls._tcp.contoso.com. @ SRV 0 0 5061 po
dnscmd . /zoneadd pool01.contoso.com. /dsprimary
dnscmd . /recordadd pool01.contoso.com. @ A 192.168.10.90
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
dnscmd . /recordadd pool01.contoso.com. @ A 192.168.10.91
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
```

  If your environment contains a second SIP domain (for example, fabrikam.com), you need the following pin-point zones and A records in your internal DNS:

```
dnscmd . /zoneadd _sipinternaltls._tcp.fabrikam.com. /dsprimary
dnscmd . /recordadd _sipinternaltls._tcp.fabrikam.com. @ SRV 0 0 5061 p
dnscmd . /zoneadd pool01.fabrikam.com. /dsprimary
dnscmd . /recordadd pool01.fabrikam.com. @ A 192.168.10.90
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
dnscmd . /recordadd pool01.fabrikam.com. @ A 192.168.10.91
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
```

Note:
The Front End pool FQDN appears twice, but with two different IP addresses. This is because DNS load balancing is used, but if hardware load balancing is used, there would be only a single Front End pool entry. Also, the Front End pool FQDN values change between the contoso.com example and the fabrikam.com example, but the IP addresses remain the same. This is because users signing in from either SIP domain, use the same Front End pool for automatic configuration.

For details, see the DMTF blog article, "Communicator Automatic Configuration and Split-Brain DNS," at http://go.microsoft.com/fwlink/p/?linkId=200707.

Note:
The content of each blog and its URL are subject to change without notice.

Configuring the domain name system (DNS) for Disaster Recovery

To configure DNS to redirect Lync Server 2013 Web traffic to your disaster recovery and failover sites, you must be using a DNS provider that supports GeoDNS. You can set up your DNS records for Web to support disaster recovery, so that features that use Web services continue even if one entire Front End pool goes down. This disaster recovery feature supports the Autodiscover (Lyncdiscover URL), Meet and Dial-In simple URLs.

You define and configure additional DNS host (A and AAAA if using IPv6) records for internal and external resolution of Web services at your GeoDNS provider. The following details assume paired pools, geographically dispersed, and GeoDNS supported by your provider with either round-robin DNS, or configured to use Pool1 as primary, and fail over to Pool2 in the event of communications loss or hardware failure.

GeoDNS record (example)	Pool records (example)	CNAME records (example)	DNS settings (select one option)
Meet-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Meet.contoso.com alias to Pool1InternalWebFQDN.contoso.com Meet.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Meet-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Meet.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Meet.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Dialin-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Dialin.contoso.com alias to Pool1InternalWebFQDN.contoso.com Dialin.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Dialin-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Dialin.contoso.com alias to Pool1ExternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure

		Dialin.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	
Lyncdiscoverint-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Lyncdiscoverinternal.contoso.com alias to Pool1InternalWebFQDN.contoso.com Lyncdiscoverinternal.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Lyncdiscover-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Lyncdiscover.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Lyncdiscover.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Scheduler-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Scheduler.contoso.com alias to Pool1InternalWebFQDN.contoso.com Scheduler.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Scheduler-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Scheduler.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Scheduler.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure

DNS Load Balancing

DNS load balancing is typically implemented at the application level. The application (for example, a client running Lync), tries to connect to a server in a pool by connecting to one of the IP addresses returned from the DNS A and AAAA (if IPv6 addressing is used) record query for the pool fully qualified domain name (FQDN).

For example, if there are three front end servers in a pool named pool01.contoso.com, the following will happen:

- Clients running Lync query DNS for pool01.contoso.com. The query returns three IP addresses and caches them as follows (not necessarily in this order):
  pool01.contoso.com 192.168.10.90
  pool01.contoso.com 192.168.10.91

pool01.contoso.com 192.168.10.92

- The client attempts to establish a Transmission Control Protocol (TCP) connection to one of the IP addresses. If that fails, the client tries the next IP address in the cache.
- If the TCP connection succeeds, the client negotiates TLS to connect to the primary registrar on pool01.contoso.com.
- If the client tries all cached entries without a successful connection, the user is notified that no servers running Lync Server 2013 are available at the moment.

Note:

DNS-based load balancing is different from DNS round robin (DNS RR) which typically refers to load balancing by relying on DNS to provide a different order of IP addresses corresponding to the servers in a pool. Typically DNS RR only enables load distribution, but does not enable failover. For example, if the connection to the one IP address returned by the DNS A and AAAA (if you are using IPv6 addressing) query fails, the connection fails. Therefore, DNS round robin by itself is less reliable than DNS-based load balancing. You can use DNS round robin in conjunction with DNS load balancing.

DNS load balancing is used for the following:

- Load balancing server-to-server SIP to the Edge Servers
- Load balancing Unified Communications Application Services (UCAS) applications such as Conferencing Auto Attendant, Response Group, and Call Park
- Preventing new connections to UCAS applications (also known as "draining")
- Load balancing all client-to-server traffic between clients and Edge Servers

DNS load balancing cannot be used for the following:

- Client-to-server web traffic to Director or Front End Servers

DNS load balancing and federated traffic:

If multiple DNS records are returned by a DNS SRV query, the Access Edge service always picks the DNS SRV record with the lowest numeric priority and highest numeric weight. The Internet Engineering Task Force document "A DNS RR for specifying the location of services (DNS SRV)" http://www.ietf.org/rfc/rfc2782.txt specifies that if there are multiple DNS SRV records defined, priority is first used, then weight. For example DNS SRV record A has a weight of 20 and a priority of 40 and DNS SRV record B has a weight of 10 and priority of 50. DNS SRV record A with priority 40 will be selected. The following rules apply to DNS SRV record selection:

- Priority is considered first. A client MUST attempt to contact the target host defined by the DNS SRV record with the lowest numbered priority it can reach. Targets with the same priority SHOULD be tried in an order defined by the weight field.
- The weight field specifies a relative weight for entries with the same priority. Larger weights SHOULD be given a proportionately higher probability of being selected. DNS administrators SHOULD use Weight 0 when there isn't any server selection to do. In the presence of records containing weights greater than 0, records with weight 0 should have a very small chance of being selected.

If multiple DNS SRV records with equal priority and weight are returned, the Access Edge service will select the SRV record that was received first from the DNS server.

DNS Requirements for Front End Pools

[Planning](#) > [Network Planning for Lync Server](#) > [Domain Name System (DNS) Requirements](#) >

Topic Last Modified: *2012-11-07*

This section describes the Domain Name System (DNS) records that are required for deployment of Front End pools.

DNS Records for Front End Pools

The following table specifies DNS requirements for a Lync Server 2013 Front End pool deployment.

DNS Requirements for a Front End Pool

Deployment scenario	DNS requirement
Front End pool with multiple Front End Servers and a hardware load balancer (whether or not DNS load balancing is also deployed on that pool)	When using both DNS load balancing and a hardware load balancer, you need to Host (A) records. Create an internal A record that resolves the fully qualified domain name (FQDN) of the Front End pool for DNS load balancing. Create an internal host (A) record for the internal Web services to the virtual IP (VIP) address of the load balancer. You must use the internal Web services name as defined in Topology Builder. For example, if you use both DNS load balancing and hardware load balancing, you would have an A record for each Front End Server in a pool for DNS load balancing, and an A record for the internal Web services pointing to the virtual IP of the hardware load balancer: • DNS load balancing: Pool01.contoso.net IP Address of pool 10.10.10.5 ⚠**Warning:** Each Front End Server will also have a distinct A record: .1.FE01.contoso.net 10.10.10.1 .2.FE02.contoso.net 10.10.10.2 .3.FE03.contoso.net 10.10.10.3 .4.FE04.contoso.net 10.10.10.4 • Hardware load balancing: WebInternal.contoso.net IP Address of HLB VIP 192.168.10.5 All traffic except for HTTP/HTTPS traffic will use the Pool01.contoso.net record. HTTP/HTTPS traffic will use the defined internal Web services address of 192.168.10.5
Front End pool with DNS load balancing deployed	A set of internal A records that resolve the FQDN of the pool to the IP address of each server in the pool. There must one A record for each server in the pool.

Front End pool with DNS load balancing deployed	A set of internal A records that resolve the FQDN of each server in the pool to the IP address of that server. For details, see DNS Load Balancing in the Planning documentation.
Front End pool with a single Front End Server and a dedicated back-end database but no load balancer	An internal A record that resolves the FQDN of the Front End pool to the IP address of the single Enterprise Edition Front End Server.
Automatic client sign-in	For each supported SIP domain, an SRV record for _sipinternaltls._tcp.<domain> over port 5061 that maps to the FQDN of the Front End pool that authenticates and redirects client requests for sign-in. For details, see DNS Requirements for Automatic Client Sign-In.
Device Update Web service discovery by unified communications (UC) devices	An internal A record with the name ucupdates-r2.<SIP domain> that resolves to the IP address of the Front End pool that hosts the Device Update Web service. In the situation where a UC device is turned on, but a user has never logged into the device, the A record allows the device to discover the Front End pool hosting Device Update Web service and obtain updates. Otherwise, devices obtain this information though in-band provisioning the first time a user logs in. ◆**Important:** If you have an existing deployment of Device Update Web service in Lync Server 2010, you have already created an internal A record with the name ucupdates.<*SIP domain*>. For Microsoft Office Communications Server 2007 R2, you must create an additional DNS A record with the name ucupdates-r2.<*SIP domain*>.
A reverse proxy to support HTTP traffic	An external A record that resolves the external web farm FQDN to the external IP address of the reverse proxy. Clients and UC devices use this record to connect to the reverse proxy. For details, see Determine DNS Requirements in the Planning documentation.

The following table shows an example of the DNS records required for the internal web farm FQDN.

Example DNS Records for Internal Web Farm FQDN

Internal web farm FQDN	Pool FQDN	DNS A record(s)
webcon.contoso.com	ee-pool.contoso.com	DNS A record for the ee-pool.contoso.com that resolves to the VIP address of the load balancer used by the Front End Servers. DNS A record for webcon.contoso.com that resolves to the VIP address of the load balancer used by the Front End Servers.

ee-pool.contoso.com	ee-pool.contoso.com	DNS A record for ee-pool.contoso.com that resolves to the virtual IP (VIP) address of the load balancer used by the Enterprise Edition Front End Servers in the Front End pool. Note that if you are using DNS load balancing on this pool, your Front End pool and internal web farm cannot have the same FQDN.

1.3.3.4.3 DNS Requirements for Standard Edition Servers

DNS Requirements for Standard Edition Servers

Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2012-06-19*

This section describes the Domain Name System (DNS) records that are required for deployment of Standard Edition servers.

DNS Records for Standard Edition Servers

The following table specifies DNS requirements for Lync Server 2013 Standard Edition server deployment.

DNS Requirements for a Standard Edition Server

Deployment scenario	**DNS requirement**
Standard Edition server	An internal A record that resolves the fully qualified domain name (FQDN) of the server to its IP address.
Automatic client sign-in	For each supported SIP domain, an SRV record for _sipinternaltls._tcp.<*domain*> over port 5061 that maps to the FQDN of the Standard Edition server that authenticates and redirects client requests for sign-in. For details, see DNS Requirements for Automatic Client Sign-In.
Device Update Web service discovery by unified communications (UC) devices	An internal A record with the name ucupdates-r2.<*SIP domain*> that resolves to the IP address of the Standard Edition server hosting Device Update Web service. In the situation where a UC device is turned on, but a user has never logged into the device, the A record allows the device to discover the server hosting Device Update Web service and obtain updates. Otherwise, devices obtain the server information

	though in-band provisioning the first time a user logs in.
A reverse proxy to support HTTP traffic	An external A record that resolves the external web farm FQDN to the external IP address of the reverse proxy. Clients and UC devices use this record to connect to the reverse proxy. For details, see Determine DNS Requirements in the Planning documentation.

1.3.3.4.4 DNS Requirements for Simple URLs

DNS Requirements for Simple URLs

Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2013-02-22*

Lync Server 2013 supports simple URLs, which make joining meetings easier for your users, and make getting to Lync Server administrative tools easier for your administrators. For details about simple URLs, see Planning for Simple URLs.

Lync Server supports the following three simple URLs: Meet, Dial-In, and Admin. You are required to set up simple URLs for Meet and Dial-In, and the Admin simple URL is optional. The Domain Name System (DNS) records that you need to support simple URLs depend on how you have defined these simple URLs, and whether you want to support disaster recovery for Simple URLs.

Simple URL Option 1

In Option 1, you create a new base URL for each simple URL.

Note:

When a user clicks a simple URL meeting link, the server that the DNS A record resolves to determines the correct client software to start. After the client software is started, it automatically communicates with the pool where the conference is hosted. This way, users are directed to the appropriate server for meeting content no matter which server or pool the simple URL DNS A records resolve to.

Simple URL Option 1

Simple URL	Example
Meet	https://meet.contoso.com, https://meet.fabrikam.com, and so on (one for each SIP domain in your organization)
Dial-in	https://dialin.contoso.com
Admin	https://admin.contoso.com

If you use Option 1, you must define the following:

- For each Meet simple URL, you need a DNS A record that resolves the URL to the IP address of the Director, if you have one deployed. Otherwise, it should resolve to the IP address of the load balancer of a Front End pool. If you have not deployed a pool and are using a Standard Edition server deployment, the DNS A record must resolve to the IP address of one Standard Edition server in

your organization.
If you have more than one SIP domain in your organization and you use this option, you must create Meet simple URLs for each SIP domain and you need a DNS A record for each Meet simple URL. For example, if you have both contoso.com and fabrikam.com, you will create DNS A records for both https://meet.contoso.com and https://meet.fabrikam.com.
Alternatively, if you have multiple SIP domains and you want to minimize the DNS record and certificate requirements for these simple URLs, use Option 3 as described later in this topic.

- For the Dial-in simple URL, you need a DNS A record that resolves the URL to the IP address of the Director, if you have one deployed. Otherwise, it should resolve to the IP address of the load balancer of a Front End pool. If you have not deployed a pool and are using a Standard Edition server deployment, the DNS A record must resolve to the IP address of one Standard Edition server in your organization.
- The Admin simple URL is internal only. It requires a DNS A record that resolves the URL to the IP address of the Director, if you have one deployed. Otherwise, it should resolve to the IP address of the load balancer of a Front End pool. If you have not deployed a pool and are using a Standard Edition server deployment, the DNS A record must resolve to the IP address of one Standard Edition server in your organization.

Simple URL Option 2

With Option 2, the Meet, Dial-in, and Admin simple URLs all have a common base URL, such as lync.contoso.com. Therefore, you need only one DNS A record for these simple URLs, which resolves lync.contoso.com to the IP address of a Director pool or Front End pool. If you have not deployed a pool and are using a Standard Edition server deployment, the DNS A record must resolve to the IP address of one Standard Edition server in your organization.

Note that if you have more than one SIP domain in your organization, you must still create Meet simple URLs for each SIP domain and you need a DNS A record for each Meet simple URL. In this example, while three simple URLs are all based on lync.contoso.com, an additional Meet simple URL for fabrikam.com is set up with a different base URL. In this example, you must create DNS A records for both https://lync.contoso.com and https://lync.fabrikam.com. Simple URL Option 3 shows another way to handle naming and DNS A records if you have multiple SIP domains.

Simple URL Option 2

Simple URL	**Example**
Meet	https://lync.contoso.com/Meet, https://lync.fabrikam.com/Meet, and so on (one for each SIP domain in your organization)
Dial-in	https://lync.contoso.com/Dialin
Admin	https://lync.contoso.com/Admin

Simple URL Option 3

Option 3 is most useful if you have many SIP domains, and you want them to have separate simple URLs but want to minimize the DNS record and certificate requirements for these simple URLs. In this example, you need only one DNS A record, which resolves lync.contoso.com to the IP address of a Director pool or Front End pool.

Simple URL Option 3

Simple URL	Example
Meet	https://lync.contoso.com/contosoSIPdomain/Meet https://lync.contoso.com/fabrikamSIPdomain/Meet
Dial-in	https://lync.contoso.com/contosoSIPdomain/Dialin
Admin	https://lync.contoso.com/contosoSIPdomain/Admin

Disaster Recovery Option for Simple URLs

If you have multiple sites that contain Front End pools and your DNS provider supports GeoDNS, you can set up your DNS records for Simple URLs to support disaster recovery, so that Simple URL functionality continues even if one entire Front End pool goes down. This disaster recovery feature supports the Meet and Dial-In simple URLs.

To configure this, create two GeoDNS addresses. Each address has two DNS A or CNAME records that resolve to two pools which are paired together for disaster recovery purposes. One GeoDNS address is used for internal access, and resolves to the internal web FQDN or load balancer IP address for the two pools. The other GeoDNS address is used for external access and resolves to the external web FQDN or load balancer IP address for the two pools. The following is an example for the Meet simple URL, using the FQDNs for the pools.

```
Meet-int.geolb.contoso.com
     Pool1InternalWebFQDN.contoso.com
     Pool2InternalWebFQDN.contoso.com
```

```
Meet-ext.geolb.contoso.com
     Pool1ExternalWebFQDN.contoso.com
     Pool2ExternalWebFQDN.contoso.com
```

Then create CNAME records that resolve your Meet simple URL (such as meet.contoso.com) to the two GeoDNS addresses.

Note:

If your network uses *hairpinning* (routing all your Simple URL traffic through the external link, including traffic that comes from within your organization), then you can just configure the external GeoDNS address and resolve your Meet simple URL to only that external address.

When you use this method, you can configure each GeoDNS address to use either a round robin method to distribute requests to the two pools, or to connect primarily to one pool (such as the pool located geographically closer) and use the other pool only in case of connectivity failure.

You can set up the same configuration for the Dial-In simple URL. To do so, create additional records like those in the previous example, substituting `dialin` for `meet` in the DNS records. For the Admin simple URL, use one of the three options listed earlier in this section.

Once this configuration is set up, you must use a monitoring application to set up HTTP monitoring to watch for failures. For external access, monitor to make sure that HTTPS GET autodiscovery requests to the the external web FQDN or load balancer IP address for the two pools are successful. For example, the following requests must not contain any

ACCEPT header and must return **200 OK**.

```
HTTPS GET Pool1ExternalWebFQDN.contoso.com/autodiscover/autodiscoverservice.svc/r
HTTPS GET Pool2ExternalWebFQDN.contoso.com/autodiscover/autodiscoverservice.svc/r
```

For internal access, you must monitor port 5061 on the internal web FQDN or load balancer IP address for the two pools. If any connectivity failures are detected, the VIP for these pools must close ports 80, 443 and 444.

1.3.3.4.5 DNS Requirements for Automatic Client Sign-In

DNS Requirements for Automatic Client Sign-In

Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2012-06-19*

This section explains the Domain Name System (DNS) records that are required for automatic client sign-in. When you deploy your Standard Edition servers or Front End pools, you can configure your clients to use automatic discovery to sign in to the appropriate Standard Edition server or Front End pool. If you plan to require your clients to connect manually to Lync Server 2013, you can skip this topic.

To support automatic client sign-in, you must:

- Designate a single server or pool to distribute and authenticate client sign-in requests. This can be an existing server or pool in your organization that hosts users, or you can designate a dedicated server or pool for this purpose that hosts no users. For high availability, we recommend that you designate a Front End pool for this function.
- Create an internal DNS SRV record to support automatic client sign-in for this server or pool.

Note:

In the following record requirements, SIP domain refers to the host portion of the SIP URIs assigned to users. For example, if SIP URIs are of the form *@contoso.com, contoso.com is the SIP domain. The SIP domain is often different from the internal Active Directory domain. An organization can also support multiple SIP domains.

To enable automatic configuration for your clients, you must create an internal DNS SRV record that maps one of the following records to the fully qualified domain name (FQDN) of the Front End pool or Standard Edition server that distributes sign-in requests from Lync clients:

- _sipinternaltls._tcp.<*domain*> - for internal TLS connections

You only need to create a single SRV record for the Front End pool or Standard Edition server or that will distribute sign-in requests.

The following table shows some example records required for the fictitious company Contoso, which supports SIP domains of contoso.com and retail.contoso.com.

Example of DNS Records Required for Automatic Client Sign-in with Multiple SIP Domains

FQDN of Front End pool used to distribute sign-in requests	SIP domain	DNS SRV record

pool01.contoso.com	contoso.com	An SRV record for _sipinternaltls._tcp.contoso.com domain over port 5061 that maps to pool01.contoso.com
pool01.contoso.com	retail.contoso.com	An SRV record for _sipinternaltls._tcp.retail.contoso.com domain over port 5061 that maps to pool01.contoso.com

Note:

By default, queries for DNS records adhere to strict domain name matching between the domain in the user name and the SRV record. If you prefer that client DNS queries use suffix matching instead, you can configure the DisableStrictDNSNaming Group Policy. For details, see Planning for Clients and Devices in Lync Server 2013 in the Planning documentation.

Example of the Certificates and DNS Records Required for Automatic Client Sign-In

This example uses the same example names in the preceding table. The Contoso organization supports the SIP domains of contoso.com and retail.contoso.com, and all of its users have a SIP URI in one of the following forms:

- <*user*>@retail.contoso.com
- <*user*>@contoso.com

1.3.3.4.6 DNS Requirements for Mobility

DNS Requirements for Mobility

Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2012-11-13*

When you deploy the Lync Server 2013 mobility feature, you can use the new URLs that are available with the Microsoft Lync Server 2013 Autodiscover Service, or you can use your existing Web Services URLs. If you use your existing URLs, users need to manually enter the URLs in their mobile device settings. This option is typically used for troubleshooting. When you use the new URLs, mobile clients can automatically discover Lync Server 2013 resources. When you support automatic discovery, you need to add new Domain Name System (DNS) records. This section describes the DNS records that are required for automatic discovery.

To support automatic discovery, you need to create the following DNS records for each SIP domain:

- An internal DNS record to support mobile users who connect from within your organization's network
- An external, or public, DNS record to support mobile users who connect from the Internet

The internal automatic discovery URL should not be addressable from outside your network. The external automatic discovery URL should not be addressable from within your network. However, if you cannot meet this requirement for the external URL, mobile client functionally should not be affected.

The DNS records can be either CNAME records or A (host) records.

Internal DNS records

You need to create one of the following internal DNS records:

Record type	Host name or SRV definition	Resolves to
CNAME	lyncdiscoverinternal.*<sipdomain>*	Internal Web Services fully qualified domain name (FQDN) for your Director pool, if you have one, or for your Front End pool if you do not have a Director
A (host)	lyncdiscoverinternal.*<sipdomain>*	Internal Web Services IP address (virtual IP (VIP) address if you use a load balancer) of your Director pool, if you have one, or of your Front End pool if you do not have a Director

External DNS records

You need to create one of the following external DNS records:

Record type	Host name	Resolves to
CNAME	lyncdiscover. *<sipdomain>*	External Web Services FQDN for your Director pool, if you have one, or for your Front End pool if you do not have a Director
A (host)	lyncdiscover. *<sipdomain>*	External or public IP address (VIP address if you use a load balancer) of the reverse proxy
SRV	_sipfederationtls._tcp. *<sipdomain>* Resolves to host (A or AAAA) record for the Access Edge service	To support Push Notification Service and Apple Push Notification service, you create one SRV record for each SIP domain that has Microsoft Lync Mobile clients. **Important:** This requirement applies only to Microsoft Lync Mobile clients on Apple or Microsoft based mobile devices. Andriod and Nokia Symbian devices do not use push notification.

Note:

Lyncdiscover, also known as autodiscover, traffic goes through the reverse proxy. SRV record points to a record that resolves through the Access Edge service.

1.3.3.4.7 DNS Load Balancing

DNS Load Balancing

Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2013-01-23*

Lync Server enables DNS load balancing, a software solution that can greatly reduce the administration overhead for load balancing on your network. DNS load balancing balances the network traffic that is unique to Lync Server, such as SIP traffic and media traffic.

If you deploy DNS load balancing, your organization's administration overhead for hardware load balancers will be minimized. Additionally, complex troubleshooting of problems related to misconfiguration of load balancers for SIP traffic will be eliminated. You can also prevent server connections so that you can take servers offline. DNS load balancing also ensures that hardware load balancer problems do not affect elements of SIP traffic such as basic call routing.

If you use DNS load balancing, you may also be able to purchase lower-cost hardware load balancers than if you used the hardware load balancers for all types of traffic. You should use load balancers that have passed interoperability qualification testing with Lync Server. For details about load balancer interoperability testing, see "Lync Server 2010 Load Balancer Partners" at http://go.microsoft.com/fwlink/p/?linkId=202452.

DNS load balancing is supported for Front End pools, Edge Server pools, Director pools, and stand-alone Mediation Server pools.

DNS Load Balancing on Front End Pools and Director Pools

You can use DNS load balancing for the SIP traffic on Front End pools and Director pools. With DNS load balancing deployed, you still need to also use hardware load balancers for these pools, but only for client-to-server HTTPS traffic. The hardware load balancer is used for HTTPS traffic from clients over ports 443 and 80.

Although you still need hardware load balancers for these pools, their setup and administration will be primarily for HTTPS traffic, which the administrators of hardware load balancers are accustomed to.

DNS Load Balancing and Supporting Older Clients and Servers

DNS load balancing supports automatic failover only for servers running Lync Server 2013 or Lync Server 2010, and for Lync 2013 and Lync 2010 clients. Earlier versions of clients and Office Communications Server can still connect to pools running DNS load balancing, but if they cannot make a connection to the first server that DNS load balancing refers them to, they are unable to fail over to another server in the pool.

Additionally, if you are using Exchange UM, you must use a minimum of Exchange 2010 SP1 to get support for Lync Server DNS load balancing. If you use an earlier version of Exchange, your users will not have failover capabilities for these Exchange UM scenarios:

- Playing their Enterprise Voice voice mail on their phone
- Transferring calls from an Exchange UM Auto Attendant

All other Exchange UM scenarios will work properly.

Deploying DNS Load Balancing on Front End Pools and Director Pools

Deploying DNS load balancing on Front End pools and Director pools requires you to perform a couple of extra steps with FQDNs and DNS records.

- A pool that uses DNS load balancing must have two FQDNs: the regular pool FQDN that is used by DNS load balancing (such as pool01.contoso.com), and resolves to the physical IPs of the servers in the pool, and another FQDN for the pool's Web services (such as web01.contoso.com), which resolves to virtual IP address of the pool.
  In Topology Builder, if you want to deploy DNS load balancing for a pool, to create this extra FQDN for the pool's Web services you must select the **Override internal Web Services pool FQDN** check box and type the FQDN, in the **Specify the Web Services URLs for this Pool** page.
- To support the FQDN used by DNS load balancing, you must provision DNS to resolve the pool FQDN (such as pool01.contoso.com) to the IP addresses of all the servers in the pool (for example, 192.168.1.1, 192.168.1.2, and so on). You should include only the IP addresses of servers that are currently deployed.

⚠**Warning:**
If you have more than one Front End pool or Front End Server the external Web services FQDN must be unique. For example, if you define the external Web services FQDN of a Front End Server as **pool01.contoso.com**, you cannot use **pool01.contoso.com** for another Front End pool or Front End Server. If you are also deploying Directors, the external Web services FQDN defined for any Director or Director pool must be unique from any other Director or Director pool as well as any Front End pool or Front End Server. If decide to override the Internal web services with a self-defined FQDN, each FQDN must be unique from any other Front End pool, Director or a Director pool.

DNS Load Balancing on Edge Server Pools

You can deploy DNS load balancing on Edge Server pools. If you do, you must be aware of some considerations.

Using DNS load balancing on your Edge Servers causes a loss of failover ability in the following scenarios:

- Federation with organizations that are running versions of Office Communications Server released prior to Lync Server 2010.
- Instant message exchange with users of public instant messaging (IM) services, such as Windows Live, AOL, and Yahoo!, in addition to XMPP-based providers and servers, such as Google Talk.

Important:
• Google Talk is currently the only supported XMPP partner. • As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013). • The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down. • More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

These scenarios will work as long as all Edge Servers in the pool are up and running, but if one Edge Server is unavailable, any requests for these scenarios that are sent to it will fail, instead of routing to another Edge Server.

Using DNS load balancing also causes a loss of failover ability for these Exchange UM scenarios for remote Exchange UM users:

- Playing their Enterprise Voice voice mail on their phone
- Transferring calls from an Exchange UM Auto Attendant

All other Exchange UM scenarios will work properly.

The internal Edge interface and external Edge interface must use the same type of load balancing. You cannot use DNS load balancing on one Edge interface and hardware load balancing on the other Edge interface.

Deploying DNS Load Balancing on Edge Server Pools

To deploy DNS load balancing on the external interface of your Edge Server pool, you need the following DNS entries:

- For the Access Edge service, you need one entry for each server in the pool. Each entry must resolve the FQDN of the Access Edge service (for example, sip.contoso.com) to the IP address of the Access Edge service on one of the Edge Servers in the pool.
- For the Web Conferencing Edge service, you need one entry for each server in the pool. Each entry must resolve the FQDN of the Web Conferencing Edge service (for example, webconf.contoso.com) to the IP address of the Web Conferencing Edge service on one of the Edge Servers in the pool.
- For the Audio/Video Edge service, you need one entry for each server in the pool. Each entry must resolve the FQDN of the Audio/Video Edge service (for example, av.contoso.com) to the IP address of the A/V Edge service on one of the Edge Servers in the pool.

To deploy DNS load balancing on the internal interface of your Edge Server pool, you must add one DNS A record, which resolves the internal FQDN of the Edge Server pool to the IP address of each server in the pool.

Using DNS Load Balancing on Mediation Server Pools

You can use DNS load balancing on stand-alone Mediation Server pools. All SIP and media traffic is balanced by DNS load balancing.

To deploy DNS load balancing on a Mediation Server pool, you must provision DNS to resolve the pool FQDN (for example, mediationpool1.contoso.com) to the IP addresses of all the servers in the pool (for example, 192.168.1.1, 192.168.1.2, and so on).

Blocking Traffic to a Server With DNS Load Balancing

If you use DNS load balancing and you need to block traffic to a specific computer, it is not sufficient to just remove the IP address entries from the Pool FQDN. You must remove the DNS entry for the computer as well.

Note that for server-to-server traffic, Lync Server 2013 uses topology-aware load balancing. Servers read the published topology in the Central Management store to obtain the FQDNs of servers in the topology, and automatically distribute the traffic among the servers. To block a server from receiving server-to-server traffic, you must remove the server from the topology.

1.3.3.4.8 DNS Requirements for Persistent Chat Servers

DNS Requirements for Persistent Chat Servers

Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2012-06-28*

This section describes the Domain Name System (DNS) records that are required for deployment of Persistent Chat Servers.

DNS Records for Persistent Chat Servers

The following table specifies DNS requirements for Persistent Chat Server deployment.

DNS Requirements for a Persistent Chat Server

Deployment scenario	DNS requirement
One Persistent Chat Server	An internal A record that resolves the fully qualified domain name (FQDN) of the server to its IP address.
Persistent Chat pool	An internal A record that resolves the fully qualified domain name (FQDN) of the servers to its IP address. **Example** PersistentChatServer01.contoso.com 10.10.10.1 PersistentChatServer02.contoso.com 10.10.10.2 An internal A record that resolves the fully qualified domain name (FQDN) of the servers to its IP address. **Example** PersistentChatPool.contoso.com 10.10.10.1 PersistentChatPool.contoso.com 10.10.10.2

1.3.3.4.9 DNS Requirements for Edge Servers and Features

DNS Requirements for Edge Servers and Features

Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2013-01-26*

Lync Server 2013 Edge Servers, Edge pools, and reverse proxies have specific requirements for domain name system (DNS) records. In Lync Server 2013 when IPv4 and IPv6 are in use, you must plan for both host A and AAAA records.

The topics listed below define the use of DNS records for your deployment planning:

- DNS Summary - Single Consolidated Edge with Private IP Addresses Using NAT
- DNS Summary - Single Consolidated Edge with Public IP Addresses
- DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT
- DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses
- DNS Summary - Scaled Consolidated Edge with Hardware Load Balancers
- DNS Summary - Reverse Proxy
- DNS Summary - Lync Server and Office Communications Server Federation
- DNS Summary - Public Instant Messaging Connectivity
- DNS Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

1.3.3.4.9.1 DNS Summary - Single Consolidated Edge with Private IP Addresses Using NAT

DNS Summary - Single Consolidated Edge with Private IP Addresses Using NAT

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-09-08*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about automatic configuration of clients running Lync 2013 if split-brain DNS is not configured, see “Automatic Configuration without Split-Brain DNS” in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the single consolidated edge topology shown in the Single Consolidated Edge Topology figure. Note that certain DNS records are required only for automatic configuration of Lync 2013 and Lync 2010 clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated automatic configuration records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Single Consolidated Edge Topology figure in Single Consolidated Edge with Private IP Addresses and NAT, the default gateway would point to the external firewall (10.45.16.1).

You can configure two network adapters in your Edge Server as follows:

- **Network adapter 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 10.45.16.10 for Access Edge, 10.45.16.20 for Web Conferencing Edge, 10.45.16.30 for AV Edge

  Note:

  It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge, 444/TCP for the Web Conferencing Edge and 443/TCP for the AV Edge might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

  Access Edge IP address is primary with default gateway set to integrated router (10.45.16.1).
  Web conferencing and A/V Edge IP addresses secondary.

Tip:

Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Single Consolidated Edge with Private IP Addresses Using NAT (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20	Web Conferencing Edge external interface
External DNS/A	av.contoso.com	131.107.155.30	A/V Edge external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.

External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of federated partners known as "Allowed SIP Domain" (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users
Internal DNS/A	lsedge.contoso.net	172.25.33.10	Consolidated Edge internal interface

Important:

The records listed in the previous table are shown with either a *.net* extension or a *.com* extension to highlight which zone they need to reside in if you are not using split-brain DNS. If you are using split-brain DNS, all records would be in the same *.com* zone, with the only distinction being whether they are in the internal or external DNS zone version. For details, see "Split-Brain DNS" in Determine DNS Requirements.

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of your federation to other potential federation partners, and is known as "Allowed SIP Domains" (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users **Important:** This SRV record is required for mobility and the push notification clearing house

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat as necessary for all internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An allowed XMPP domain must also be configured in the XMPP Federated Partners policy. See topics in **See Also** for additional details
External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP proxy	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service. Typically, the SRV record that you create will point to this host (A or AAAA) record

1.3.3.4.9.2 DNS Summary - Single Consolidated Edge with Public IP Addresses

DNS Summary - Single Consolidated Edge with Public IP Addresses

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-09-08*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about automatic configuration of clients running Lync 2013 if split-brain DNS is not configured, see “Automatic Configuration without Split-Brain DNS” in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the single consolidated edge topology shown in the Single Consolidated Edge Topology figure. Note that certain DNS records are required only for automatic configuration of Lync 2013 and Lync 2010 clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated automatic configuration records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Single Consolidated Edge Topology with Public IP Addresses figure in Single Consolidated Edge with Public IP Addresses, the default gateway would point to the external router at your Internet perimeter or firewall that can provide a public IP addresses. The network relationship for Edge Server interfaces is a route relationship instead of a NAT relationship.

You can configure two network adapters in your Edge Server as follows:

- **Network adapter 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 (External Interface)**
  Three public IP addresses are assigned to this network adapter, for example 131.107.155.10 for Access Edge, 131.107.155.20 for Web Conferencing Edge, 131.107.155.30 for AV Edge.

  > **Note:**
  > It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge, 444/TCP for the Web Conferencing Edge and 443/TCP for the AV Edge might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

  The Access Edge public IP address is primary with default gateway set to the public router (131.107.155.1).
  Web conferencing and A/V Edge public IP addresses are additional IP addresses in the **Advanced** section of the properties of **Internet Protocol**

Version 4 (TCP/IPv4) and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.

Tip:

Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Single Consolidated Edge with Public IP Addresses (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20	Web Conferencing Edge external interface
External DNS/A	av.contoso.com	131.107.155.30	A/V Edge external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of federated partners known as "Allowed SIP Domain" (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users
Internal DNS/A	lsedge.contoso.net	172.25.33.10	Consolidated Edge internal interface

Important:

The records listed in the previous table are shown with either a *.net* extension or a *.com* extension to highlight which zone they need to reside in if you are not using split-brain DNS. If you are using split-brain DNS, all records would be in the same zone, with the only distinction being whether they are in the internal or external version. For details, see "Split-Brain DNS" in Determine DNS Requirements.

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of your federation to other potential federation partners, and is known as "Allowed SIP Domains" (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users ◆**Important:** This SRV record is required for mobility and the push notification clearing house

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat as necessary for all

			internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An allowed XMPP domain must also be configured in the XMPP Federated Partners policy. See topics in **See Also** for additional details
External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP proxy	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service. Typically, the SRV record that you create will point to this host (A or AAAA) record

1.3.3.4.9.3 DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-09-08*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about configuring automatic configuration of Lync 2013 clients if split-brain DNS is not configured, see the "Automatic Configuration without Split Brain DNS" section in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the single consolidated edge topology shown in the Single Consolidated Edge Topology figure. Note that certain DNS records are required only for automatic configuration of Lync 2013 clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Scaled Consolidated Edge Scenario figure in Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT, the default gateway would point to the external firewall.

You can configure two network adapters in each of your Edge Server as follows:

- **Network adapter 1 - Node 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 1 - Node 2 (Internal Interface)**
  Internal interface with 172.25.33.11 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 Node 1 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 10.45.16.10 for Access Edge, 10.45.16.20 for Web Conferencing Edge, 10.45.16.30 for AV Edge.

  Note:
  It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge, 444/TCP for the Web Conferencing Edge and 443/TCP for the AV Edge might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

  The Access Edge public IP address is primary with default gateway set to the integrated router (10.45.16.1).
  Web conferencing and A/V Edge private IP addresses are additional IP addresses in the **Advanced** section of the properties of **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.
- **Network adapter 2 Node 2 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 10.45.16.11 for Access Edge, 10.45.16.21 for Web Conferencing Edge, 10.45.16.31 for AV Edge.
  The Access Edge public IP address is primary with default gateway set to the integrated router (10.45.16.1).
  Web conferencing and A/V Edge private IP addresses are additional IP addresses in the **Advanced** section of the properties of **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.

Tip:
Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct

network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10 and 131.107.155.11	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20 and 131.107.155.21	Web Conferencing Edge external interface
External DNS/A	av.contoso.com	131.107.155.30 and 131.107.155.31	A/V Edge external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface. Required for automatic DNS discovery of federated partners known as “Allowed SIP Domain” (called enhanced federation in previous releases). Repeat as necessary for all SIP domains with Lync enabled users
Internal DNS/A	lsedge.contoso.net	172.25.33.10 and 172.25.33.11	Consolidated Edge internal interface

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of your

			federation to other potential federation partners, and is known as "Allowed SIP Domains" (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users **Important:** This SRV record is required for mobility and the push notification clearing house

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat as necessary for all internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An

			allowed XMPP domain must also be configured in the XMPP Federated Partners policy. See topics in **See Also** for additional details
External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP proxy	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service. Typically, the SRV record that you create will point to this host (A or AAAA) record

1.3.3.4.9.4 DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-10-20*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about configuring automatic configuration of Lync 2013 clients if split-brain DNS is not configured, see the "Automatic Configuration without Split Brain DNS" section in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the single consolidated edge topology shown in the Single Consolidated Edge Topology figure. Note that certain DNS records are required only for automatic configuration of Lync 2013 clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Scaled Consolidated Edge Scenario figure in Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses , the default gateway would point to the external firewall.

You can configure two network adapters in each of your Edge Server as follows:

- **Network adapter 1 - Node 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 1 - Node 2 (Internal Interface)**
  Internal interface with 172.25.33.11 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 Node 1 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 131.107.155.10 for Access Edge service, 131.107.155.20 for Web Conferencing Edge service, 131.107.155.30 for A/V Edge service.
  The Access Edge service public IP address is primary with default gateway set to the public router (131.107.155.1).
  Web Conferencing Edge service and A/V Edge service private IP addresses are additional IP addresses in the **Advanced** section of the properties of **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.

  Note:

  It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge service, 444/TCP for the Web Conferencing Edge service and 443/TCP for the A/V Edge service might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

- **Network adapter 2 Node 2 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 131.107.155.11 for Access Edge service, 131.107.155.21 for Web Conferencing Edge service, 131.107.155.31 for A/V Edge service.
  The Access Edge service public IP address is primary with default gateway set to the public router (131.107.155.1).
  Web Conferencing Edge service and A/V Edge service private IP addresses are additional IP addresses in the **Advanced** section of the properties of **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.

Tip:

Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10 and 131.107.155.11	Access Edge service external interface (Contoso) Repeat as necessary for all SIP

			domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20 and 131.107.155.21	Web Conferencing Edge service external interface
External DNS/A	av.contoso.com	131.107.155.30 and 131.107.155.31	A/V Edge service external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge service external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	Access Edge service external interface Required for automatic DNS discovery of federated partners known as "Allowed SIP Domain" (called enhanced federation in previous releases). Repeat as necessary for all SIP domains with Lync enabled users
Internal DNS/A	lsedge.contoso.net	172.25.33.10 and 172.25.33.11	Consolidated Edge internal interface

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge service external interface Required for automatic DNS discovery of your federation to other potential federation partners, and is known as "Allowed SIP Domains" (called enhanced federation in previous releases). ◆**Important:**

			Repeat as necessary for all SIP domains with Lync enabled users and Microsoft Lync Mobile clients that use either the Push Notification Service or the Apple Push Notification service

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge service external interface (Contoso)Repeat as necessary for all SIP domains with Lync enabled users

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat as necessary for all internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An allowed XMPP domain must also be configured in the XMPP Federated Partners policy. See topics in **See Also** for additional details

External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP proxy	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service. Typically, the SRV record that you create will point to this host (A or AAAA) record

1.3.3.4.9.5 DNS Summary - Scaled Consolidated Edge w ith Hardw are Load Balancers

DNS Summary - Scaled Consolidated Edge with Hardware Load Balancers

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2013-01-27*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about configuring automatic configuration of Lync 2013 clients if split-brain DNS is not configured, see the "Automatic Configuration without Split Brain DNS" section in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the Scaled Consolidated Edge Topology (Hardware Load Balanced) figure. Note that certain DNS records are required only for automatic configuration for Lync clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Scaled Consolidated Edge Scenario figure in Scaled Consolidated Edge with Hardware Load Balancers, the default gateway would point to the external firewall.

You can configure two network adapters in each of your Edge Servers as follows:

- **Network adapter 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway.
  Ensure there is a route from the network containing the Edge Server internal interface to any networks that contain Lync Server clients or servers running Lync Server (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 (External Interface)**
  Three public IP addresses are assigned to this network adapter, for example 131.107.155.10 for Access Edge service, 131.107.155.20 for Web

Conferencing Edge service, 131.107.155.30 for A/V Edge service.

Note:

The IP addresses that are assigned to the actual external network interfaces of the Edge Server may depend on which hardware load balancer you choose. Refer to the documentation for your hardware load balancer to understand the actual IP address requirements.
It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge service, 444/TCP for the Web Conferencing Edge service and 443/TCP for the A/V Edge service might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

Access Edge service IP address is primary with default gateway set to Internet-facing router (131.107.155.1).
Web Conferencing Edge service and A/V Edge service IP addresses secondary.

Tip:

Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Scaled Consolidated Edge, Hardware Load Balanced (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10	Access Edge service external interface (Contoso). Repeat as necessary for all SIP domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20	Web Conferencing Edge service external interface
External DNS/A	av.contoso.com	131.107.155.30	A/V Edge service external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge service external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge service external interface Required for

			automatic DNS discovery of federated partners known as "Allowed SIP Domain" (called enhanced federation in previous releases). Repeat as necessary for all SIP domains with Lync enabled users and Microsoft Lync Mobile clients that use either the Push Notification Service or the Apple Push Notification service
Internal DNS/A	lsedge.contoso.net	172.25.33.10	Consolidated Edge internal interface

1.3.3.4.9.6 DNS Summary - Reverse Proxy

DNS Summary - Reverse Proxy

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-10-31*

You configure two network adapters in your reverse proxy as follows:

Reverse Proxy Network Adapter Requirements

- **Network adapter 1 (Internal Interface)** example
  Internal interface with 172.25.33.40 assigned.
  No default gateway is defined.
  Ensure there is a route from the network containing the reverse proxy internal interface to any networks that contain Lync Server Front End pool servers (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 (External Interface)** example
  A minimum of one public IP address is assigned to this network adapter.
  Gateway is defined to point to the router or integrated firewall in your outer perimeter. (10.45.16.1 in the scenario examples)

DNS Records Required for Reverse Proxy

Location/TYPE/Port	FQDN	IP address	Maps to/comments
External DNS/A	webext.contoso.com	Assigned listener for externally published resources	External web services from the internal deployment. Additional records can be defined and created for all pools and single servers for any SIP

			domain that will use this reverse proxy, and has defined external web services.
External DNS/A	webdirext.contoso.com	Assigned listener for externally published resources	External web services for the Directors or Director pools in your deployment. You can define as many Directors as there are distinct Directors, of which may be associated with other SIP domains. ◆**Important:** Defining the DNS records for and publishing the Directors is not an either the Front End pool or the Director decision. You must define and publish both the Director and the Front End pool external web services if you are using Directors. Specific traffic types (for authentication and other uses) will be sent to the Director first, if it is defined in the topology.
External DNS/A	dialin.contoso.com	Assigned listener for externally published resources	Dial-in conferencing published externally
External DNS/A	meet.contoso.com	Assigned listener for externally published resources	Conferences published externally
External DNS/A	officewebapps01.contoso.com	Assigned listener for Office Web Apps Server	Office Web Apps Server deployed internally or in the perimeter, and published for external client access
External DNS/A	lyncdiscover.contoso.com	Assigned listener for externally published resources	Lync Discover External record for externally published AutoDiscover, and includes Mobility, Microsoft Lync Web App, and scheduler Web app

External DNS/A	lsrp.contoso.com	Assigned listener for externally published resources	Reference record for the reverse proxy external name

1.3.3.4.9.7 DNS Summary - Lync Server and Office Communications Server Federation

DNS Summary - Lync Server and Office Communications Server Federation

See Also

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-10-20*

The domain name system (DNS) records that will be required for defining a federation with Office Communications Server or Lync Server partners is determined by your decision to either allow automatic DNS discovery of your domain by other perspective partners. If you publish the _sipfederationtls._tcp. <*SIP domain name*> SRV record, any other SIP federated domain will be able to “discover” your federation. You can control which federated domains can communicate with you by using the Allows domains and Blocked Domains settings in the Lync Server Control Panel, or by setting the allowed or blocked domains configuration using the Lync Server Management Shell and the **Get**, **Set**, **New**, **Remove-CsAllowedDomain** and **-CsBlockedDomain** PowerShell cmdlets. For additional information on how to configure theses settings and the use of the PowerShell cmdlets, see **Related Topics** at the end of this topic.

The DNS records summary table depicts the required entries for an open, or discoverable, federation. If you do not want to implement Federation Discovery, You can decide to not configure the _sipfederationtls._tcp. <*SIP domain name*> record.

Important:

There are specific scenarios in which you must have the _sipfederationtls._tcp. <*SIP domain name*> SRV record, but you do not want to have a discoverable federation. One such instance is where you have deployed mobility for your users. The mobility push notification clearinghouse (PNCH) is a special type of federation that is used for Microsoft Lync Mobile clients on Apple iPhone or Windows Phone. The _sipfederationtls._tcp. <*SIP domain name*> SRV record is used in the case of mobility and PNCH. To mitigate this issue and control your discoverability, clear the setting **Enable partner domain discovery** to turn off discovery.

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	Access Edge service external interface Required for automatic DNS discovery of your federation to other potential federation partners, and is known as “Allowed SIP Domains” (called enhanced federation in

			previous releases).Repeat as necessary for all SIP domains with Lync enabled users **Important:** This SRV record is required for mobility and the push notification clearing house. In cases where there is more than one SIP domain, create and publish an SRV record for each domain that will have Lync Mobile clients. The Push Notification Service and Apple Push Notification service may not operate as expected if there is not an explicit SRV record for each SIP domain that the deployment supports.

⊟See Also

Tasks

Configuring for Push Notifications
Enable or Disable Discovery of Federation Partners

Other Resources

Manage SIP Federated Domains for Your Organization

1.3.3.4.9.8 DNS Summary - Public Instant Messaging Connectivity

DNS Summary - Public Instant Messaging Connectivity

See Also

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2013-02-16*

When you configure domain name system (DNS) for public instant messaging connectivity, you will find that the configuration that supports external users will support public IM connectivity. If you have already configured your Edge Server or Edge pool, you should have the DNS records necessary to support public IM connectivity.

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments

External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge service external interface (Contoso). Repeat as necessary for all SIP domains with Lync enabled users.

See Also

Concepts

Scenarios for External User Access

1.3.3.4.9.9 DNS Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

DNS Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

See Also

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-10-20*

To configure extensible messaging and presence protocol (XMPP) for your deployment, you create two domain name system (DNS) records in an external DNS server that will resolve the records to the Access Edge service of your Edge Server or Edge pool.

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat as necessary for all internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An allowed XMPP domain must also be configured in the XMPP Federated

			Partners policy. See topics in **See Also** for additional details
External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP proxy	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service. Typically, the SRV record that you create will point to this host (A or AAAA) record

⊟See Also

Tasks

Setting Up XMPP Federation

Concepts

Determine DNS Requirements

1.3.3.5 Port Requirements

Port Requirements

Microsoft Lync Server 2013 > Planning > Network Planning for Lync Server >

Topic Last Modified: *2012-11-16*

Lync Server requires that specific ports on the firewall be open. Additionally, if Internet Protocol security (IPsec) is deployed in your organization, IPsec must be disabled over the range of ports used for the delivery of audio, video, and panorama video.

This section includes the following topics:

- Ports and Protocols for Internal Servers
- IPsec Exceptions
- Port Summary - Single Consolidated Edge with Private IP Addresses Using NAT
- Port Summary - Single Consolidated Edge with Public IP Addresses
- Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT
- Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses
- Port Summary - Scaled Consolidated Edge with Hardware Load Balancers
- Port Summary - Reverse Proxy
- Port Summary - Lync Server and Office Communications Server Federation
- Port Summary - Public Instant Messaging Connectivity
- Port Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

1.3.3.5.1 Ports and Protocols for Internal Servers

Ports and Protocols for Internal Servers

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-12-12*

This section summarizes the ports and protocols used by servers, load balancers, and clients in a Lync Server deployment.

Port and Protocol Details

Note:

Windows Firewall must be running before you start the Lync Server services on a server, because that is when Lync Server opens the required ports in the firewall.

For details about firewall configuration for edge components, see Determine External A/V Firewall and Port Requirements.

The following table lists the ports that need to be open on each internal server role.

Required Server Ports (by Server Role)

Server role	Service name	Port	Protocol	Notes
All Servers	SQL Browser	1434	UDP	SQL Browser for the local replicated copy of the the Central Management Store database.
Front End Servers	Lync Server Front-End service	5060	TCP	Optionally used by Standard Edition servers and Front End Servers for static routes to trusted services, such as remote call control servers.
Front End Servers	Lync Server Front-End service	5061	TCP (TLS)	Used by Standard Edition servers and Front End pools for all internal SIP communications between servers (MTLS), for SIP communications between Server and Client (TLS) and for SIP communications between Front End Servers and Mediation Servers (MTLS). Also used for communications with Monitoring Server.
Front End Servers	Lync Server Front-End service	444	HTTPS TCP	Used for HTTPS communication between the Focus (the Lync

				Server component that manages conference state) and the individual servers. This port is also used for TCP communication between Survivable Branch Appliances and Front End Servers.
Front End Servers	Lync Server Front-End service	135	DCOM and remote procedure call (RPC)	Used for DCOM based operations such as Moving Users, User Replicator Synchronization, and Address Book Synchronization.
Front End Servers	Lync Server IM Conferencing service	5062	TCP	Used for incoming SIP requests for instant messaging (IM) conferencing.
Front End Servers	Lync Server Web Conferencing service	8057	TCP (TLS)	Used to listen for Persistent Shared Object Model (PSOM) connections from client.
Front End Servers	Lync Server Web Conferencing Compatibility service	8058	TCP (TLS)	Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Lync Server.
Front End Servers	Lync Server Audio/Video Conferencing service	5063	TCP	Used for incoming SIP requests for audio/video (A/V) conferencing.
Front End Servers	Lync Server Audio/Video Conferencing service	57501-65335	TCP/UDP	Media port range used for video conferencing.
Front End Servers	Lync Server Web Compatibility	80	HTTP	Used for communication

	service			from Front End Servers to the web farm FQDNs (the URLs used by IIS web components) when HTTPS is not used.
Front End Servers	Lync Server Web Compatibility service	443	HTTPS	Used for communication from Front End Servers to the web farm FQDNs (the URLs used by IIS web components).
Front End Servers	Lync Server Web Compatibility service	8080	TCP and HTTP	Used by web components for external access.
Front End Servers	Web server component	4443	HTTPS	
Front End Servers	Web server component	8060	TCP (MTLS)	
Front End Servers	Web server component	8061	TCP (MTLS)	
Front End Servers	Mobility Services component	5086	TCP (MTLS)	SIP port used by Mobility Services internal processes
Front End Servers	Mobility Services component	5087	TCP (MTLS)	SIP port used by Mobility Services internal processes
Front End Servers	Mobility Services component	443	HTTPS	
Front End Servers	Lync Server Conferencing Attendant service (dial-in conferencing)	5064	TCP	Used for incoming SIP requests for dial-in conferencing.
Front End Servers	Lync Server Conferencing Attendant service (dial-in conferencing)	5072	TCP	Used for incoming SIP requests for Attendant (dial in conferencing).
Front End Servers that also run a Collocated Mediation Server	Lync Server Mediation service	5070	TCP	Used by the Mediation Server for incoming requests from the Front End

				Server to the Mediation Server.
Front End Servers that also run a Collocated Mediation Server	Lync Server Mediation service	5067	TCP (TLS)	Used for incoming SIP requests from the PSTN gateway to the Mediation Server.
Front End Servers that also run a Collocated Mediation Server	Lync Server Mediation service	5068	TCP	Used for incoming SIP requests from the PSTN gateway to the Mediation Server.
Front End Servers that also run a Collocated Mediation Server	Lync Server Mediation service	5081	TCP	Used for outgoing SIP requests from the Mediation Server to the PSTN gateway.
Front End Servers that also run a Collocated Mediation Server	Lync Server Mediation service	5082	TCP (TLS)	Used for outgoing SIP requests from the Mediation Server to the PSTN gateway.
Front End Servers	Lync Server Application Sharing service	5065	TCP	Used for incoming SIP listening requests for application sharing.
Front End Servers	Lync Server Application Sharing service	49152-65335	TCP	Media port range used for application sharing.
Front End Servers	Lync Server Conferencing Announcement service	5073	TCP	Used for incoming SIP requests for the Lync Server Conferencing Announcement service (that is, for dial-in conferencing).
Front End Servers	Lync Server Call Park service	5075	TCP	Used for incoming SIP requests for the Call Park application.
Front End Servers	Lync Server Audio Test service	5076	TCP	Used for incoming SIP requests for the Audio Test service.
Front End Servers	Not applicable	5066	TCP	Used for outbound

				Enhanced 9-1-1 (E9-1-1) gateway.
Front End Servers	Lync Server Response Group service	5071	TCP	Used for incoming SIP requests for the Response Group application.
Front End Servers	Lync Server Response Group service	8404	TCP (MTLS)	Used for incoming SIP requests for the Response Group application.
Front End Servers	Lync Server Bandwidth Policy Service	5080	TCP	Used for call admission control by the Bandwidth Policy service for A/V Edge TURN traffic.
Front End Servers	Lync Server Bandwidth Policy Service	448	TCP	Used for call admission control by the Lync Server Bandwidth Policy Service.
Front End Servers where the Central Management store resides	Lync Server Master Replicator Agent service	445	TCP	Used to push configuration data from the Central Management store to servers running Lync Server.
All Servers	SQL Browser	1434	UDP	SQL Browser for local replicated copy of Central Management store data in local SQL Server instance
All internal servers	Various	49152-57500	TCP/UDP	Media port range used for audio conferencing on all internal servers. Used by all servers that terminate audio: Front End Servers (for Lync Server Conferencing Attendant service, Lync Server Conferencing

				Announcement service, and Lync Server Audio/ Video Conferencing service), and Mediation Server.
Directors	Lync Server Front-End service	5060	TCP	Optionally used for static routes to trusted services, such as remote call control servers.
Directors	Lync Server Front-End service	444	HTTPS TCP	Inter-server communication between Front End and Director. Additionally, client certificate publish (to Front End Servers) or validate if the client certificate has already been published.
Directors	Lync Server Web Compatibility service	80	TCP	Used for initial communication from Directors to the web farm FQDNs (the URLs used by IIS web components). In normal operation, will switch to HTTPS traffic, using port 443 and protocol type TCP.
Directors	Lync Server Web Compatibility service	443	HTTPS	Used for communication from Directors to the web farm FQDNs (the URLs used by IIS web components).
Directors	Lync Server Front-End service	5061	TCP	Used for internal communications between servers and for client connections.
Mediation Servers	Lync Server Mediation service	5070	TCP	Used by the Mediation Server for incoming requests from

				the Front End Server.
Mediation Servers	Lync Server Mediation service	5067	TCP (TLS)	Used for incoming SIP requests from the PSTN gateway.
Mediation Servers	Lync Server Mediation service	5068	TCP	Used for incoming SIP requests from the PSTN gateway.
Mediation Servers	Lync Server Mediation service	5070	TCP (MTLS)	Used for SIP requests from the Front End Servers.
Persistent Chat Front End Server	Persistent Chat SIP	5041	TCP (MTLS)	
Persistent Chat Front End Server	Persistent Chat Windows Communication Foundation (WCF)	881	TCP (TLS) and TCP (MTLS)	
Persistent Chat Front End Server	Persistent Chat File Transfer Service	443	TCP (TLS)	

Note:

Some remote call control scenarios require a TCP connection between the Front End Server or Director and the PBX. Although Lync Server no longer uses TCP port 5060, during remote call control deployment you create a trusted server configuration, which associates the RCC Line Server FQDN with the TCP port that the Front End Server or Director will use to connect to the PBX system. For details, see the **CsTrustedApplicationComputer** cmdlet in the Lync Server Management Shell documentation.

For your pools that use only hardware load balancing (not DNS load balancing), the following table shows the ports that need to open the hardware load balancers.

Hardware Load Balancer Ports if Using Only Hardware Load Balancing

Load Balancer	Port	Protocol
Front End Server load balancer	5061	TCP (TLS)
Front End Server load balancer	444	HTTPS
Front End Server load balancer	135	DCOM and remote procedure call (RPC)
Front End Server load balancer	80	HTTP
Front End Server load balancer	8080	TCP - Client and device retrieval of root certificate from Front End Server –

		clients and devices authenticated by NTLM
Front End Server load balancer	443	HTTPS
Front End Server load balancer	4443	HTTPS (from reverse proxy)
Front End Server load balancer	5072	TCP
Front End Server load balancer	5073	TCP
Front End Server load balancer	5075	TCP
Front End Server load balancer	5076	TCP
Front End Server load balancer	5071	TCP
Front End Server load balancer	5080	TCP
Front End Server load balancer	448	TCP
Mediation Server load balancer	5070	TCP
Front End Server load balancer (if the pool also runs Mediation Server)	5070	TCP
Director load balancer	443	HTTPS
Director load balancer	444	HTTPS
Director load balancer	5061	TCP
Director load balancer	4443	HTTPS (from reverse proxy)

Your Front End pools and Director pools that use DNS load balancing also must have a hardware load balancer deployed. The following table shows the ports that need to be open on these hardware load balancers.

Hardware Load Balancer Ports if Using DNS Load Balancing

Load Balancer	Port	Protocol
Front End Server load balancer	80	HTTP
Front End Server load balancer	443	HTTPS
Front End Server load balancer	8080	TCP - Client and device retrieval of root certificate from Front End Server – clients and devices authenticated by NTLM
Front End Server load balancer	4443	HTTPS (from reverse proxy)
Director load balancer	443	HTTPS

Director load balancer	444	HTTPS
Director load balancer	4443	HTTPS (from reverse proxy)

Required Client Ports

Component	Port	Protocol	Notes
Clients	67/68	DHCP	Used by Lync Server to find the Registrar FQDN (that is, if DNS SRV fails and manual settings are not configured).
Clients	443	TCP (TLS)	Used for client-to-server SIP traffic for external user access.
Clients	443	TCP (PSOM/TLS)	Used for external user access to web conferencing sessions.
Clients	443	TCP (STUN/MSTURN)	Used for external user access to A/V sessions and media (TCP)
Clients	3478	UDP (STUN/MSTURN)	Used for external user access to A/V sessions and media (TCP)
Clients	5061	TCP (MTLS)	Used for client-to-server SIP traffic for external user access.
Clients	6891-6901	TCP	Used for file transfer between Lync clients and previous clients (clients of Microsoft Office Communications Server 2007 R2, Microsoft Office Communications Server 2007, and Live Communications Server 2005).
Clients	1024-65535 *	TCP/UDP	Audio port range (minimum of 20 ports required)
Clients	1024-65535 *	TCP/UDP	Video port range (minimum of 20 ports required).
Clients	1024-65535 *	TCP	Peer-to-peer file transfer (for conferencing file

			transfer, clients use PSOM).
Clients	1024-65535 *	TCP	Application sharing.
Aastra 6721ip common area phone Aastra 6725ip desk phone HP 4110 IP Phone (common area phone) HP 4120 IP Phone (desk phone) Polycom CX500 IP common area phone Polycom CX600 IP desk phone Polycom CX700 IP desk phone Polycom CX3000 IP conference phone	67/68	DHCP	Used by the listed devices to find the Lync Server certificate, provisioning FQDN, and Registrar FQDN.

***** To configure specific ports for these media types, use the CsConferencingConfiguration cmdlet (ClientMediaPortRangeEnabled, ClientMediaPort, and ClientMediaPortRange parameters).

Note:

The set programs for Lync clients automatically create the required operating-system firewall exceptions on the client computer.

Note:

The ports that are used for external user access are required for any scenario in which the client must traverse the organization’s firewall (for example, any external communications or meetings hosted by other organizations).

1.3.3.5.2 IPsec Exceptions

IPsec Exceptions

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-06-27*

For enterprise networks where Internet Protocol security (IPsec) (see IETF RFC 4301-4309) has been deployed, IPsec must be disabled over the range of ports used for the delivery of audio, video, and panorama video. The recommendation is motivated by the need to avoid any delay in the allocation of media ports due to IPsec negotiation.

The following table explains the recommended IPsec exception settings.

Recommended IPsec Exceptions

Rule name	Source IP	Destination IP	Protocol	Source port	Destination port	Authentication Requirement
A/V Edge Server Internal Inbound	Any	A/V Edge Server Internal	UDP and TCP	Any	Any	Do not authenticate
A/V Edge Server External Inbound	Any	A/V Edge Server External	UDP and TCP	Any	Any	Do not authenticate
A/V Edge Server Internal Outbound	A/V Edge Server Internal	Any	UDP & TCP	Any	Any	Do not authenticate
A/V Edge Server External Outbound	A/V Edge Server External	Any	UDP and TCP	Any	Any	Do not authenticate
Mediation Server Inbound	Any	Mediation Server(s)	UDP and TCP	Any	Any	Do not authenticate
Mediation Server Outbound	Mediation Server(s)	Any	UDP and TCP	Any	Any	Do not authenticate
Conferencing Attendant Inbound	Any	Front End Server running Conferencing Attendant	UDP and TCP	Any	Any	Do not authenticate
Conferencing Attendant Outbound	Front End Server running Conferencing Attendant	Any	UDP and TCP	Any	Any	Do not authenticate
A/V Conferencing Inbound	Any	Front End Servers	UDP and TCP	Any	Any	Do not authenticate
A/V Conferencing Outbound	Front End Servers	Any	UDP and TCP	Any	Any	Do not authenticate
Exchange Inbound	Any	Exchange Unified Messaging	UDP and TCP	Any	Any	Do not authenticate
Application Sharing Servers Inbound	Any	Application Sharing Servers	TCP	Any	Any	Do not authenticate

Application Sharing Server Outbound	Application Sharing Servers	Any	TCP	Any	Any	Do not authenticate
Exchange Outbound	Exchange Unified Messaging	Any	UDP and TCP	Any	Any	Do not authenticate
Clients	Any	Any	UDP	Specified media port range	Any	Do not authenticate

1.3.3.5.3 Port Summary - Single Consolidated Edge with Private IP Addresses Using NAT

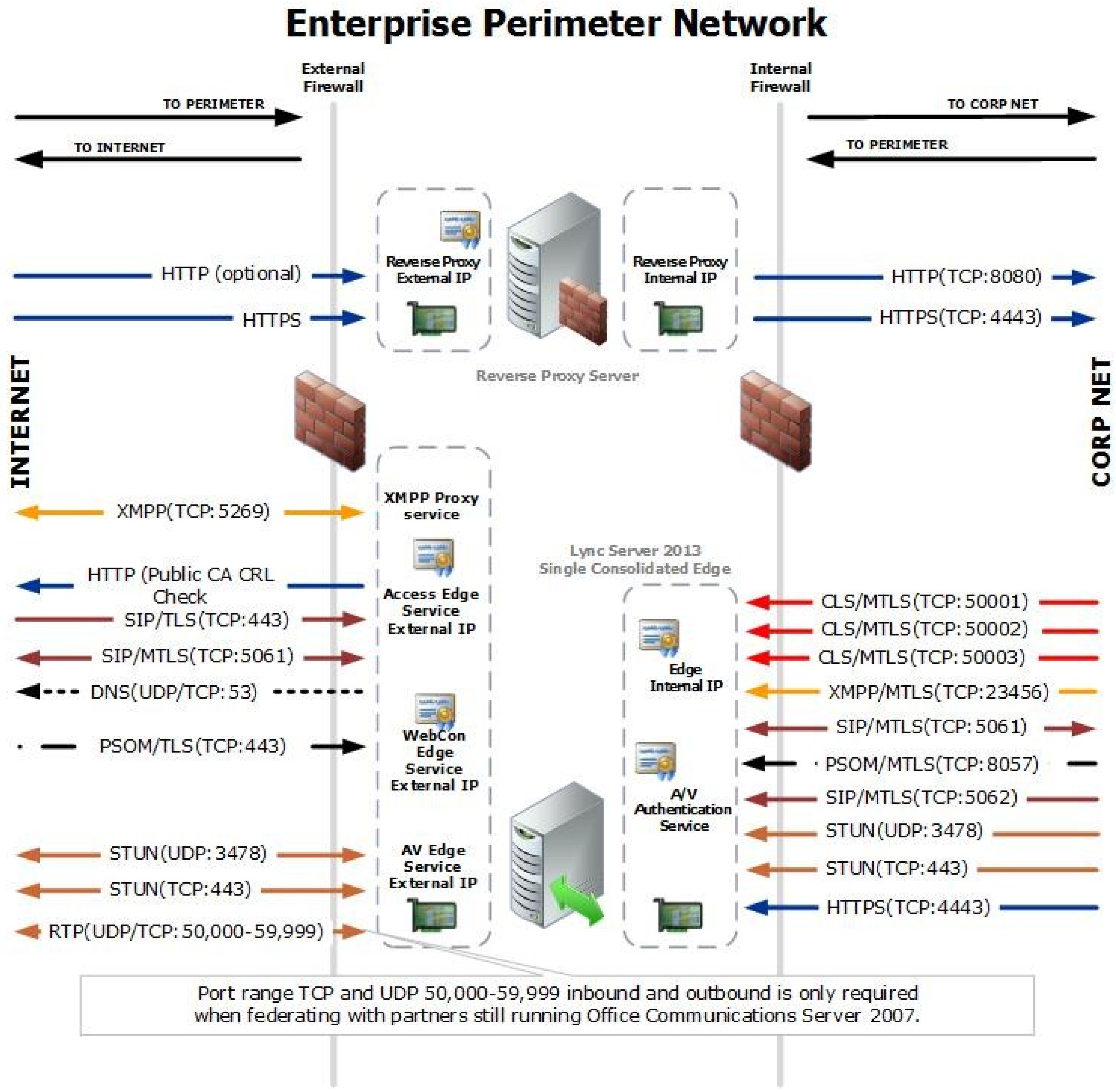
Port Summary - Single Consolidated Edge with Private IP Addresses Using NAT

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2013-02-22*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.



Port and Protocol Details

We recommend that you open only the ports required to support the functionality for which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bi-directionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V), and federation.

Firewall Summary for Single Consolidated Edge with Private IP Addresses using NAT: External Interface

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP

			federations
Access/HTTP/TCP/80	Edge Server Access Edge service	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service	Any	DNS query over UDP
Access/SIP(TLS)/ TCP/443	Any	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Any	For federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)/TCP/443	Any	Edge Server Web Conferencing Edge service	Web Conferencing media
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-59,999	Edge Server A/V Edge service	Any	Required only for federation with partners running Office Communications Server 2007.
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service	Required only for federation with partners running Office Communications Server 2007
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service	Required only for federation with partners running Office Communications Server 2007
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service	Any	3478 outbound is used to determine

			the version of Edge Server that Lync Server is communicating with and also for media traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/ UDP/3478	Any	Edge Server A/V Edge service	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/ TCP/443	Any	Edge Server A/V Edge service	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/ TCP/443	Edge Server A/V Edge service	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Single Consolidated Edge with Private IP Addresses Using NAT: Internal Interface

Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Comments
XMPP/MTLS/ TCP/23456	Any (can be defined as Standard Edition server IP, Standard Edition server IP address, or pool IP address running the XMPP Gateway service)	Edge Server internal interface	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
SIP/MTLS/TCP/5061	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Edge Server internal interface	Outbound SIP traffic (from Director, Director pool IP address, Front End Server or Front End pool IP address) to Edge Server internal interface
SIP/MTLS/TCP/5061	Edge Server internal interface	Any (can be defined as Director, Director pool IP address, Front End Server or Front	Inbound SIP traffic (to Director, Director pool IP address, Front End Server or Front End

		End pool IP address)	pool IP address) from Edge Server internal interface
PSOM/MTLS/TCP/8057	Any (can be defined as Front End Server IP address, or each Front End Server IP address in a Front End pool)	Edge Server internal interface	Web conferencing traffic from Front End Server or each Front End Server if in a pool, to Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server internal interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/ UDP/3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server
STUN/MSTURN/ TCP/443	Any	Edge Server internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server if UDP communication cannot be established, TCP is used for file transfer and desktop sharing
HTTPS/TCP/4443	Any (can be defined as the Front End Server IP address, or pool that holds the Central Management store)	Edge Server internal interface	Replication of changes from the Central Management store to the Edge Server
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line

			(ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Access Edge service public IP address	Any	For federated and public IM connectivity using SIP

Firewall Summary – Public Instant Messaging Connectivity

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Public IM connectivity partners	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Public IM connectivity partners	For federated and public IM connectivity using SIP
Access/SIP(TLS)/ TCP/443	Clients	Edge Server Access Edge service	Client-to-server SIP traffic for external

			user access
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/UDP/3478	Edge Server A/V Edge service	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger
A/V/STUN,MSTURN/UDP/3478	Live Messenger clients	Edge Server A/V Edge service	Required for public IM connectivity with Windows Live Messenger

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Edge Server Access Edge serviceinterface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Edge Server Access Edge service interface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from the Edge Server XMPP proxy to federated XMPP partners
XMPP/MTLS/TCP/23456	Any	Each internal Edge Server Interface IP	Internal XMPP traffic from the XMPP Gateway on the Front End Server or Front End pool to the Edge Server internal IP address or each Edge pool member’s internal IP address

1.3.3.5.4 Port Summary - Single Consolidated Edge w ith Public IP Addresses

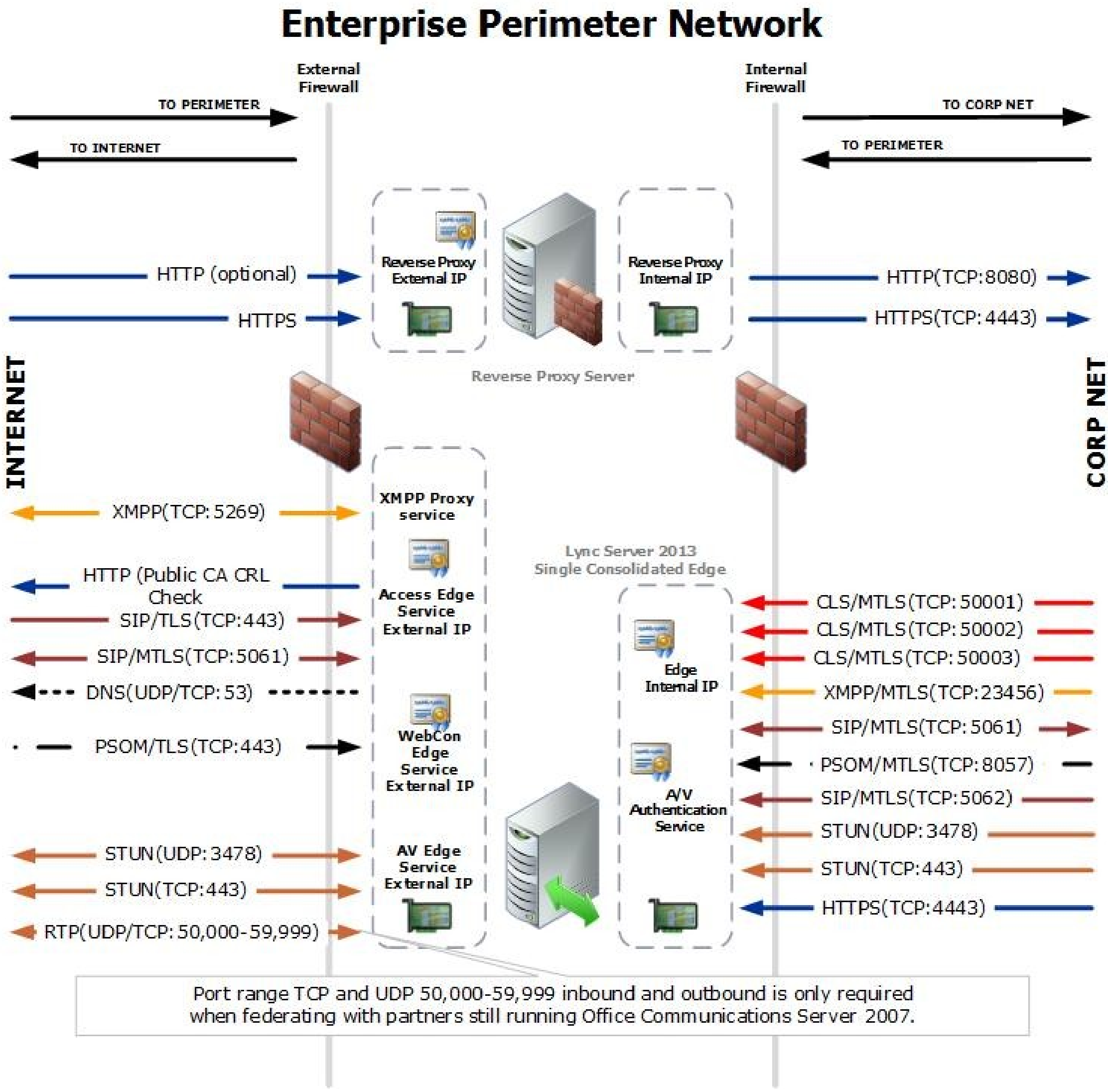
Port Summary - Single Consolidated Edge with Public IP Addresses

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2013-02-21*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool. Planning information for the reverse proxy and federation are found in Scenarios for Reverse Proxy and Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation sections, respectively.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.



Port range TCP and UDP 50,000-59,999 inbound and outbound is only required when federating with partners still running Office Communications Server 2007.

Port and Protocol Details

We recommend that you open only the ports required to support the functionality for which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bidirectionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V) and federation.

Firewall Summary for Single Consolidated Edge with Public IP Addresses: External Interface

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations
Access/HTTP/TCP/80	Edge Server Access Edge service public IP address	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service public IP address	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service public IP address	Any	DNS query over UDP
Access/SIP(TLS)/ TCP/443	Any	Edge Server Access Edge service public IP address	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Edge Server Access Edge service public IP address	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service public IP address	Any	For federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)/TCP/443	Any	Edge Server Web Conferencing Edge service public IP address	Web Conferencing media
A/V/RTP/TCP/50,000-59,999	Edge Server Access Edge service public IP address	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-59,999	Edge Server A/V Edge service public IP address	Any	Required only for federation with partners running Office Communications

			Server 2007
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007.
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007.
A/V/STUN,MSTURN/UDP/3478	Edge Server A/V Edge service public IP address	Any	3478 outbound is used to determine the version of Edge Server that Lync Server is communicating with and also for media traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/UDP/3478	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/TCP/443	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/TCP/443	Edge Server A/V Edge service public IP address	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Single Consolidated Edge with Public IP Addresses: Internal Interface

Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Comments
XMPP/MTLS/TCP/23456	Any (can be defined as Standard Edition server IP, Standard Edition server IP	Edge Server internal interface	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or

	address, or pool IP address running the XMPP Gateway service)		Front End pool
SIP/MTLS/TCP/5061	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Edge Server IP, or pool that holds the internal interface	Outbound SIP traffic (from Director, Director pool IP address, Front End Server or Front End pool IP address) to Edge Server internal interface
SIP/MTLS/TCP/5061	Edge Server internal interface	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool address)	Inbound SIP traffic (to Director, Director pool IP address, Front End Server or Front End pool IP address) from Edge Server internal interface
PSOM/MTLS/TCP/8057	Any (can be defined as Front End Server IP address, or each Front End Server IP address in a Front End pool)	Edge Server internal interface	Web conferencing traffic from Front End Server or each Front End Server if in a pool, to Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server internal interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/ UDP/3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server
STUN/MSTURN/ TCP/443	Any	Edge Server internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server if UDP communication cannot be established, TCP is used for file transfer and desktop sharing

HTTPS/TCP/4443	Any (can be defined as the Front End Server IP address, or pool that holds the Central Management store)	Edge Server internal interface	Replication of changes from the Central Management store to the Edge Server
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	**Source IP address**	**Destination IP address**	**Notes**
Access/SIP(MTLS)/ TCP/5061	Access Edge service public IP address	Any	For federated and public IM connectivity using SIP

Firewall Summary – Public Instant

Messaging Connectivity

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Public IM connectivity partners	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Public IM connectivity partners	For federated and public IM connectivity using SIP
Access/SIP(TLS)/ TCP/443	Clients	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger
A/V/STUN,MSTURN/ UDP/3478	Live Messenger clients	Edge Server A/V Edge service	Required for public IM connectivity with Windows Live Messenger

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Edge Server Access Edge service interface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Edge Server Access Edge service interface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from the Edge Server XMPP proxy to federated XMPP partners
XMPP/MTLS/ TCP/23456	Any	Each internal Edge Server Interface IP	Internal XMPP traffic from the XMPP

			Gateway on the Front End Server or Front End pool to the Edge Server internal IP address or each Edge pool member’s internal IP address

1.3.3.5.5 Port Summary - Scaled Consolidated Edge, DNS Load Balancing w ith Private IP Addresses Using NAT

Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

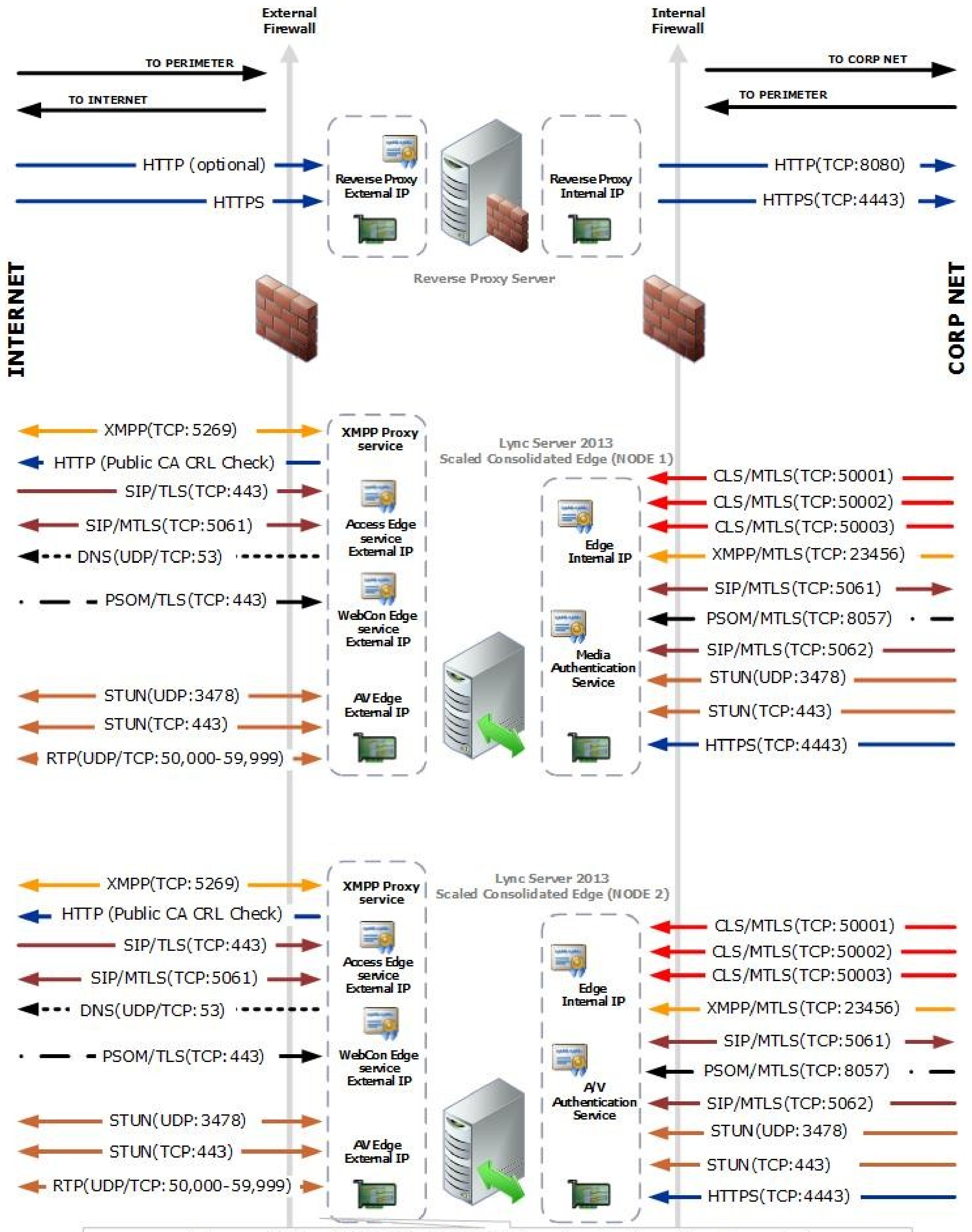
Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-12-04*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.

Enterprise Perimeter Network



Port range TCP and UDP 50,000-59,999 inbound and outbound is only required when federating with partners still running Office Communications Server 2007. (Applies to all nodes in the pool.)

Port and Protocol Details

It is recommended that you open only the ports required to support the functionality for

which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bi-directionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V) and federation.

Firewall Summary for Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT: External Interface – Node 1 and Node 2 (Example)

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations
XMPP/TCP/5269	XMPP Proxy service (shares IP address with Access Edge service)	Any	XMPP Proxy service sends traffic to XMPP contacts in defined XMPP federations
Access/HTTP/TCP/80	Edge Server Access Edge service	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service	Any	DNS query over UDP
Access/SIP(TLS)/ TCP/443	Any	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Any	For federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)/TCP/443	Any	Edge Server Web Conferencing Edge service	Web Conferencing media
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-	Edge Server A/V Edge	Any	Required only for

59,999	service		federation with partners running Office Communications Server 2007.
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service	Required only for federation with partners running Office Communications Server 2007
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service	Required only for federation with partners running Office Communications Server 2007
A/V/STUN,MSTURN/UDP/3478	Edge Server A/V Edge service	Any	3478 outbound is used to determine the version of Edge Server that Lync Server is communicating with and also for media traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/UDP/3478	Any	Edge Server A/V Edge service	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/TCP/443	Any	Edge Server A/V Edge service	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/TCP/443	Edge Server A/V Edge service	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT: Internal Interface – Node 1 and Node 2 (Example)

Protocol/TCP or	Source IP address	Destination IP	Comments

UDP/Port		**address**	
XMPP/MTLS/ TCP/23456	Any (can be defined as Front End Server address, or Front End pool IP address running the XMPP Gateway service)	Edge Server internal interface IP address	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
SIP/MTLS/TCP/5061	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Edge Server internal interface	Outbound SIP traffic (from Director, Director pool IP address, Front End Server or Front End pool IP address) to Edge Server internal interface
SIP/MTLS/TCP/5061	Edge Server internal interface	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Inbound SIP traffic (to Director, Director pool IP address, Front End Server or Front End pool IP address) from Edge Server internal interface
PSOM/MTLS/TCP/8057	Any (can be defined as Front End Server IP address, or each Front End Server IP address in a Front End pool)	Edge Server internal interface	Web conferencing traffic from Front End Server or each Front End Server if in a pool, to Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server internal interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/ UDP/3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server
STUN/MSTURN/ TCP/443	Any	Edge Server internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch

			Server if UDP communication cannot be established, TCP is used for file transfer and desktop sharing
HTTPS/TCP/4443	Any (can be defined as the Front End Server IP address, or pool that holds the Central Management store)	Edge Server internal interface	Replication of changes from the Central Management store to the Edge Server
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	**Source IP address**	**Destination IP address**	**Notes**
Access/SIP(MTLS)/	Access Edge service	Any	For federated and

TCP/5061	public IP address		public IM connectivity using SIP

Firewall Summary – Public Instant Messaging Connectivity

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Public IM connectivity partners	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Public IM connectivity partners	For federated and public IM connectivity using SIP
Access/SIP(TLS)/ TCP/443	Clients	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger
A/V/STUN,MSTURN/ UDP/3478	Live Messenger clients	Edge Server A/V Edge service	Required for public IM connectivity with Windows Live Messenger

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Edge Server Access Edge service interface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Edge Server Access Edge service interface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from

			the Edge Server XMPP proxy to federated XMPP partners
XMPP/MTLS/ TCP/23456	Any	Each internal Edge Server interface IP	Internal XMPP traffic from the XMPP Gateway on the Front End Server or Front End pool to the Edge Server internal IP address or each Edge pool member’s internal IP address

1.3.3.5.6 Port Summary - Scaled Consolidated Edge, DNS Load Balancing w ith Public IP Addresses

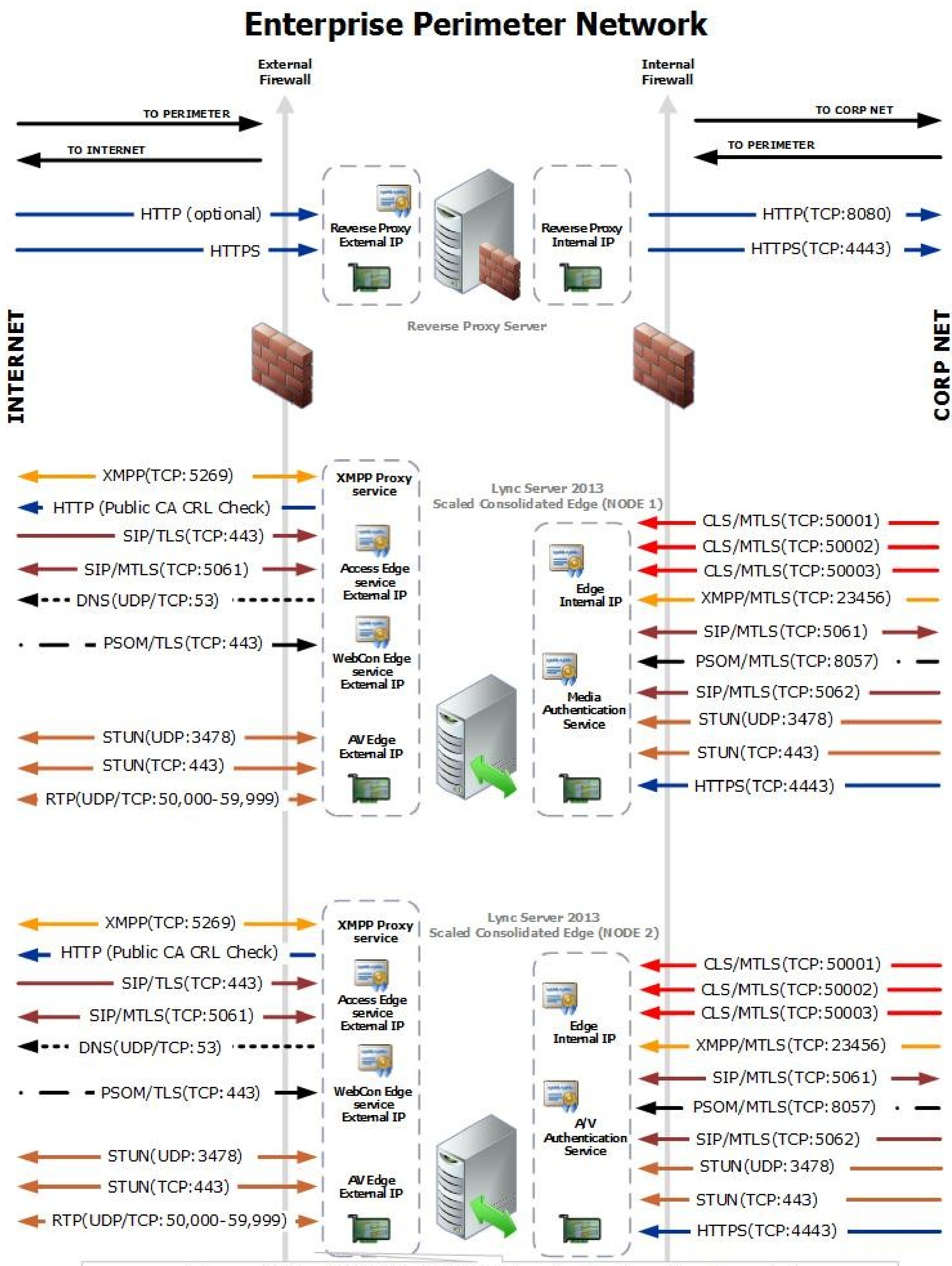
Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-12-04*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.



Port range TCP and UDP 50,000-59,999 inbound and outbound is only required when federating with partners still running Office Communications Server 2007. (Applies to all nodes in the pool.)

Port and Protocol Details

It is recommended that you open only the ports required to support the functionality for

which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bi-directionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V) and federation.

Firewall Summary for Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses: External Interface – Node 1 and Node 2 (Example)

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations
Access/HTTP/TCP/80	Edge Server Access Edge service public IP address	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service public IP address	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service public IP address	Any	DNS query over UDP
Access/SIP(TLS)/ TCP/443	Any	Edge Server Access Edge service public IP address	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Edge Server Access Edge service public IP address	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service public IP address	Any	For federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)TCP/443	Any	Edge Server Web Conferencing Edge service public IP address	Web Conferencing media
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service public IP address	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-59,999	Edge Server A/V Edge service public IP	Any	Required only for federation with

	address		partners running Office Communications Server 2007.
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007
A/V/STUN,MSTURN/UDP/3478	Edge Server A/V Edge service public IP address	Any	3478 outbound is used to determine the version of Edge Server that Lync Server is communicating with and also for media traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/UDP/3478	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/TCP/443	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/TCP/443	Edge Server A/V Edge service	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses: Internal Interface – Node 1 and Node 2 (Example)

Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Comments

XMPP/MTLS/ TCP/23456	Any (can be defined as Front End Server address, or Front End pool IP address running the XMPP Gateway service)	Edge Server internal interface	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
SIP/MTLS/TCP/5061	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Edge Server internal interface	Outbound SIP traffic (from Director, Director pool IP address, Front End Server or Front End pool IP address) to Edge Server internal interface
SIP/MTLS/TCP/5061	Edge Server internal interface	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Inbound SIP traffic (to Director, Director pool IP address, Front End Server or Front End pool IP address) from Edge Server internal interface
PSOM/MTLS/TCP/8057	Any (can be defined as Front End Server IP address, or each Front End Server IP address in a Front End pool)	Edge Server internal interface	Web conferencing traffic from Front End Server or each Front End Server if in a pool, to Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server internal interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/ UDP/3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server
STUN/MSTURN/ TCP/443	Any	Edge Server internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server if UDP

			communication cannot be established, TCP is used for file transfer and desktop sharing
HTTPS/TCP/4443	Any (can be defined as the Front End Server IP address, or pool that holds the Central Management store)	Edge Server internal interface	Replication of changes from the Central Management store to the Edge Server
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Access Edge service public IP address	Any	For federated and public IM connectivity

			using SIP

Firewall Summary – Public Instant Messaging Connectivity

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Public IM connectivity partners	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Public IM connectivity partners	For federated and public IM connectivity using SIP
Access/SIP(TLS)/ TCP/443	Clients	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger
A/V/STUN,MSTURN/ UDP/3478	Live Messenger clients	Edge Server A/V Edge service	Required for public IM connectivity with Windows Live Messenger

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Edge Server Access Edge serviceinterface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Edge Server Access Edge serviceinterface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from the Edge Server XMPP

			proxy to federated XMPP partners
XMPP/MTLS/ TCP/23456	Any	Each internal Edge Server Interface IP	Internal XMPP traffic from the XMPP Gateway on the Front End Server or Front End pool to the Edge Server internal IP address or each Edge pool member’s internal IP address

1.3.3.5.7 Port Summary - Scaled Consolidated Edge w ith Hardw are Load Balancers

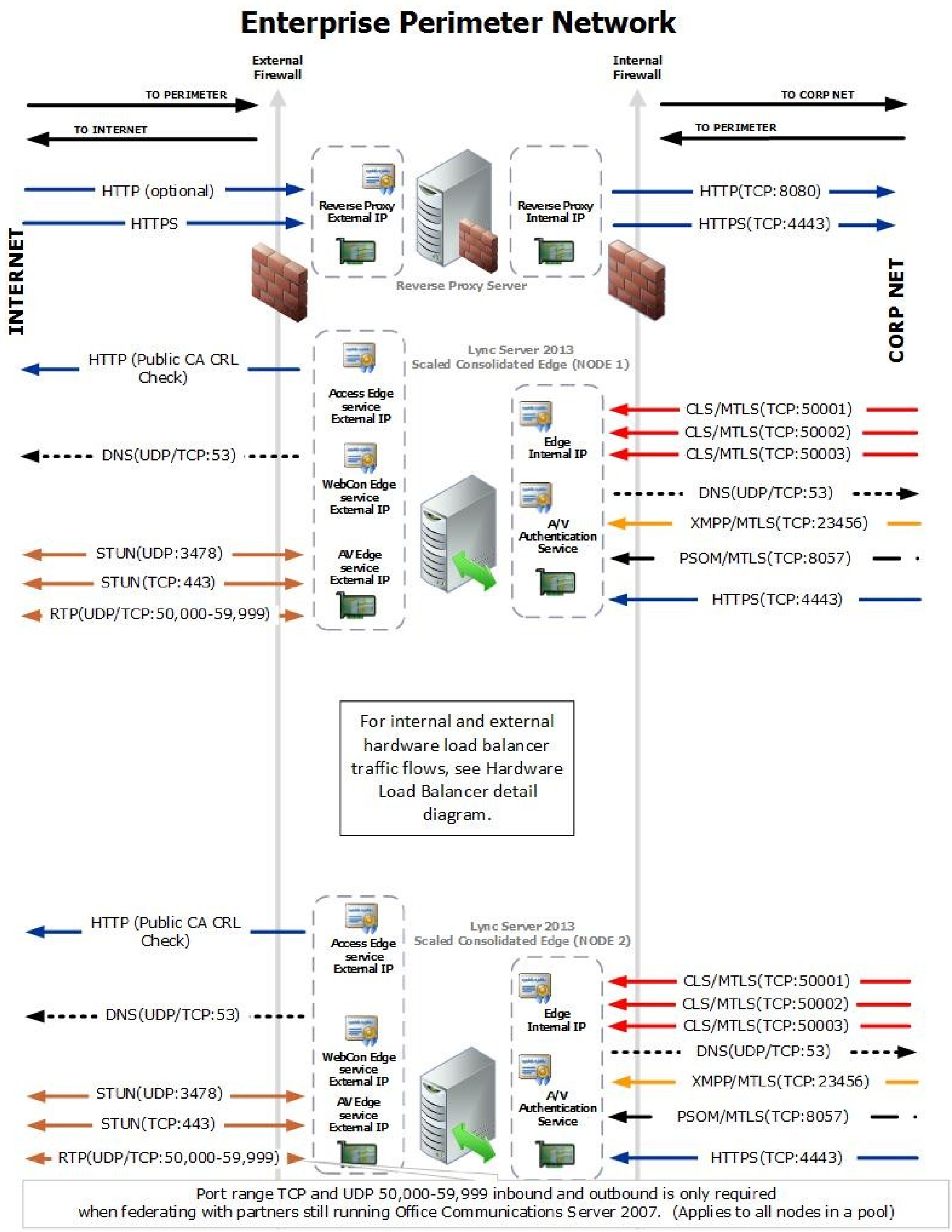
Port Summary - Scaled Consolidated Edge with Hardware Load Balancers

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-12-04*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.


Enterprise Perimeter Network
External Firewall
Internal Firewall
TO PERIMETER
TO INTERNET
TO CORP NET
TO PERIMETER
INTERNET
CORP NET
HTTP (optional)
HTTPS
Reverse Proxy External IP
Reverse Proxy Internal IP
Reverse Proxy Server
HTTP(TCP:8080)
HTTPS(TCP:4443)
Lync Server 2013 Scaled Consolidated Edge (NODE 1)
HTTP (Public CA CRL Check)
Access Edge service External IP
DNS(UDP/TCP:53)
WebCon Edge service External IP
STUN(UDP:3478)
STUN(TCP:443)
RTP(UDP/TCP:50,000-59,999)
AV Edge service External IP
Edge Internal IP
A/V Authentication Service
CLS/MTLS(TCP:50001)
CLS/MTLS(TCP:50002)
CLS/MTLS(TCP:50003)
DNS(UDP/TCP:53)
XMPP/MTLS(TCP:23456)
PSOM/MTLS(TCP:8057)
HTTPS(TCP:4443)
For internal and external hardware load balancer traffic flows, see Hardware Load Balancer detail diagram.
Lync Server 2013 Scaled Consolidated Edge (NODE 2)
HTTP (Public CA CRL Check)
Access Edge service External IP
DNS(UDP/TCP:53)
WebCon Edge service External IP
AV Edge service External IP
STUN(UDP:3478)
STUN(TCP:443)
RTP(UDP/TCP:50,000-59,999)
Edge Internal IP
A/V Authentication Service
CLS/MTLS(TCP:50001)
CLS/MTLS(TCP:50002)
CLS/MTLS(TCP:50003)
DNS(UDP/TCP:53)
XMPP/MTLS(TCP:23456)
PSOM/MTLS(TCP:8057)
HTTPS(TCP:4443)
Port range TCP and UDP 50,000-59,999 inbound and outbound is only required when federating with partners still running Office Communications Server 2007. (Applies to all nodes in a pool)

Port and Protocol Details

It is recommended that you open only the ports required to support the functionality for which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bi-directionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V) and federation.

Firewall Summary for Scaled Consolidated Edge, Hardware Load Balanced: External Interface – Node 1 and Node 2 (Example)

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/HTTP/TCP/80	Edge Server Access Edge service public IP address	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service public IP address	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service public IP address	Any	DNS query over UDP
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service IP address	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-59,999	Edge Server A/V Edge service public IP address	Any	Required only for federation with partners running Office Communications Server 2007.
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service public IP address	Any	3478 outbound is used to determine the version of Edge Server that Lync Server is communicating with and also for media

			traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/ UDP/3478	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/ TCP/443	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/ TCP/443	Edge Server A/V Edge service public IP address	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Scaled Consolidated Edge, Hardware Load Balanced: Internal Interface Node 1 and Node 2

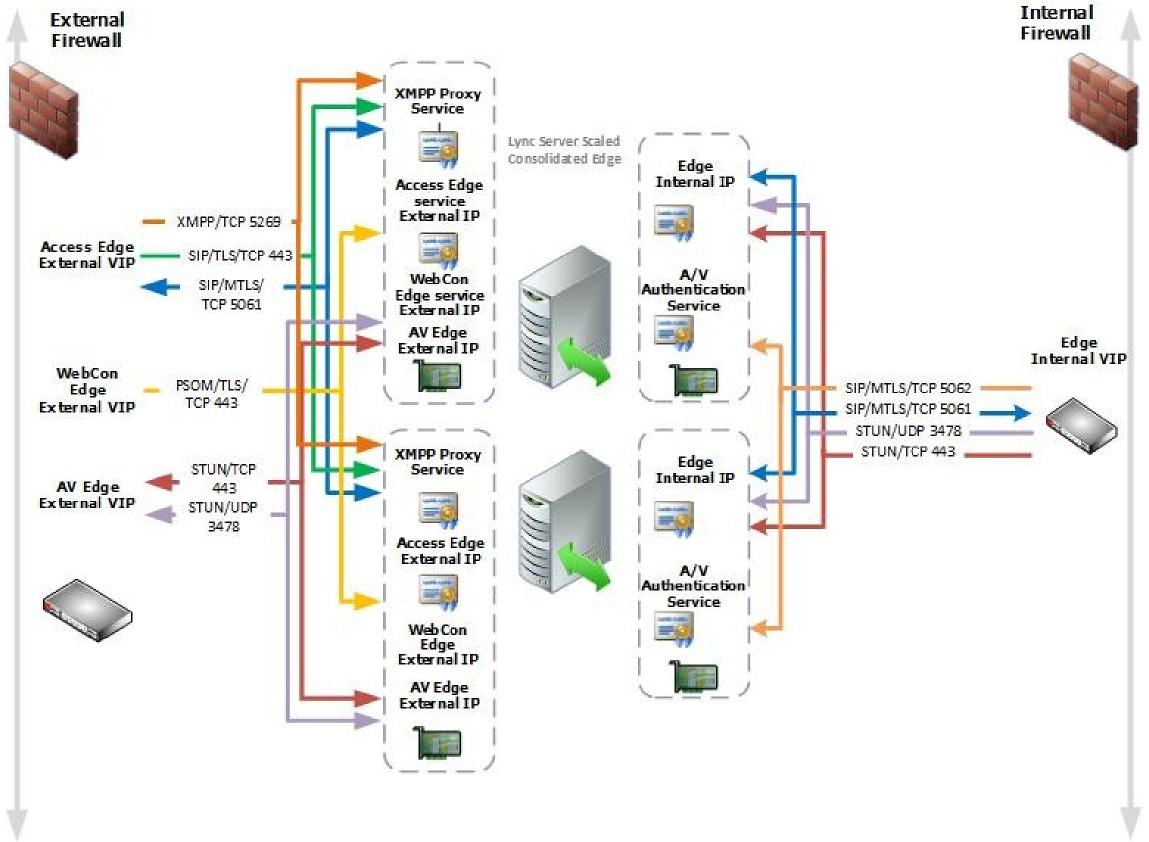
Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/MTLS/ TCP/23456	Any (can be defined as Front End Server address, or Front End pool virtual IP address running the XMPP Gateway service)	Edge Server internal interface	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
HTTPS/TCP/4443	Any (can be defined as the Front End Server server IP or pool that holds the Central Management store)	Edge Server Internal interface	Replication of changes from the Central Management store to the Edge Server
PSOM/MTLS/TCP/8057	Any (can be defined as Director IP, Front End Server IP or Pool virtual IP)	Edge Server Internal interface	Web conferencing traffic from Internal deployment to Internal Edge Server interface
STUN/MSTURN/ UDP/3478	Any (can be defined as Director IP, Front End Server IP or Pool virtual IP)	Edge Server Internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or

			Survivable Branch Server
STUN/MSTURN/ TCP/443	Any (can be defined as Director IP, Front End Server IP or Pool virtual IP)	Edge Server Internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server if UDP communication cannot be established, TCP is used for file transfer and desktop sharing
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Hardware load balancers have specific requirements when deployed to provide availability and load balancing for Lync Server. The requirements are defined in the following figure and tables. Third party vendors may use different terminology for the requirements defined here. It will be necessary to map the requirements of Lync Server to the features and configuration options provided by your hardware load balancer vendor.

When configuring hardware load balancers, consider the following requirements:

- Source Network Address Translation (SNAT) can be configured on the hardware load balancer (HLB) for Access Edge service and Web Conferencing Edge service
- SNAT cannot be configured on the A/V Edge service– the A/V Edge service must respond with the real server address, not the HLB virtual IP (VIP), for simple traversal of UDP over NAT (STUN)/traversal using relay NAT (TURN)/ federation TURN (FTURN) to work properly
- Public IP addresses are used on each server interface and on the VIPs of the HLB, and your public IP address requirements are N+1, where there is a public IP address for each real server interface and one for each HLB VIP. Where you have 2 Edge servers in the pool, this results in 6 public IP addresses, where 3 are used for the HLB VIPs, and one for each Edge server interface (a total of six for the servers)
- For the Access Edge service and Web Conferencing Edge service, (and using NAT on the HLB) the client contacts the VIP, the VIP changes the source IP address from the client to its own IP address. The server interface addresses the return address to the VIP, the VIP changes the source address from the server interface IP address and sends the packet to the client
- For the A/V Edge service, the VIP must NOT change the source IP address, and the real server address is returned to the client directly – you cannot configure NAT on the HLB for AV traffic
- For AV, the external firewall will retain the real server public IP address for all packets
- Once established, client to A/V Edge service communication is to the real server, not the HLB
- Internal edge to internal servers and clients must be routed, and persistent routes are set for all internal networks that host servers or clients
- The HLB Access Edge service VIP will act as the default gateway for each Edge server interface



External Port Settings Required for Scaled Consolidated Edge, Hardware Load Balanced: External Interface Virtual IPs

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations
XMPP/TCP/5269	XMPP Proxy service (shares IP address with Access Edge service)	Any	XMPP Proxy service sends traffic to XMPP contacts in defined XMPP federations
Access/SIP(TLS)/ TCP/443	Any	Access Edge service public VIP address	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Access Edge service public VIP address	SIP signaling, federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Access Edge service public VIP address	Federated partner	SIP signaling, federated and public IM connectivity using SIP

Web Conferencing/ PSOM(TLS)/TCP/443	Any	Edge Server Web Conferencing Edge service public VIP address	Web Conferencing media
A/V/STUN,MSTURN/ UDP/3478	Any	Edge Server A/V Edge service public VIP address	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/ TCP/443	Any	Edge Server A/V Edge service public VIP address	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Scaled Consolidated Edge, Hardware Load Balanced: Internal Interface Virtual IPs

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Any (can be defined as Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address)	Edge Server Internal VIP interface	Outbound SIP traffic (from Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address)to Internal Edge VIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Internal VIP interface	Any (can be defined as Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address)	Inbound SIP traffic (to Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address) from Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server Internal VIP interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/ UDP/3478	Any	Edge Server Internal VIP interface	Preferred path for A/V media transfer between internal and external users
STUN/MSTURN/ TCP/443	Any	Edge Server Internal VIP interface	Fallback path for A/V media transfer between internal and external users if UDP communication cannot

			be established, TCP is used for file transfer and desktop sharing
STUN/MSTURN/ TCP/443	Edge Server Internal VIP interface	Any	Fallback path for A/V media transfer between internal and external users if UDP communication cannot be established, TCP is used for file transfer and desktop sharing

1.3.3.5.8 Port Summary - Reverse Proxy

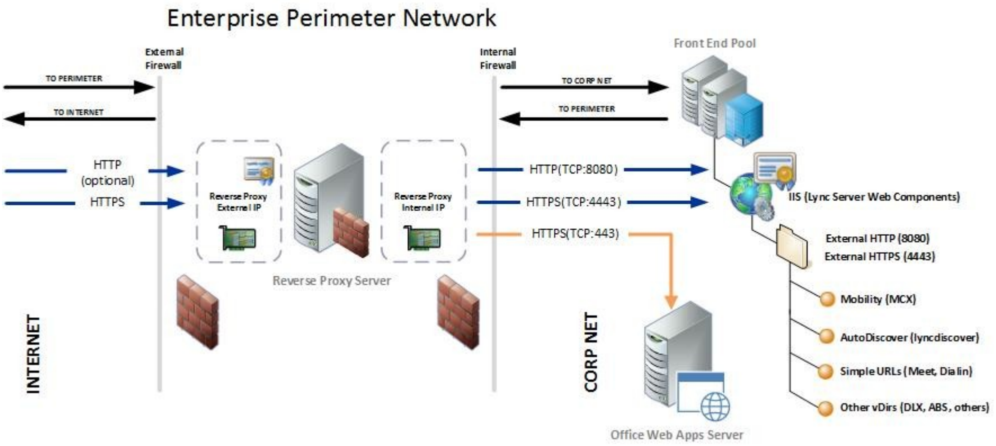
Port Summary - Reverse Proxy

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2013-02-15*

The reverse proxy has minimal requirements for firewall and port/protocol.

- External firewall requirements are the HTTPS/TCP/443 and the optional HTTP/ TCP/80. HTTPS is used for SSL and TLS secure communications through the reverse proxy. HTTP is used if you choose to allow access to the Autodiscover Service when modifying certificates might prove difficult or not cost justified.
- Clients expect to contact the Office Web Apps Server on HTTPS. The Office Web Apps Server expects communication from internal clients on HTTPS/ TCP/443. The recommended configuration is to allow HTTPS/TCP/443 from the reverse proxy to the Office Web Apps Server.
- Port 8080 is used to route traffic from the reverse proxy internal interface to the Front End Server, Front End pool virtual IP (VIP) or the optional Director or Director pool VIP. Port TCP 8080 is required for mobile devices running Lync to locate the Autodiscover Service in situations where modifying the external web service publishing rule certificate is undesirable (for example, if you have a large number of SIP domains). If you choose to acquire new certificates with the necessary SAN entries, the port TCP 8080 is not needed and is optional.
- Port 4443 is used for traffic from the reverse proxy internal interface to the Front End Server, Front End pool virtual IP (VIP) or the optional Director or Director pool VIP



Caution:
Do not confuse the 4443 over TCP from the reverse proxy to the internal deployment for the port 4443 over TCP traffic from the Standard Edition server or the Front End pool that manages the Central Management store role.

Port and Protocol Details

Firewall Details for Reverse Proxy Server: External Interface

Protocol/TCP or UDP/Port	Source IP Address	Destination IP Address	Notes
HTTP/TCP/80	Any	Reverse proxy listener	(Optional) Redirection to HTTPS if user enters http://<*publishedSiteFQDN*>. Also required if using Office Web Apps for conferencing and the Autodiscover Service for mobile devices running Lync in situations where the organization does not want to modify the external web service publishing rule certificate.
HTTPS/TCP/443	Any	Reverse proxy listener	Address book downloads, Address Book Web Query service, Autodiscover, client updates, meeting content, device updates, group expansion, Office Web Apps for conferencing, dial-in conferencing, and meetings.

Firewall Details for Reverse Proxy Server: Internal Interface

Protocol/TCP or UDP/Port	Source IP Address	Destination IP Address	Notes
HTTP/TCP/8080	Internal reverse proxy interface	Front End Server, Front End pool, Director, Director pool	Required if using the Autodiscover Service for mobile devices running Lync in situations where the organization does not want to modify the external web service publishing rule certificate.

			Traffic sent to port 80 on the reverse proxy external interface is redirected to a pool on port 8080 from the reverse proxy internal interface so that the pool Web Services can distinguish it from internal web traffic.
HTTPS/TCP/4443	Internal reverse proxy interface	Front End Server, Front End pool, Director, Director pool	Traffic sent to port 443 on the reverse proxy external interface is redirected to a pool on port 4443 from the reverse proxy internal interface so that the pool web services can distinguish it from internal web traffic.
HTTPS/TCP/443	Internal reverse proxy interface	Office Web Apps for conferencing	

1.3.3.5.9 Port Summary - Lync Server and Office Communications Server Federation

Port Summary - Lync Server and Office Communications Server Federation

See Also

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-10-20*

Port, protocol and firewall requirements for federation with Microsoft Lync Server 2013, Lync Server 2010 and Office Communications Server are similar to those for the deployed Edge Server. Clients initiate communication with the Access Edge service over TLS/SIP/TCP 443. Federated partners however, will initiate communications to the Access Edge service over MTLS/SIP/TCP 5061.

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/TCP/5061	Access Edge service public IP address	Any	For federated and public IM connectivity using SIP

⊟See Also

Concepts

Scenarios for External User Access

1.3.3.5.10 Port Summary - Public Instant Messaging Connectivity

Port Summary - Public Instant Messaging Connectivity

See Also

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2013-02-16*

To configure your firewall for ports and protocols necessary to support public instant messaging connectivity, first note that SIP/MTLS/TCP 5061 is bidirectional to account for the ability of contacts in the public IM provider to contact Lync clients, or for Lync to contact public IM contacts.

Windows Live Messenger can participate in audio/video communications with Lync clients. This accounts for the very similar firewall port and protocol configuration that you would typically have on the firewall to support Lync clients as external users.

> **Important:**
>
> More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard Client Access License (CAL). Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.
> Federation with Messenger client contacts will officially end on March 15, 2013, except for mainland China. Skype will become the federation client for federated users who previously used Messenger.

Firewall Summary – Public Instant Messaging Connectivity

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Public IM connectivity partners	Edge Server Access interface	For federated and public IM connectivity that use SIP.
Access/SIP(MTLS)/ TCP/5061	Edge Server Access interface	Public IM connectivity partners	For federated and public IM connectivity that use SIP.
Access/SIP(TLS)/ TCP/443	Clients	Edge Server Access interface	Client-to-server SIP traffic for external user access.
A/V/RTP/TCP/50,000-59,999	Edge Server Access interface	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/ UDP/3478	Edge Server Access interface	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger.
A/V/STUN,MSTURN/	Live Messenger	Edge Server Access	Required for public IM

UDP/3478	clients	interface	connectivity with Windows Live Messenger.

⊟See Also

Concepts

Scenarios for External User Access
Determine External A/V Firewall and Port Requirements

1.3.3.5.11 Port Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

Port Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

See Also

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-10-20*

The ports and protocols defined for the extensible messaging and presence protocol (XMPP) proxy deployed on the Edge Server allow communications from the XMPP federated partner to the Edge Server, and also allows communication from your Edge Server to the XMPP federated partner. A rule is also defined on the internal-facing firewall from the Front End Server or Front End pool to the Edge Server or Edge pool.

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Access Edge service interface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Access Edge service interface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from the Edge Server XMPP proxy to federated XMPP partners
XMPP/MTLS/23456	Any	Internal Edge Server Interface IP	Internal XMPP traffic from the XMPP Gateway on the Front End Server or Front End pool to the Edge Server

⊟See Also

Tasks

Example XMPP Configuration – XMPP Federation with Google Talk

Other Resources

Manage XMPP Federated Partners for Your Organization

1.3.3.6 Network Bandwidth Requirements for Media Traffic

Network Bandwidth Requirements for Media Traffic

Microsoft Lync Server 2013 > Planning > Network Planning for Lync Server >

Topic Last Modified: *2012-10-22*

An important part of network planning is ensuring that your network can handle the media traffic generated by Lync Server. This section helps you plan for that media traffic.

Media Traffic Network Usage

The media traffic bandwidth usage can be challenging to calculate because of the number of different variables, such as codec usage, resolution, and activity levels. The bandwidth usage is a function of the codec used and the activity of the stream, both of which vary between scenarios. The following table lists the audio codecs commonly used in Lync Server 2013 scenarios.

Audio Codec Bandwidth

Audio codec	Scenarios	Audio payload bitrate (KBPS)	Bandwidth audio payload and IP header only (Kbps)	Bandwidth audio payload, IP header, UDP, RTP and SRTP (Kbps)	Bandwidth audio payload, IP header, UDP, RTP, SRTP and forward error correction (Kbps)
RTAudio Wideband	Peer-to-peer	29.0	45.0	57.0	86.0
RTAudio Narrowband	Peer-to-peer, PSTN	11.8	27.8	39.8	51.6
G.722	Conferencing	64.0	80.0	95.6	159.6
G.722 Stereo	Peer-to-peer, Conferencing	128.0	144.0	159.6	223.6
G.711	PSTN	64.0	80.0	92.0	156.0
Siren	Conferencing	16.0	32.0	47.6	63.6

The bandwidth numbers in the previous table are based on 20ms packetization (50 packets per second) and for Siren and G.722 include the additional secure real-time transport protocol (SRTP) overhead from conferencing scenarios and assume the stream is 100% active. Forward Error Correction (FEC) is dynamically used when there is packet loss on the link to help maintain the quality of the audio stream.

The stereo version of the G.722 codec is used by systems based on the Lync 2013 Meeting Room Edition, which enables stereo microphone capture to allow listeners to better distinguish multiple talkers in the meeting room.

For video, the default codec is the H.264/MPEG-4 Part 10 Advanced Video Coding standard together with its scalable video coding extensions for temporal scalability. To maintain interoperability with Lync 2010 or Office Communicator 2007 R2 clients, the RTVideo codec is still used for peer-to-peer calls between Lync 2013 and legacy clients. In conference sessions with both, Lync 2013 and legacy clients the Lync 2013 endpoint may encode the video using both video codecs and send the H.264 bitstream to the Lync 2013 and the RTVideo bitstream to Lync 2010 or Office Communicator 2007 R2 clients.

The bandwidth required depends on the resolution, quality, and frame rate. For each resolution, there are two interesting bit rates:

- **Maximum payload bitrate** This is the bitrate that a Lync 2013 endpoint will use for resolution at the maximum frame rate supported for this resolution. This value is interesting because it allows the highest quality and frame rate video.
- **Minimum payload bitrate** This is the bitrate below which a Lync 2013 endpoint will switch to the next lower resolution. In order to guarantee a certain resolution, the available video payload bitrate must not fall below this minimum bitrate for that resolution. This value is interesting so that you can understand the lowest value possible in cases where the maximum bitrate is not available or practical. For some users, such a low bitrate video might be considered an unacceptable video experience, so use caution when considering these minimum video payload bitrates. Note that for video scenes with little or no movement of the user the actual bitrate may temporarily also fall below the minimum bitrate.

Lync 2013 supports many more resolutions. This allows you to better adjust to different network bandwidth and receiving client capabilities. In addition the default aspect ratio for Lync 2013 has been changed to 16:9. The 4:3 aspect ratio is still supported for webcams which don't allow capture in 16:9 aspect ratio.

Video Resolution Bandwidth

Video codec	Resolution and aspect ratio	Maximum video payload bitrate (Kbps)	Minimum video payload bitrate (Kbps)
H.264	320x180 (16:9) 212x160 (4:3)	250	15
H.264/RTVideo	424x240 (16:9)) 320x240 (4:3	350	100
H.264	480x270 (16:9) 424x320 (4:3)	450	200
H.264/RTVideo	640x360 (16:9) 640x480 (4:3)	800	300
H.264	848x480 (16:9)	1500	400
H.264	960x540 (16:9)	2000	500
H.264/RTVideo	1280x720 (16:9)	2500	700
H.264	1920x1080 (16:9)	4000	500

H.264/RTVideo	960x144 (20:3)	500	15
H.264	1280x192 (20:3)	1000	250
H.264	1920x288 (20:3)	2000	500

Video FEC is included in the video payload bitrate when it is used so there are not separate values with video FEC and without video FEC.

Endpoints do not stream audio or video packets continuously. Depending on the scenario there are different levels of stream activity which indicate how often packets are sent for a stream. The activity of a stream depends on the media and the scenario, and does not depend on the codec being used. In a peer-to-peer scenario:

- Endpoints send audio streams only when the users speak.
- Both participants receive audio streams.
- If video is used, both endpoints send and receive video streams during the entire call.
- For video scenes with little or no movement the actual bitrate may temporarily be very low as the video codec will skip encoding regions of the video without change.

In a conferencing scenario:

- Endpoints send audio streams only when the users speak.
- All participants receive audio streams.
- If video is used, all participants can receive up to five receive video streams and one panoramic (for example, aspect ratio 20:3) video stream. By default the five receive video streams are based on active speaker history but users can also manually select the participants from which they want to receive a video stream.
- Each participant that turns on the user's send video stream will send one or more video streams. Lync 2013 add the capability of sending up to five video streams to optimize the video quality for all the receiving clients. The actual number of video streams being sent is determined by the sender based on CPU capability, available uplink bandwidth, and the number of receiving clients requesting a certain video stream. The most common case is that one H.264 and one RTVideo video stream are being sent in case a legacy client joins the conference. Another common scenario is that several H.264 video streams (for example, with different video resolutions) are sent to accommodate different receiver requests.

In addition to the bandwidth required for the real-time transport protocol (RTP) traffic for audio and video media, bandwidth is required for real-time transport control protocol (RTCP). RTCP is used for reporting statistics and out-of-band control of the RTP stream. For planning, use the bandwidth numbers in the following table for RTCP traffic. These values represent the maximum bandwidth used for RTCP and differ between audio and video streams because of differences in the control data

RTCP Bandwidth

Media	**RTCP maximum bandwidth (Kbps)**
Audio	5
Video (Only H.264 or RTVideo being sent/ received)	10
Video (H.264 and RTVideo being sent/ received)	15

For capacity planning purposes, the following two bandwidths are of interest:

- **Maximum bandwidth without FEC** The maximum bandwidth that a stream will consume, including the typical activity of the stream and the typical codec used in the scenario without FEC. This is the bandwidth when the stream is at 100% activity and there is no packet loss triggering the use of FEC. This is interesting for computing how much bandwidth must be allocated to allow the codec to be used in a given scenario.
- **Maximum bandwidth with FEC** The maximum bandwidth that a stream consumes, including the typical activity of the stream and the typical codec used in the scenario with FEC. This is the bandwidth when the stream is at 100% activity and there is packet loss triggering the use of FEC to improve quality. This is interesting for computing how much bandwidth must be allocated to allow the codec to be used in a given scenario and allow the use of FEC to preserve quality under packet-loss conditions.

The following tables also list an additional bandwidth value, **Typical bandwidth**. This is the average bandwidth that a stream consumes, including the typical activity of the stream and the typical codec used in the scenario. This bandwidth can be used for approximating how much bandwidth at any given time is being consumed by media traffic but should not be used for capacity planning, because individual calls will exceed this value when the activity level is higher than average. The typical video stream bandwidth in the tables below is based on a mix of different video resolutions as observed in measured customer data. For example, in peer-to-peer sessions a majority of users would use the default video render window whereas some percentage of users would increase or maximize the Lync application to allow higher video resolutions.

The following tables provide these three bandwidth values for the various scenarios.

Audio/Video Capacity Planning for Peer-to-Peer Sessions

Media	**Codec**	**Typical stream bandwidth (Kbps)**	**Maximum stream bandwidth without FEC**	**Maximum stream bandwidth with FEC**
Audio	RTAudio Wideband	39.8	62	91
Audio	RTAudio Narrowband	29.3	44.8	56.6
Main video when calling Lync 2013 endpoints	H.264	460	4010 (for maximum resolution of 1920x1080)	Not applicable
Main video when calling Lync 2010 or Office Communicator 2007 R2 endpoints	RTVideo	460	2510 (for maximum resolution of 1280x720)	Not applicable
Panoramic video when calling Lync 2013 endpoints	H.264	190	2010 (for maximum resolution of 1920x288)	Not applicable
Panoramic video when calling Lync 2010 or Office Communicator 2007 R2	RTVideo	190	510 (for maximum resolution of 960x144)	Not applicable

endpoints				

Audio/Video Capacity Planning for Conferences

Media	Typical codec	Typical stream bandwidth (Kbps)	Maximum stream bandwidth without FEC	Maximum stream bandwidth with FEC
Audio	G.722	46.1	100.6	164.6
Audio	Siren	25.5	52.6	68.6
Main video receive	H.264 and/or RTVideo	260	8015	Not applicable
Main video send	H.264 and/or RTVideo	270	8015	Not applicable
Panoramic video receive	H.264 and/or RTVideo	190	2010 (for maximum resolution of 1920x288)	Not applicable
Panoramic video send	H.264 and/or RTVideo	190	2515 (for sending bitstreams using multiple resolutions/ codecs	Not applicable

For the main video the typical and maximum stream bandwidth is the aggregated bandwidth over all received video streams and over all send video streams respectively. Even with multiple video streams the typical video bandwidth is smaller than in the peer-to-peer scenario because many video conferences are using content sharing that leads to much smaller video windows and thus smaller video resolutions. The maximum supported aggregated video payload bandwidth is 8000 Kbps for both, send and receive streams which would be used e.g. if there are two incoming 1920x1080p video streams.

The typical stream bandwidth for panoramic video is based on currently available devices that only stream up to 960x144 panoramic video. Once devices with 1920x288 panoramic video become available the typical stream bandwidth is expected to increase.

Audio Capacity Planning for PSTN

Media	Typical codec	Typical stream bandwidth (Kbps)	Maximum stream bandwidth without FEC	Maximum stream bandwidth with FEC
Audio	G.711	64.8	97	161
Audio	RTAudio Narrowband	30.9	44.8	56.6

The network bandwidth numbers in these tables represent one-way traffic only and include 5 Kbps for RTCP traffic overhead for each stream. For video the maximum video bit rate is used for computing the maximum stream.

1.3.3.7 Managing Quality of Service (QoS)

Managing Quality of Service (QoS)

Microsoft Lync Server 2013 > Planning > Network Planning for Lync Server >

Topic Last Modified: *2013-02-21*

Quality of Service (QoS) is a networking technology used in some organizations to help provide an optimal end-user experience for audio and video communications. QoS is most-commonly used on networks where bandwidth is limited: with a large number of network packets competing for a relatively small amount of available bandwidth, Quality of Service provides a way for administrators to assign higher priorities to packets carrying audio or video data. By giving these packets a higher priority, audio and video communications are likely to complete faster, and with less interruption, than network sessions involving things like file transfers, web browsing, or database backups. That's because network packets used for file transfers or database backups are assigned a "best effort" priority.

Note:

As a general rule, Quality of Service applies only to communication sessions on your internal network. When you implement QoS, you configure your servers and routers to support packet marking; however, you configure these devices to support packet marking in a particular manner. You cannot assume that Quality of Service will be supported on the Internet or on other networks. Even if Quality if Service is supported on other networks, there is no guarantee that QoS will be configured the same way that you configured the service on your network.

Microsoft Lync Server 2013 does not require Quality of Service; if you do not currently use QoS there is no requirement that you install the service before installing Lync Server 2013. If you experience a considerable amount of packet loss on your network the recommended way to alleviate this problem is to add additional bandwidth. If adding more bandwidth is not possible, then you might want to implement Quality of Service instead.

Lync Server 2013 offers full support for Quality of Service: that means that organizations that are already using QoS can easily integrate Lync Server into their existing network infrastructure. In order to do this you must perform the following tasks:

- Enabling QoS for Devices that Are Not Based on Windows. By default, QoS is disabled for computers and other devices (such as iPhones) that run other operating systems. Although you can use Lync Server to enable and disable Quality of Service for devices, you typically cannot use the product to modify the DSCP codes used by these devices.
- Configuring Port Ranges for Your Conferencing, Application, and Mediation Servers. You must reserve a unique set of ports for different packet types, such as audio and video. With Lync Server 2013 you do not enable or disable Quality of Service by, say, setting a property value to True or to False. Instead, you enable Quality of Service by configuring port ranges and then creating and applying Group Policy. If you later decide not to use QoS you can “disable” Quality of Service simply by removing the appropriate Group Policy objects.
- Configuring Port Ranges for Your Edge Servers. Although not required, you can configure your Edge servers to use the same port ranges as your other servers.
- Configuring Port Ranges for Your Microsoft Lync Clients. These port ranges apply only to client computers and are typically not the same as the port ranges configured on your servers.
- Configuring a Quality of Service Policy for Your Conferencing, Application, and Mediation Servers. These policies determine the DSCP codes that are applied to different packet types.

- Configuring a Quality of Service Policy for Your A/V Edge Servers. This should only be done for the internal side of your Edge servers. That's because Quality of Service is designed for use on your internal network and not on the Internet.
- Configuring Quality of Service Policies for Clients Running on Windows 7 or Windows 8. Note that Microsoft Lync Server 2013 does not support QoS for other Windows operating systems, such as Windows Vista or Windows XP.
- Configuring Quality of Service on Microsoft Lync Phone Edition Devices. By default, QoS is enabled for Lync Phone Edition devices. However, you might want to change the default DSCP value in order to ensure that all audio packets in your organization use the same DSCP code.

Note:

If you are using Microsoft Windows Server 2012 you might be interested in the new set of Windows PowerShell cmdlets available for managing Quality of Service on that platform. For more information, see Network Quality of Service Cmdlets in Windows PowerShell at http://go.microsoft.com/fwlink/p/?LinkId=285379.

1.3.4 Capacity Planning

Capacity Planning

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-10-04*

The topics in this section help you understand how to plan and deploy Lync Server 2013 so that you can adequately plan for the number of users in your organization and plan for the server load that their activities generate.

- Capacity Planning Using the User Models
- Estimating Voice Usage and Traffic
- Deployment Guidelines for Mediation Server
- Lync Server 2013 User Models

1.3.4.1 Capacity Planning Using the User Models

Capacity Planning Using the User Models

Microsoft Lync Server 2013 > Planning > Capacity Planning >

Topic Last Modified: *2013-03-12*

This section provides guidance on how many servers you need at a site for the number of users at that site, according to the usage described in Lync Server 2013 User Models.

Tested Hardware Platform

All the performance results and deployment recommendations in this section are based on performance testing on servers running the hardware described in the following table. We recommend that you use similar hardware. If you use less powerful hardware, you may experience functionality problems or poor performance. Note that these hardware recommendations are higher than those of previous versions of Lync Server.

Hardware Used in Performance Testing

Hardware component	Recommended
CPU	64-bit dual processor, hex-core, 2.26 gigahertz

	(GHz) or higher Intel Itanium processors are not supported for Lync Server server roles.
Memory	32 gigabytes (GB)
Disk	• 8 or more 10,000-RPM hard disk drives with at least 72 GB free disk space. Two of the disks should use RAID 1, and six should use RAID 10. - OR - • Solid state drives (SSDs) which provide performance similar to 8 10,000-RPM mechanical disk drives.
Network	• 1 dual-port network adapter, 1 Gbps or higher (2 recommended, which requires teaming with a single MAC address and single IP address)

Summary of Results

The following table summarizes these recommendations.

Server role	Maximum number of users supported
Front End pool with twelve Front End Servers and one Back End Server or a mirrored pair of Back End Servers.	80,000 unique users simultaneously logged in, plus 50% multiple points of presence (MPOP) representing non-mobile instances, plus 40% of users enabled for Mobility for a total of 152,000 endpoints.
A/V Conferencing	The A/V Conferencing service provided by a Front End pool supports the pool's conferences assuming a maximum conference size of 250 users, and only one such large conference running at a time. **Note:** Additionally, you can support large conferences of between 250 and 1000 users by deploying a separate Front End pool with two Front End Servers to host the large conferences. For details, see Supporting Large Meetings Using Lync Server 2013.
One Edge Server	12,000 concurrent remote users
One Director	12,000 concurrent remote users
Monitoring and Archiving	In Lync Server 2013, the Monitoring and Archiving front end services now run on each Front End Server, instead of on separate server roles. Monitoring and Archiving each still require their own database stores. If you also run Exchange 2013, you can keep your Archiving data in Exchange, rather than in a dedicated SQL database.

One Mediation Server	Mediation Server collocated with Front End Server runs on every Front End Server in a pool, and should provide enough capacity for the users in the pool. For stand-alone Mediation Server, see the "Mediation Server" section later in this topic.
One Standard Edition server	We strongly recommend that if you use Standard Edition servers to host users, you always use two servers, paired using the recommendations in Planning for High Availability and Disaster Recovery. Each server in the pair can host up to 2,500 users, and if one server fails the remaining server can support 5,000 users in a failover scenario. If your deployment includes a lot of audio or video traffic, server performance may suffer even if you have fewer than 2,500 users per server. In this case, you should consider adding more Standard Edition servers or moving to Lync Server Enterprise Edition.

Front End Server

In a Front End pool, you should have one Front End Server for every 6,660 users homed in the pool, assuming that hyper-threading is enabled on all servers in the pool, and that the server hardware meets the recommendations in Server Hardware Platforms. The maximum number of users in one Front End pool is 80,000, assuming that hyper-threading is enabled on all the servers in the pool. If you have more than 80,000 users at a site, you can deploy more than one Front End pool.

When you account for the number of users in a Front End pool, include the users homed on Survivable Branch Appliances and Survivable Branch Servers at branch offices that are associated with this Front End pool.

When an active server is unavailable, its connections are transferred automatically to the other servers in the pool. For example, if you have 30,000 users and five Front End Servers, then if one server is unavailable, the connections of 6000 users need to be transferred to the other four servers. The remaining four servers will each have 7500 users, which is a larger number than recommended.

If instead you had started with six Front End Servers for your 30,000 users and subsequently one became unavailable, a total of 5000 users will be moved to the remaining five servers. These five servers will each host 6000 users, which is in the recommended range.

The maximum number of users in a Front End pool is 80,000. The maximum number of Front End Servers in a pool is 12.

For a Front End pool with 80,000 users, twelve Front End Servers is sufficient for performance, in typical deployments that follow the Lync Server 2013 User Models. Deployments designed to support disaster recovery failover assume that a maximum of 40,000 users can be hosted in each of two paired Front End pools, in which each pool has enough Front End Servers to accommodate the users in both pools should one pool need to be failed over to the other.

The number of users supported with good performance by a particular Front End pool may differ from these numbers for the following reasons:

- The hardware for your Front End Servers does not meet the recommendations in Server Hardware Platforms.
- Your organization’s usage differs significantly from the user models, such as significantly more conferencing traffic.

Important:

In Lync Server 2013, the presence databases are now hosted on Front End Servers, unlike in Lync Server 2010 where they were hosted on the Back End Server. This means that the disk performance and capacity of your Front End Servers should not be compromised from the recommendations listed earlier in this section and in Server Hardware Platforms, regardless of the number of users hosted by your Front End Servers.

The following table shows the average bandwidth for IM and presence, given the user model, as defined in Lync Server 2013 User Models.

Average bandwidth per user	Bandwidth requirements per Front End Server with 6,660 users
1.3 Kpbs	13 Mbps

Note:

To improve the media performance of the co-located A/V Conferencing and Mediation Server functionality on your Front End Servers, you should enable receive-side scaling (RSS) on the network adapters on your Front End Servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, see "Receive-Side Scaling Enhancements in Windows Server 2008" at http://go.microsoft.com/fwlink/p/?linkId=268731. For details about how to enable RSS, see your network adapter documentation.

Conferencing Maximums

Given the user model that 5% of users in a pool may be in a conference at any one time, a pool of 80,000 users could have about 4,000 users in conferences at one time. These conferences are expected to be a mix of media (some IM-only, some IM with audio, some audio/video, for example) and number of participants. There is no hard limit for the actual number of conferences allowed, and actual usage determines the actual performance. For example, if your organization has many more mixed-mode conferences than are assumed in the user model, you might need to deploy more Front End Servers or A/V Conferencing Servers than the recommendations in this document. For details about the assumptions in the user model, see Lync Server 2013 User Models.

The maximum supported conference size hosted by a regular Lync Server 2013 Front End pool which also hosts users is 250 participants. While a 250-user conference is happening, the pool still supports other conferences as well, such that a total of 5% of pool users are in concurrent conferences. For example, in a pool of twelve Front End Servers and 80,000 users, while the 250-user conference is happening, Lync Server supports 3,750 other users participating in smaller conferences.

Regardless of the number of users homed on the Front End pool or Standard Edition server, Lync Server supports a minimum of 125 other users participating in smaller conferences on the same pool or server which is hosting a 250-user conference.

To enable conferences with between 250 and 1000 users, you can set up a separate Front End pool just to host those conferences. This Front End pool will not host any users. For details, see Supporting Large Meetings Using Lync Server 2013.

If your organization has many more mixed-mode conferences than are assumed in the user model, you might need to deploy more Front End Servers than the recommendations in this document (up to a limit of 12 FEs). For details about the assumptions in the user model, see Lync Server 2013 User Models.

Edge Server

You should deploy one Edge Server for every 12,000 remote users who will access a site concurrently. At a minimum we recommend two Edge Servers for high availability. These recommendations assume that the hardware for your Edge Servers meets the recommendations in Server Hardware Platforms.

When you account for the number of users for the Edge Servers, include the users homed on Survivable Branch Appliances and Survivable Branch Servers at branch offices that are associated with a Front End pool at this site.

Note:
To improve the performance of the A/V Conferencing Edge service on your Edge Servers, you should enable receive-side scaling (RSS) on the network adapters on your Edge Servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, see "Receive-Side Scaling Enhancements in Windows Server 2008" at http://go.microsoft.com/fwlink/p/?linkId=268731. For details about how to enable RSS, see your network adapter documentation.

Director

If you deploy the Director server role we recommend that you deploy one Director for every 12,000 remote users who will access a site concurrently. At a minimum we recommend two Directors for high availability. These recommendations assume that the hardware for your Edge Servers meets the recommendations in Server Hardware Platforms.

When you account for the number of users for the Directors, include the users homed on Survivable Branch Appliances and Survivable Branch Servers at branch offices that are associated with a Front End pool at this site.

Mediation Server

If you collocate Mediation Server with Front End Server, Mediation Server runs on every Front End Server in the pool, and should provide enough capacity for the users in the pool.

If you deploy a stand-alone Mediation Server pool, then how many Mediation Servers to deploy depends on many factors, including the hardware used for Mediation Server, the number of VoIP users you have, the number of gateway peers that each Mediation Server pool controls, the busy hour traffic through those gateways, and the percentage of calls with media that bypasses the Mediation Server.

The following tables provide a guideline for how many concurrent calls a Mediation Server can handle, assuming that the hardware for the Mediation Servers meets the requirements in Server Hardware Platforms and that hyper-threading is enabled. For details about Mediation Server scalability, see Estimating Voice Usage and Traffic and Deployment Guidelines for Mediation Server.

All the following tables assume usage as summarized in Lync Server 2013 User Models.

Stand-alone Mediation Server Capacity: 70% Internal Users, 30%

External users with non-bypass call capacity (media transcoding performed by Mediation Server)

Server hardware	Maximum number of calls	Maximum number of T1 lines	Maximum number of E1 lines
Dual processor, hex core, 2.26 GHz hyper-threaded CPU **with hyper-threading disabled**, with 32 GB memory and one dual-port network adapter card.	1100	46	35
Dual processor, hex core, 2.26 GHz hyper-threaded CPU, with 32 GB memory and one dual-port network adapter card.	1500	63	47

Note:
Although servers with 32 GB of memory were used for performance testing, servers with 16 GB of memory are supported for stand-alone Mediation Server, and are sufficient to provide the performance shown in this table.

Mediation Server Capacity (Mediation Server Collocated with Front End Server) 70% Internal Users, 30% External Users, Non-Bypass Call Capacity (Media Processing Performed by Mediation Server)

Server hardware	Maximum number of calls
Dual processor, hex core, 2.26 GHz hyper-threaded CPU, with 32 GB memory and 2 1GB network adapter cards.	150

Note:
This number is much smaller than the numbers for the stand-alone Mediation Server because the Front End Server has to handle other features and functions for the 6600 users homed on it, in addition to the transcoding needed for voice calls.

Note:
To improve the performance of the Mediation Server, you should enable receive-side scaling (RSS) on the network adapters on your Mediation Servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, see "Receive-Side Scaling Enhancements in Windows Server 2008" at http://go.microsoft.com/fwlink/p/?linkId=268731. For details about how to enable RSS, see your network adapter documentation.

Back End Server

In Lync Server 2013, the presence databases are located on the Front End Servers instead of the Back End Server. This has resulted in a much simpler requirement for each Back End Server in Lync Server 2013, equivalent to the hardware requirement for the Front End Server. Contrast this to Lync Server 2010, where the Back End Server was required to be a much higher grade server with 25 disks. However, the workload of Back End Servers is still such that you should not fail to meet the hardware recommendations listed earlier in this section and in Server Hardware Platforms.

To provide high availability of your Back End Server, we recommend deploying server mirroring. For more information, see Back End Server High Availability.

Monitoring and Archiving

In Lync Server 2013, if you deploy Monitoring or Archiving, the front end functionality of these services runs on the Front End Servers, instead of on separate server roles. Monitoring and Archiving each still use their own database store, separate from the Back End store. Alternatively, if you have Exchange 2013 deployed, you can store instant message Archiving data in Exchange instead of in a dedicated SQL store.

The following table indicates approximately how much database storage is required per user per day for Monitoring and Archiving data.

	CDR (Monitoring)	**QoE (Monitoring)**	**Archiving**
Disk space required per user per day	49 KB	28 KB	57 KB

Microsoft used the hardware in the following table for the database server for Monitoring and Archiving during its performance testing. The testing collected the data of two Front End pools, each of which contained 80,000 users.

Hardware Used in Monitoring and Archiving Performance Testing

<table>
<tr><th>Hardware component</th><th>Recommended</th></tr>
<tr><td>CPU</td><td>64-bit dual processor, hex-core, 2.26 gigahertz (GHz) or higher</td></tr>
<tr><td>Memory</td><td>48 gigabytes (GB)</td></tr>
<tr><td>Disk</td><td>25 10,000-RPM hard disk drives with 300 GB on each disk, with the following configuration
<table>
<tr><th>Drive</th><th>RAID Configuration</th><th>Number of disks</th></tr>
<tr><td>CDR, QoE, and Archiving database data files, on a single drive</td><td>1+0</td><td>16</td></tr>
<tr><td>CDR database log file</td><td>1</td><td>2</td></tr>
<tr><td>QoE database log file</td><td>1</td><td>2</td></tr>
<tr><td>Archiving database log file</td><td>1</td><td>2</td></tr>
</table></td></tr>
<tr><td>Network</td><td><ul><li>1 dual-port network adapter, 1 Gbps or higher (2 recommended, which requires teaming with a single MAC address and single IP address)</li></ul></td></tr>
</table>

In This Section

- Estimating Voice Usage and Traffic
- Deployment Guidelines for Mediation Server

1.3.4.1.1 Estimating Voice Usage and Traffic

Estimating Voice Usage and Traffic

Planning > Capacity Planning > Capacity Planning Using the User Models >

Topic Last Modified: *2012-08-07*

The Microsoft Lync Server 2013, Planning Tool uses the following metric to estimate user traffic at each site and the number of ports that are required to support that traffic.

- For **Light traffic** (one PSTN call per user per hour), figure 15 users per port.
- For **Medium traffic** (2 PSTN calls per user per hour), figure 10 users per port.
- For **Heavy traffic** (3 or more PSTN per user calls per hour), figure 5 users per port.

The number of ports in turn determines the number of Mediation Servers and gateways that will be required. The public switched telephone network (PSTN) gateways that most organizations consider deploying range in size from 2 ports to as many as 960 ports. (There are even larger gateways, but these are used mainly by telephony service providers.)

For example, an organization with 10,000 users and medium traffic would require 1000 ports. The number of gateways required would equal the total number of ports required as determined by the total capacity of the gateways.

1.3.4.1.2 Deployment Guidelines for Mediation Server

Deployment Guidelines for Mediation Server

Planning > Capacity Planning > Capacity Planning Using the User Models >

Topic Last Modified: *2012-10-12*

This topic describes planning guidelines for Mediation Server deployment. After reviewing these guidelines, we recommend that you use the Planning Tool to create and view possible alternative topologies, which can serve as models for what the final tailored topology that you decide to deploy would look like.

Collocated or Stand-alone Mediation Server?

Mediation Server is by default collocated on the Standard Edition server or Front End Server in a Front End pool at central sites. The number of public switched telephone network (PSTN) calls that can be handled and the number of machines required in the pool will depend on the following:

- The number of gateway peers that the Mediation Server pool controls
- The high-volume traffic periods through those gateways
- The percentage of calls that are calls whose media bypass the Mediation

Server

When planning, be sure to take into account the media processing requirements for PSTN calls and A/V conferences that are not configured for media bypass, as well as the processing needed to handle signaling interactions for the number of busy-hour calls that need to be supported. If there is not enough CPU, then you must deploy a stand-alone pool of Mediation Servers; and PSTN gateways, IP-PBXs, and SBCs will need to be split into subsets that are controlled by the collocated Mediation Servers in one pool and the stand-alone Mediation Servers in one or more stand-alone pools.

If you deployed PSTN gateways, IP-PBXs, or Session Border Controllers (SBCs) that do not support the correct capabilities to interact with a pool of Mediation Servers, including the following, then they will need to be associated with a stand-alone pool consisting of a single Mediation Server:

- Perform network layer Domain Name System (DNS) load balancing across Mediation Servers in a pool (or otherwise route traffic uniformly to all Mediation Servers in a pool)
- Accept traffic from any Mediation Server in a pool

You can use the Microsoft Lync Server 2013, Planning Tool to evaluate whether collocating the Mediation Server with your Front End pool can handle the load. If your environment cannot meet these requirements, then you must deploy a stand-alone Mediation Server pool.

Central Site and Branch Site Considerations

Mediation Servers at the central site can be used to route calls for IP-PBXs or PSTN gateways at branch sites. If you deploy SIP trunks, however, you must deploy a Mediation Server at the site where each trunk terminates. Having a Mediation Server at the central site route calls for an IP-PBX or PSTN gateway at a branch site does not require the use of media bypass. However, if you can enable media bypass, doing so will reduce media path latency and, consequently, result in improved media quality because the media path is no longer required to follow the signaling path. Media bypass will also decrease the processing load on the pool.

Note:

Media bypass will not interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed on Unified Communications Open Interoperability Program – Lync Server at http://go.microsoft.com/fwlink/p/?LinkId=268730.

If branch site resiliency is required, a Survivable Branch Appliance or combination of a Front End Server, a Mediation Server, and a gateway must be deployed at the branch site. (The assumption with branch site resiliency is that presence and conferencing are not resilient at the site.) For guidance on branch site planning for voice, see Planning for Branch-Site Voice Resiliency.

For interactions with an IP-PBX, if the IP-PBX does not correctly support early media interactions with multiple early dialogs and RFC 3960 interactions, there can be clipping of the first few words of the greeting for incoming calls from the IP-PBX to Lync endpoints. This behavior can be more severe if a Mediation Server at a central site is routing calls for an IP-PBX where the route terminates at a branch site, because more time is needed for signaling to complete. If you experience this behavior, deploying a Mediation Server at the branch site is the only way to reduce clipping of the first few words.

Finally, if your central site has a TDM PBX, or if your IP-PBX does not eliminate the need for a PSTN gateway, then you must deploy a gateway on the call route connecting Mediation Server and the PBX.

Note:
To improve the media performance of standalone Mediation Server, you should enable receive-side scaling (RSS) on the network adapters on these servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, see "Receive-Side Scaling Enhancements in Windows Server" at http://go.microsoft.com/fwlink/p/?LinkId=268731. For details about how to enable RSS, see your network adapter documentation.

1.3.4.2 Lync Server 2013 User Models

Lync Server 2013 User Models

Microsoft Lync Server 2013 > Planning > Capacity Planning >

Topic Last Modified: *2013-01-11*

The user models described here provide the basis for the capacity planning measurements and recommendations described in Capacity Planning Using the User Models.

Lync Server 2013 User Models

The following table describes the user model for registration, contacts, instant messaging (IM), and presence for Lync Server 2013.

Environment and Registration User Model

Category	Description
Deployment size and distribution	We model a large deployment with three central sites, with one Front End pool per site.
Percentage of Active Directory users	We assume that 70% of all Active Directory users in the organization are enabled for Lync Server. 80% of those enabled users are logged on to Lync Server each day (80% concurrency). The concurrent users are the basis for the numbers in the rest of this section.
Active Directory changes	We assume that 0.5% of total users are created and enabled for Lync in Active Directory each week, and that 0.5% of total users are disabled from Active Directory and from Lync each week. 5% of users have at least one Active Directory attribute changed each week.
Active Directory distribution groups	We assume that the number of Active Directory distribution groups in the organization is equal to three times the number of all users in Active Directory. The distribution groups have the following sizes: • 64% have 2-30 users • 13% have 31-50 users • 10% have 51-100 users • 13% have 101-500 users
Voice over IP (VoIP) users	60% of Lync Server users are enabled for unified communications (UC) (that is, their phone numbers are owned by Lync Server).
Registered client distribution	65% of clients run Lync 2013 software, including Lync and Lync Phone Edition.

	30% of clients running client software from a previous version of Lync. 5% of clients using Lync Web App. If mobility is enabled, we assume that 40% of users are using mobility concurrently with the other previously cited registered client options. In this case the client multiple point of presence (MPOP) ratio is 1:1.9. If mobility is disabled, the MPOP ratio is 1:1.5.
Remote user distribution	70% of users connecting internally. 30% of users connecting through an Edge Server and a Director.
Contact distribution	The maximum number of contacts a user has is 1,000. Less than 1% of users have 1,000 contacts. Less than 25% of users have 100 or more contacts. Average of 80 contacts for users with public cloud connectivity. Of these users: • 50% of the contacts are within the organization. 10% of those users are remote users, connecting from outside the firewall. • 40% of the contacts are public cloud users (such as users of AOL, Yahoo!, MSN, or Google Talk). • 10% of the contacts are from federated partners. **Important:** • As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013). • The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down. • More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world.

	Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice. Average of 50 contacts for users without public cloud connectivity. Of these users: • 80% of the contacts are within the organization. 10% of those users are remote users, connecting from outside the firewall. • 20% of the contacts are from federated partners. Each user has 1 distribution group in their contact list. For performance testing, we assume that distribution groups are always expanded. 25% of a user's contacts use XMPP.
Session time	The average user logon session lasts 12 hours. All users log on within 120 minutes of the start of the session.

IM and Presence User Model

Category	Description
Peer-to-peer IM sessions	Each user averages six peer-to-peer IM sessions per day. 10 instant messages per session. Each message is matched by two SIP INFO messages and 2 SIP 200 OK messages (for the status indicators such as "<Name> is Typing")
Presence polling	Overall, we assume presence polling at an average of 60 polls per user per hour. For each user, assume an average of: • One poll per day of the presence of users in the user's organization tab (but not Contacts list). Average number of non-contacts in the user's organization tab is 15 users. Two contact card viewing operations per day. • One presence poll every time the user clicks another user to start a conversation, estimated at once per hour. • Six user searches per hour. Every time a search is performed, a batch poll is sent for everyone in the search result list. We assume the average size of search results is 20. If the search results stay on screen, the batch poll is refreshed every 5 minutes; we assume

	that there will be two such refreshes per hour. - When the user opens or previews an email in Outlook, a poll of the presence of users in the To: and CC: fields of the email, estimated at five emails per hour and four users per email.
Presence subscriptions	When one user adds another as a contact, the first user is *subscribing* to five categories of information about the second user. Updates of these categories of information are automatically sent to the first user. For each client, a single batch subscription request is sent to obtain the presence state of an average of 40 contacts, with an additional 40 dialogs to obtain presence for federated contacts. Presence for members of an expanded distribution group is found through persistent presence subscriptions, not polling, and is modeled as 1 expansion per user for each 2 hours. *Short subscriptions* happen when a user logs in, there is a batch subscription for all the user's contacts, and then the user soon logs off. We assume 6 short subscriptions per user per hour, where each subscription lasts 10 minutes.
Presence Publication	Presence state is published at an average of 4 publications per user per hour, with a maximum 6 per user per hour.
Presence Document Size	The average size of a complete presence document is assumed to be 4K, with a maximum of 25K.

The following table describes the user model for address book use.

Address Book Usage User Model

Address Book search mode	Usage
Address Book Web Query only (all queries performed by Address Book Web Query service)	Four prefix queries per user per day. 60 exact search queries per user per day. 40% of those are batched, with an average of 20 contacts per query. The other 60% of the queries are for a single contact. 25 photo queries per user per day. 24 are for a single photo, the other is a batch query with an average of 20 contacts. One total organization search query per user per day.
Mixed mode, both address book file and web queries used. This is the default mode.	Only two types of queries go to the network, the photo and total organizational search queries. 25 photo queries per user per day. 24 are

	for a single photo, the other is a batch query with an average of 20 contacts. One total organization search query per user per day.

The following table describes the conferencing model.

Conferencing Model

Category	Description
Scheduled meetings versus "Meet now" meetings	60% scheduled, 40% unscheduled. Of the scheduled meetings, we assume that 80% are assigned conferences, which are occurences of recurring conferences; 10% are one-time open meetings; 8% are one-time anonymous meetings, and 2% are one-time closed meetings.
Conferencing client distribution	For scheduled meetings: • 65% of conferencing users use Lync 2013. • 5% of conferencing users use Microsoft Lync Web App. • 30% of conferencing users use earlier clients, including Microsoft Lync 2010, Office Communicator 2007 R2, Office Communicator 2007, and Microsoft Office Communicator Web Access (2007 release). For unscheduled meetings: • 70% of conferencing users use Lync 2013. • 30% of conferencing users use earlier clients, including Microsoft Lync 2010, Office Communicator 2007 R2, Office Communicator 2007, and Microsoft Office Communicator Web Access (2007 release).
Meeting concurrency	5% of users will be in conferences during working hours. Thus, in an 80,000-user pool, as many as 4,000 users might be in conferences at any one time.
Meeting audio distribution	40% mixed VoIP audio and dial-in conferencing, with a 3:1 ratio of VoIP users to dial-in users. 35% VoIP audio only. 15% dial-in conferencing audio only. 10% no audio (IM-only conferences, with an average of five messages sent per user).
Media mix for conferences	75% of conferences are web conferences, which include audio plus some other collaboration modalities.

	For these conferences, the other collaboration methods are as follows: **Note:** These numbers add up to more than 100% because one conference can have multiple collaboration methods. - 50% add application sharing. We assume one users sends data at a peak of 1.1 MB per second. - 50% add instant messaging (with an average of 2 messages per user). - 20% add data collaboration, including PowerPoint or whiteboard In these, an average of 2 PowerPoint files presented per conference, with an average PowerPoint file size of 10 MB (without embedded video) or 30 MB (with embedded video). Average of 20 annotations per whiteboard. - 20% add video. Of these users, 70% are in conferences enabled for multiview video, where each user receives 2-3 video streams. - 15% add shared notes.
Meeting participant distribution	50% internal, authenticated users. 25% remote access, authenticated users. 15% anonymous users. 10% federated users.
Meeting join distribution	Users are simulated as joining the meeting within the first 5 minutes.

In regular Front End pools, Lync Server 2013 has a maximum supported meeting size of 250 users. Each pool can host one 250-user meeting at a time. While this large meeting is occurring, the pool can also host other smaller conferences. Additionally, you can support meetings of up to 1000 users by setting up a dedicated pool to host these meetings. For details, see Support for Large Meetings.

Conferences were simulated as follows:

- 85% of conferences had four participants.
- 10% of conferences had six participants.
- 5% of conferences had 11 participants.
- One large conference of 250 users.

The following table provides details about the user model for conferences involving dial-in users.

Dial-In Conferencing User Model

Category	Description
Authenticated/anonymous	70% of callers join as anonymous and are prompted for a recorded name. 30% join as authenticated users.

Call duration and music on hold	Average call duration without music on hold: 50 seconds. 50% of call-in users hear music on hold, for an average of 5 minutes.
Dual-tone multifrequency (DTMF)	15% of conferences that are dial-in only have phone leaders. 10% of mixed conferences that include dial-in users also have phone leaders. 20% of phone leaders use 2 DTMF commands per conference.
Announcement languages	Simulations use English as the announcement language.

The following table provides details about the user model for conference lobbies.

Conference Lobby User Model

Category	Description
Number of users in lobby	5% of dial-in users go through the lobby, and 25% of other users go through the lobby
Admitting from lobby	In simulations, all users were admitted by the presenter before client timeout.

The following table describes the user model for other peer-to-peer sessions.

Peer-to-Peer Sessions User Model

Category	Description
Application sharing	Each user participates in 5 peer-to-peer application sharing sessions per month, for an average of 0.25 sessions per day.
File transfer	Each user participates in 1 peer-to-peer file transfer session per month (as part of an IM session), for an average of 0.05 sessions per day. The average session file size transferred is 1 MB.

The following table describes the user model for policies.

Policies User Model

Category	Description
Conferencing, Presence, and Archiving Policies	We assume that there is one global policy, 10 tag conferencing policies, 4 Archiving policies, and 10 tag presence policies.
Voice Policy	We assume that there is one global policy and 2 tag policies per site. 100% of sites have a site policy, and 30% of users have a per-user policy assigned. We assume one dial plan per site and two routes per site.

Busy Hour

For peer-to-peer sessions, peak load is calculated using busy hour call attempts (BHCA). This voice industry term assumes that 50% of all calls for the day will be completed in 20% of the time. It is calculated using the following formula:

```
BHCA=(total calls * 0.5) / 1.6
```

Performance testing simulated busy hour by running VoIP and other peer-to-peer sessions at a busy hour load for at least 1.6 hours per day.

Conferencing peak load assumes that 75% of all conferences for an eight-hour day happen in 4 peak time hours. Those peak hours have 1.5 times the average conferencing load.

Enterprise Voice to PSTN Calls

The following assumptions apply to Enterprise Voice calls:

- 50% of users are enabled for Enterprise Voice, and 60% of these users are enabled for PSTN calling.
- Each of these users enabled for PSTN calling makes 4 PSTN calls during the busy hour. Each call duration is 3 minutes.
- 65% of these PSTN voice calls use media bypass.

Mobility

40% of registered users are assumed to be enabled for Mobility. For each user that has mobility enabled, we assume that the activity of the mobile client is additive to that of the other MPOP instances for that user, with the exception of conferencing interactions, for which the mobility client is just another client type that can be used to participate in conferences.

Persistent Chat

We assume that 25% of registered users will be involved in Persistent chat sessions, with the following characteristics:

- An average of 1.5 chat rooms per user
- Each chat room results in 12 polling requests per hour, targeting an average of 10 users each

Response Group and Call Park

We assume that 0.15% of registered users belong to response groups. We assume that 0.02% of registered users have parked calls at any given point of time.

1.3.5 Planning for High Availability and Disaster Recovery

Planning for High Availability and Disaster Recovery

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-18*

As in Lync Server 2010, the main high availability scheme for most server roles in Lync Server 2013 is based on server redundancy via pooling. If a server running a certain server role fails, the other servers in the pool running the same role take the load of that server. This applies to Front End Servers, Edge Servers, Mediation Servers, and Directors.

Lync Server 2013 adds new disaster recovery measures for Front End pools by introducing geographical dispersement of your servers into two data centers to provide continuation of service should one entire pool or site go down.

Lync Server 2013 also enhances Back End Server high availability, by supporting synchronous SQL mirroring for your Back End databases.

This section explains these major high availability and disaster recovery features, and also covers what steps you can take for high availability and disaster recovery for your other server roles as well.

In This Section

- Front End Pool High Availability and Disaster Recovery
- Edge Server High Availability and Disaster Recovery
- Planning for Enterprise Voice Resiliency
- Call Management Features for High Availability and Disaster Recovery
- Configuring Persistent Chat Server for High Availability and Disaster Recovery
- Configuring Persistent Chat Server for High Availability and Disaster Recovery
- Lync Server 2010 Metropolitan Site Resiliency

1.3.5.1 Front End Pool High Availability and Disaster Recovery

Front End Pool High Availability and Disaster Recovery

Microsoft Lync Server 2013 > Planning > Planning for High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-17*

The topics in this section explain the high availability and disaster recovery abilities Front End pools in Lync Server 2013.

- Planning for Front End Pool Pairing
- User Experience During Pool Failure
- Back End Server High Availability
- File Sharing High Availability

1.3.5.1.1 Planning for Front End Pool Pairing

Planning for Front End Pool Pairing

Planning > Planning for High Availability and Disaster Recovery > Front End Pool High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-28*

For the best disaster recovery abilities in Lync Server 2013, deploy pairs of Front End pools across two geographically dispersed sites. Each site contains a Front End pool which is paired with a corresponding Front End pool in the other site. Both sites are active, and the Lync Server Backup Service provides real-time data replication to keep the pools synchronized. The Backup Service is a new feature in Lync Server 2013, designed to support the disaster recovery solution. It is installed on a Front End pool when you pair the pool with another Front End pool.

If the pool in one site fails, you can fail over the users from that pool to the pool in the other site, which then provides services to all the users in both pools. For capacity planning purposes, each pool should be designed to handle the workloads of all users in both pools in the event of a disaster.

In This Section

- Best Practices for Pairing Front End Pools
- Backup Registrar Relationships
- Recovery Time for Pool Failover and Pool Failback
- Central Management Store Failover
- Front End Pool Pairing Data Security

1.3.5.1.1.1 Best Practices for Pairing Front End Pools

Best Practices for Pairing Front End Pools

Planning for High Availability and Disaster Recovery > Front End Pool High Availability and Disaster Recovery > Planning for Front End Pool Pairing >

Topic Last Modified: *2013-02-19*

There is no restriction on the distance between two data centers that are to include Front End pools paired with each other. We recommend that you use two data centers in the same world region, with high-speed links between them. It is best if the two data centers are separated enough to avoid a single disaster hitting both at the same time.

Having two data centers across world regions is possible, but could incur higher data loss due to latency in data replication.

When you plan which pools to pair, you must keep in mind that only the following pairings are supported:

- Enterprise Edition pools can be paired only with other Enterprise Edition pools. Similarly, Standard Edition pools can be paired only with other Standard Edition pools.
- Physical pools can be paired only with other physical pools. Similarly, virtual pools can be paired only with other virtual pools.

Neither Topology Builder nor topology validation will prohibit pairing two pools in a way that does not follow these recommendations. For example, Topology Builder allows you to pair an Enterprise Edition pool with a Standard Edition pool. However, these types of pairings are not supported.

Each pool in a pair should have the capacity to serve all users from both pools in the event of a disaster.

If you pair Enterprise Edition pools, you can also implement high availability on the Back End Servers, but for pairs of Standard Edition pools only the disaster recovery measures are available.

1.3.5.1.1.2 Backup Registrar Relationships

Backup Registrar Relationships

Planning for High Availability and Disaster Recovery > Front End Pool High Availability and Disaster Recovery > Planning for Front End Pool Pairing >

Topic Last Modified: *2012-06-28*

In addition to providing disaster recovery ability, two paired pools serve as the backup Registrars for each other. In Lync Server 2013, backup Registrar relationships between Front End pools are always 1:1 and reciprocal. This means that if P1 is the backup for P2, then P2 must be the backup for P1, and neither can be the backup for any other Front End pool. This is a change from Lync Server 2010, in which Front End pool backup relationships could be many to one.

Even though backup relationships between two Front End pools must be 1:1 and symmetrical, each Front End pool can still also be the backup registrar for any number of Survivable Branch Appliances, just as in Lync Server 2010.

Note that Lync Server 2013 does not extend disaster recovery support to users homed on a Survivable Branch Appliance. If a Front End pool that serves as the backup for a Survivable Branch Appliance goes down, users signed into the Survivable Branch Appliance fall into resiliency mode even after users homed on the Front End pool are failed over to the backup Front End pool.

1.3.5.1.1.3 Recovery Time for Pool Failover and Pool Failback

Recovery Time for Pool Failover and Pool Failback

Planning for High Availability and Disaster Recovery > Front End Pool High Availability and Disaster Recovery > Planning for Front End Pool Pairing >

Topic Last Modified: *2012-09-10*

For pool failover and pool failback, the engineering target for recovery time objective (RTO) is 30 minutes. This is the time required for the failover to happen, after administrators have determined there was a disaster and initiated the failover procedures. It does not include the time for administrators to assess the situation and make a decision, nor does it include the time for users to sign in again after failover is complete.

For pool failover and pool failback, the engineering target for recovery point objective (RPO) is 30 minutes. This represents the time measure of data that could be lost due to the disaster, due to replication latency of the Backup Service. For example, if a pool goes down at 10:00 A.M., and the RPO is 30 minutes, data written to the pool between 9:30 A.M. and 10:00 A.M.might not have replicated to the backup pool, and would be lost.

All RTO and RPO numbers in this document assume that the two data centers are located within the same world region with high-speed, low-latency transport between the two sites. These numbers are measured for a pool with 40,000 concurrently active users and 200,000 users enabled for Lync with respect to a pre-defined user model where there is no backlog in data replication. They are subject to change based on performance testing and validation.

1.3.5.1.1.4 Central Management Store Failover

Central Management Store Failover

Planning for High Availability and Disaster Recovery > Front End Pool High Availability and Disaster Recovery > Planning for Front End Pool Pairing >

Topic Last Modified: *2012-10-18*

The Central Management store contains configuration data about servers and services in your Lync 2013 deployment. It provides a robust, schematized storage of the data needed to define, set up, maintain, administer, describe, and operate a Lync 2013 deployment. It also validates the data to ensure configuration consistency.

Each Lync deployment includes one Central Management store, which is hosted by the Back End Server of one Front End pool.

When you establish a pool pairing that includes the pool hosting the Central Management store, a backup Central Management store database is set up in the backup pool, and Central Management store services are installed in both pools. At any point in time, one of the two Central Management store databases is the active master, and the other is a standby. The content is replicated by the Backup Service from the active master to the standby.

During a pool failover that involves the pools hosting the Central Management store, the administrator must fail over the Central Management store before failing over the Front End pool.

After the disaster is repaired, it is not necessary to fail back the Central Management store. After repair, the Central Management store in the original backup pool can remain as the active master.

The engineering targets for Central Management store failover are 5 minutes for recovery time objective (RTO) and 5 minutes for recovery point objective (RPO).

1.3.5.1.1.5 Front End Pool Pairing Data Security

Front End Pool Pairing Data Security

Planning for High Availability and Disaster Recovery > Front End Pool High Availability and Disaster Recovery > Planning for Front End Pool Pairing >

Topic Last Modified: *2012-10-21*

The Backup Service is a data replication mechanism introduced in Lync Server 2013 that transfers user data and conference content between two paired Front End pools continuously across two data centers for disaster recovery purposes. The user data contains user SIP URIs as well as contact lists and settings. Conference content includes Microsoft PowerPoint 2010 uploads, as well as whiteboards used in conferences. From the source pool, user data and conference content are exported from the local storage, zipped, transferred to the target Pool, where it is unzipped and imported to local storage. The Backup Service assumes that the communications link between the two data centers is within the corporate network that is protected from the Internet. It does not encrypt the transferred data between the two data centers, nor is it natively encapsulated within a secure protocol, such as HTTPS. Therefore, man-in-the-middle attack from internal personnel within the corporate network is possible.

Evaluating Security Risks

Any enterprise which deploys Lync Server 2013 across multiple data centers and uses the disaster recovery feature must ensure that cross-data center traffic is protected by their corporate Intranet. Enterprises which care about internal attack protection must secure the communication links among the data centers.

The assumption that data centers of an enterprise are protected behind the corporate Intranet is standard. There are many other types of corporate sensitive data transferred among these data centers. The enterprise's IT infrastructure is at dire risk if these cross-data center links are not protected.

While the risk of man-in-the-middle attacks within the corporate network exists, it is relatively contained as compared to exposing the traffic to the Internet. Specifically, the user data exposed by Backup Service (such as SIP URIs) are generally available to all employees within the company via other means such as the Global Address Book by Exchange or other directory software. Hence, the focus should be on securing the WAN between the two data centers when the Backup Service is used to copy data between the two paired Pools.

Mitigating Security Risks

There are many ways to enhance security protection for the Backup Service traffic, ranging from restricting access to the data centers to securing the WAN transport between the two data centers. In most cases, enterprises deploying Lync Server 2013 might already have the required security infrastructure in place. For enterprises looking for guidance, Microsoft provides solution as an example of how to build a secure IT infrastructure. However, this does not imply that it is the only solution, nor does it imply that it is the preferred solution for Lync Server. We recommend that enterprise customers choose the solution suits their specific needs, based on their IT security infrastructure and requirements.The example Microsoft solution employs IPSec and Group Policy for Server and Domain Isolation. For details, see http://go.microsoft.com/fwlink/p/?LinkId=268544. For questions and comments, contact secwish@microsoft.com.

⚠**Warning:**

IPsec is not intended as a replacement for application-level security, such as SSL/TLS. One advantage of using IPsec is that it can provide network traffic security for existing applications without having to change them.Enterprises that want to just secure the transport between the two data centers should consult their respective networking hardware vendors about ways to set up secure WAN connections by using the vendor's equipment.

1.3.5.1.2 User Experience During Pool Failure

User Experience During Pool Failure

Planning > Planning for High Availability and Disaster Recovery > Front End Pool High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-03*

If a pool is failed over, all users of the affected pool are forced to sign out and then sign into the backup pool. For a brief period users who sign into the backup pool may be in resiliency mode. In Resiliency mode, users are unable to perform tasks that would cause a persistent change on Lync Server, such as adding a contact. After the failover is complete, all users can get all services from the backup pool.

Any sessions a user has when the pool fails are disrupted, and the user must re-establish those sessions after failover to continue.

Users are not rehomed during failover or failback. Users who are homed on a pool that fails will be temporarily serviced by the backup pool. When the home pool is restored, the administrator can fail back these users to be serviced by their original home pool.

Note in Lync 2013, the Location Information Server database is not replicated to the backup pool. For best practice, the administrator should regularly back up the LIS database and use the latest backup copy to restore the LIS database in the backup pool after the failover.

User Experience During Failover

When a user is in a pool that fails, the user is logged out. Any peer-to-peer session the user was participating in is terminated, as are conferences organized by that user. The user cannot log back in until either the registrar resiliency timer expires or the administrator initiates failover procedures, whichever comes first. When the user logs back in, they will log in to the backup pool. If they log in before the failover has completed, they will be in Resiliency mode until failover is complete. Only then the user is able to establish new sessions or re-establish previous sessions.

User Experience During Failback

Pool failback can happen while an affected user is logged on to the backup pool, and the user remains logged on and working during the failback. Note that the failback process takes several minute to complete. For reference, it is expected to take up to 60 minutes for a pool of 20,000 users.

The following tables show more details about how a user with a Lync 2013 client or a Microsoft Lync 2010 client is affected during and after failback, and also how users in other pools see and interact with a user in a pool who is being failed back. Users with Microsoft Office Communicator 2007 R2 clients cannot sign in until the Front End pool is completely failed back.)

The term *affected user* refers to any user who was failed over from the home pool and is being serviced by the backup pool. By definition, any user originally homed on the backup pool is not an affected user.

User Experience for an Affected User in a Pool in Failback

User state or task	During failback	After failback completion
User state of user already logged in	User stays signed in and connected to backup pool. At some point user will be signed out and sign back in to the original home pool, in Resiliency mode.	User remains signed in and goes into regular mode.
New user logging in	User can sign in to the home pool in Resiliency mode.	User can sign in to the original home pool in regular mode.
Ongoing conferences organized by affected user	All modalities of conference are terminated. Rejoin button will appear, but no users can rejoin while the affected user is in Resiliency mode.	All modalities now work. Every participant needs to click to rejoin the conference.

Ongoing conferences organized by unaffected user	Conference continues and affected user can stay in the conference. Affected user is restricted to what he/she can do in Resiliency mode.	Conference continues, and affected user can stay in the conference and all modalities work after user exits Resiliency mode.
Scheduling or modifying scheduled meetings, creating ad-hoc conferences	Not possible while user is in Resiliency mode.	Available for all modalities.
Presence as seen by other users in the same pool	Presence unknown while user is signed into backup pool during Resiliency mode.	Shows the last presence state set by the user, and presence changes will now be reflected.
Contacts list and Address Book Service availability	Not available	Available
All peer-to-peer sessions and modalities	Available	Available

User Experience for a User Homed in an Unaffected Pool During Failback of Another Pool

User task	During failback	After failback completion
Viewing presence of affected user	Shows the last presence state set by the affected user.	Working. Unaffected users see updates made by affected users.
Ongoing conferences organized by affected user	All modalities of conference are terminated.	All modalities now work. Every participant needs to click to rejoin the conference.
Ongoing conferences organized by unaffected user	Conference continues, and affected user can stay in the conference and all modalities work.	Conference continues, and affected user can stay in the conference and all modalities work.
All peer-to-peer sessions and modalities	Available	Available

1.3.5.1.3 Back End Server High Availability

Back End Server High Availability

Planning > Planning for High Availability and Disaster Recovery > Front End Pool High Availability and Disaster Recovery >

Topic Last Modified: *2013-03-12*

To ensure high availability for your Back End Servers, you can deploy two Back End Servers for a single Front End pool, using synchronous SQL mirroring. This topology is optional, but is recommended to maintain your organization's business continuity. In the rest of this document, SQL mirroring means synchronous SQL mirroring, unless otherwise explicitly stated. Asynchronous SQL mirroring is not supported for Back End Server high availability in Lync Server 2013.

When you deploy this high availability solution, all Lync Server databases in the pool are mirrored, including the Central Management store, if it is located in this pool, as well as the Response Group application database and the Call Park application database, if those applications are running in the pool.

With SQL mirroring, you do not need to use shared storage for the servers. Each server keeps its copy of the databases in local storage.

You may choose to deploy SQL mirroring with or without a witness. We recommend using a witness because it enables failover of the Back End Server to be automatic. Otherwise, an administrator must manually invoke failover. Note that even if a witness is deployed, an administrator can manually invoke Back End Server failover, if necessary.

If you use a witness, you can use a single witness for multiple pairs of Back End Servers. There is no strict 1:1 correspondence between witnesses and pairs of Back End Servers. Deployments that use a single witness for multiple pairs of Back End Servers are not quite as resilient as topologies with a separate witness for each Back End Server pair.

Recovery Time for Automatic Back End Server Failover

For automatic Back End failover, the engineering target for recovery time objective (RTO) is 5 minutes. Because of the synchronous SQL mirroring, we do not anticipate data loss during Back End Server failures except in rare occasions when both the Front End Servers and the Back End Server go down simultaneously while data is being moved between the servers. The engineering target for recovery point objective (RPO) is 5 minutes.

User Experience During Back End Server Failure

User experience during a failure depends on the nature of the failure, and on your topology.

If you have a witness configured, and the principal fails, Back End Server failover happens automatically and quickly. Active users should not notice much interruption to their ongoing sessions.

If there is no witness configured, it will take some time for the administrator to manually invoke the failover. During that time, active users may be affected. They will continue their sessions as normal for about 30 minutes. If the primary is still not restored, or an administrator has not failed over to the backup, then users are switched to Resiliency mode, meaning that they are unable to perform tasks that require a persistent change on Lync Server (such as adding a contact).

If both the principal and the mirror Back End Servers fail, or if one of those servers and the witness fails, the Back End Server will become unavailable (even if it is the principal that is still working). In this case, active users are switched to Resiliency mode after some time.

SQL Clustering Topologies

SQL clustering topologies are not supported for new Lync Server 2013 deployments. For Back End Server high availability, SQL mirroring is the recommended and supported option.

If you are upgrading from a previous version of Lync Server and you have deployed an Enterprise Edition Front End pool that uses SQL clustering in that existing Lync Server topology, we recommend that you implement SQL Mirroring as a replacement for the existing SQL clustering deployment. However, continuing to use the existing SQL cluster with Lync Server 2013 is supported.

1.3.5.1.4 File Sharing High Availability

File Sharing High Availability

Planning > Planning for High Availability and Disaster Recovery > Front End Pool High Availability and Disaster Recovery >

Topic Last Modified: *2012-03-30*

To ensure high availability for Lync Server file sharing within a single data center, you can use the Distributed File System (DFS). DFS supports failover from one file server to another within the same data center. For a large scale deployment, we recommend that you use dedicated file servers that are paired using DFS.

Depending on your network's size, and the amount of resiliency you want, you can use one pair of servers to host all file shares in a site, or use one pair per Front End pool.

DFS is a best effort file replication mechanism, with no published recovery time objective (RTO) or recovery point objective (RPO) commitment. The failover between the DFS servers should be completed quickly, but data replication delay may prevent users from being able to continue work in progress when the failover happens.

If you use DFS and data store on the fileshare is critical, you should back up the file shares frequently, such as every 4 to 8 hours. When one file share goes down and replication is not up to date, you can use the backup to restore the content on the failed server to the other server that is paired with the server that is now unavailable.

1.3.5.2 Edge Server High Availability and Disaster Recovery

Edge Server High Availability and Disaster Recovery

Microsoft Lync Server 2013 > Planning > Planning for High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-17*

As with other server roles, the best way for you to provide high availability for your Edge Servers is to deploy multiple Edge servers in pools in each site. If one Edge Server goes down, the other servers in the pool will continue to provide Edge services.

To enable disaster recovery procedures, you must have separate Edge Server pools deployed at separate sites. You do not need to explicitly pair Edge pools together as you do with Front End pools, but having multiple Edge pools still provides the availability to carry on if one entire Edge pool goes down. The following sections provide details on disaster recovery for the various functions of Edge Servers.

Remote Access

If you have multiple sites, each with a pool of Edge Servers, and one entire Edge pool fails, the remote access services will continue to function without needing administrator actions. Remote users will automatically be routed to the Edge Servers in another site, because all Edge Server pools in your organization have the same external FQDN.

To ensure that this automatic failover will work smoothly, be sure to add every Front End pool in your organization to the publishing rules on the Reverse Proxy at each site. This way, Front End Servers in one site can communicate with Edge Servers in every other site, if the Edge Servers in the same site as the Front End Servers are unavailable.

Federation

For federation relationships with other organizations running Lync Server, inbound federation requests will continue to work. Any federation requests that come to an Edge pool that is down will fail back and then connect to an Edge pool which is running.

Outbound federation is always set up through one published Edge pool or Edge Server in the organization. If this Edge pool has gone down, you must use Topology Builder to change the outbound federation route to use an Edge pool which is still running. For details, see Failing Over the Edge Pool Used for Lync Server Federation

XMPP Federation

For XMPP federation, both outbound and inbound traffic will fail if the Edge pool which is designated as the XMPP federation gateway goes down. To make XMPP federation work again, you must change XMPP federation to use a different Edge pool. For details, see Failing Over the Edge Pool Used for XMPP Federation.

Edge Pool Fails But Front End Pool Is Still Running

If an Edge pool fails at a site, but the Front End pool at that site is still running, you will need to change the Front End pool to use a different Edge pool at a different site while that first Edge pool is down. For more information, see Changing the Edge Pool Associated with a Front End Pool.

1.3.5.3 Planning for Enterprise Voice Resiliency

Planning for Enterprise Voice Resiliency

Microsoft Lync Server 2013 > Planning > Planning for High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-22*

Voice resiliency refers to the ability of users to continue making and receiving calls if a central site that hosts Microsoft Lync Server 2010 becomes unavailable, whether through a wide area network (WAN) failure or another cause. If a central site fails, Enterprise Voice service must continue uninterrupted through seamless failover to a backup site. In the event of WAN failure, branch site calls must be redirected to a local PSTN gateway. This section discusses planning for voice resiliency in the event of central-site or WAN failure.

- Planning for Central Site Voice Resiliency
- Planning for Branch-Site Voice Resiliency

Planning for Central Site Voice Resiliency

See Also

Planning > Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency >

Topic Last Modified: *2012-09-28*

Increasingly, enterprises have multiple sites spread across the globe. Maintaining emergency services, access to help desk, and the ability to conduct critical business tasks when a central site is out of service is essential for any Enterprise Voice resiliency solution. When a central site becomes unavailable, the following conditions must be met:

- Voice failover must be provided.
- Users who ordinarily register with the Front End pool at the central site must be able to register with an alternative Front End pool. This can be done by creating multiple DNS SRV records, each of which resolves to a Director pool or Front End pool in each of your central sites. You can adjust the priority and weights of the SRV records so that users who are served by that central site get the corresponding Director and Front End pool ahead of those in other SRV records.
- Calls to and from users located at other sites must be rerouted to the PSTN.

This topic describes the recommended solution for securing central site voice resiliency.

Architecture and Topology

Planning for voice resiliency at a central site requires a basic understanding of the central role played by the Lync Server 2013 Registrar in enabling voice failover. The Lync Server Registrar is a server role that enables client registration and authentication and provides routing services. It resides along with other components on a Standard Edition server, Front End Server, Director, or Survivable Branch Appliance. A Registrar pool consists of Registrar Services running on the Front End pool and residing at the same site. The Front End pool must be load balanced. DNS load balancing is recommended, but hardware load balancing is acceptable. A Lync client discovers the Front End pool through the following discovery mechanism:

1. DNS SRV record
2. Autodiscovery Web Service (new in Lync Server 2013)
3. DHCP option 120

After the Lync client connects to the Front End pool, it is directed by the load balancer to one of the Front End Servers in the pool. That Front End Server, in turn, redirects the client to a preferred Registrar in the pool.

Each user enabled for Enterprise Voice is assigned to a particular Registrar pool, which becomes that user's primary Registrar pool. At a given site, hundreds or thousands of users typically share a single primary Registrar pool. To account for the consumption of central site resources by any branch site users that rely on the central site for presence, conferencing, or failover, we recommend that you consider each branch site user as though the user were a user registered with the central site. There are currently no limits on the number of branch site users, including users registered with a Survivable Branch Appliance.

To assure voice resiliency in the event of a central site failure, the primary Registrar pool must have a single designated backup Registrar pool located at another site. The backup can be configured by using Topology Builder resiliency settings. Assuming a resilient WAN link between the two sites, users whose primary Registrar pool is no longer available are automatically directed to the backup Registrar pool.

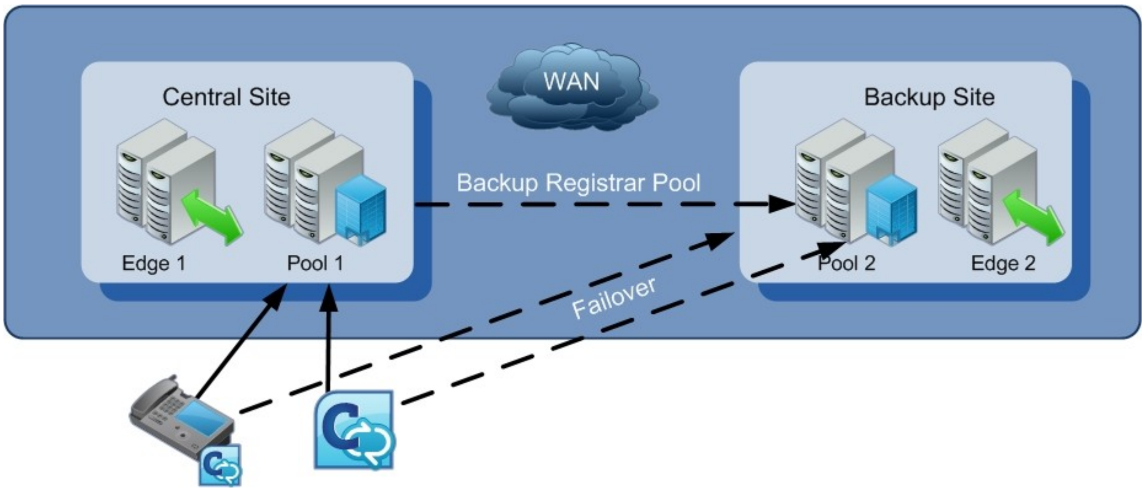
The following steps describe the client discovery and registration process:

1. A client discovers Lync Server through DNS SRV records. In Lync Server 2013, DNS SRV records can be configured to return more than one FQDN to the DNS SRV query. For example, if enterprise Contoso has three central sites (North America, Europe, and Asia-Pacific) and a Director pool at each central site, DNS SRV records can point to the Director pool FQDNs in each of the three locations. As long as the Director pool in one of the locations is available, the client can connect to the first hop Lync Server.

   Note:
   Using a Director pool is optional. A Front End pool can be used instead.

2. The Director pool informs the Lync client about the user's primary Registrar pool and backup Registrar pool.
3. The Lync client attempts to connect to the user's primary Registrar pool first. If the primary Registrar pool is available, the Registrar accepts the registration. If the primary Registrar pool is unavailable, the Lync client attempts to connect to the backup Registrar pool. If the backup Registrar pool is available and has determined that the user's primary Registrar pool is unavailable (by detecting a lack of heartbeat for a specified failover interval) the backup Registrar pool accepts the user's registration. After the backup Registrar detects that the primary Registrar is again available, the backup Registrar pool will redirect failover Lync clients to their primary pool.

The following figure shows the recommended topology for assuring central site resiliency. The two sites are connected by a resilient WAN link. If the central site becomes unavailable, users who are assigned to that pool are directed to the backup site for registration.



Requirements and Recommendations

The following requirements and recommendations for implementing central site voice resiliency are appropriate for most organizations:

- The sites in which the primary and backup Registrar pools reside should be connected by a resilient WAN link.
- Each central site must contain a Registrar pool consisting of one or more Registrars.
- Each Registrar pool must be load-balanced by using DNS load balancing or hardware load balancing.
- Each user must be assigned to a primary Registrar pool by using either the

Lync Server Management Shell **set-CsUser** cmdlet or the Lync Server Control Panel.
- The primary Registrar pool must have a single backup Registrar pool located in a different central site.
- The primary Registrar pool must be configured to fail over to the backup Registrar pool. By default, the primary Registrar is set to fail over to the backup Registrar pool after an interval of 300 seconds. You can change this interval by using the Lync Server 2013 Topology Builder.
- Configure a failover route, as described in the "Configuring a Failover Route" topic in the Planning documentation. When configuring the route, specify a gateway that is located at a different site from the gateway specified in the primary route.
- If the central site contained your primary management server and the site is likely to be down for an extended period, you will need to reinstall your management tools at the backup site; otherwise, you won't be able to change any management settings.

Dependencies

Lync Server depends on the following infrastructure and software components to assure voice resiliency:

Component	**Functional**
DNS	Resolving SRV records and A records for server-server and server-client connectivity
Exchange and Exchange Web Services (EWS)	Contact storage; calendar data
Exchange Unified Messaging and Exchange Web Services	Call logs, voice mail list, voice mail
DHCP Options 120	If DNS SRV is unavailable, the client will attempt to use DHCP Option 120 to discover the Registrar. For this to work, either a DHCP server must be configured or Lync Server 2013 DHCP must be enabled. For details, see Hardware and Software Requirements for Branch-Site Resiliency in Branch-Site Resiliency Requirements section.

Survivable Voice Features

If the preceding requirements and recommendations have been implemented, the following voice features will be provided by the backup Registrar pool:

- Outbound PSTN calls
- Inbound PSTN calls, if the telephony service provider supports the ability to fail over to a backup site
- Enterprise calls between users at both the same site and between two different sites
- Basic call handling, including call hold, retrieval, and transfer
- Two-party instant messaging and sharing audio and video between users at the same site
- Call forwarding, simultaneous ringing of endpoints, call delegation, and team call services, but only if both parties to call delegation, or all team members, are configured at the same site.
- Existing phones and clients continue to work.
- Call detail recording (CDR)

- Authentication and authorization

Depending on how they are configured, the following voice features may or may not work when a primary central site is out of service:

- Voice mail deposit and retrieval
  If you want to make Exchange UM available when the primary central site is out of service, you must do one of the following:
  - Change DNS SRV records so that the Exchange UM servers at the central site point to backup Exchange UM servers at another site.
  - Configure each user's Exchange UM dial plan to include Exchange UM servers at both the central site and the backup site, but designate the backup Exchange UM servers as disabled. If the primary site becomes unavailable, the Exchange administrator has to mark the Exchange UM servers at the backup site as enabled.

  If neither of the preceding solutions is possible, then Exchange UM will not be available in the event the central site becomes unavailable.
- Conferencing of all types
  A user who has failed over to a backup site can join a conference that is created or hosted by an organizer whose pool is available but cannot create or host a conference on his or her own primary pool, which is no longer available. Similarly, others users cannot join conferences that are hosted on the affected user's primary pool.

The following voice features do not work when a primary central site is out of service:

- Conference Auto-Attendant
- Presence and DND-based routing
- Updating call forwarding settings
- Response Group service and Call Park
- Provisioning new phones and clients
- Address Book Web Search

⊟See Also

Other Resources

Planning for Branch-Site Voice Resiliency

1.3.5.3.2 Planning for Branch-Site Voice Resiliency

Planning for Branch-Site Voice Resiliency

Planning > Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency >

Topic Last Modified: *2012-09-21*

If you want to provide branch-site resiliency, that is, high-availability Enterprise Voice service, you have three options for doing so:

- Survivable Branch Appliance
- Survivable Branch Server
- A full Lync Server deployment at the branch site

This guide will help you evaluate which resiliency solution is best for your organization and, based on your resiliency solution, which PSTN-connectivity solution to use. It will also help you prepare to deploy the solution that you choose by describing prerequisites and other planning considerations.

- Branch-Site Resiliency Features
- Branch-Site Resiliency Solutions
- Branch-Site Resiliency Requirements

1.3.5.3.2.1 Branch-Site Resiliency Features

Branch-Site Resiliency Features

Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency > Planning for Branch-Site Voice Resiliency >

Topic Last Modified: *2012-10-10*

If you provide branch-site resiliency, if a branch site's WAN connection to a central site fails or if the central site is unreachable, the following voice features should continue to be available:

- Inbound and outbound public switched telephone network (PSTN) calls
- Enterprise calls between users at both the same site and between two different sites
- Basic call handling, including call hold, retrieval, and transfer
- Two-party instant messaging
- Call forwarding, simultaneous ringing of endpoints, call delegation, and team call services, but only if the delegator and delegate (for example, a manager and the manager's administrator), or all team members, are configured at the same site
- Call detail records (CDRs)
- PSTN dial-in conferencing with Conferencing Auto-Attendant
- Voice mail capabilities, if you configure voice mail rerouting settings. (For details, see Branch-Site Resiliency Requirements.)
- User authentication and authorization

The following features will be available only if your resiliency solution is a full-scale Lync Server deployment at the branch site:

- IM, web, and A/V conferencing
- Presence and Do Not Disturb (DND)-based routing (where calls are prevented from ringing on extensions that have DND activated)
- Updating call forwarding settings
- Response Group application and Call Park application
- Provisioning new phones and clients, but only if Active Directory Domain Services (AD DS) is present at the branch site.
- Enhanced 9-1-1 (E9-1-1)
  If E9-1-1 is deployed, and the SIP trunk at the central site is not available because the WAN link is down, then the Survivable Branch Appliance will route E9-1-1 calls to the local branch gateway. To enable this feature, the branch-site users' voice policies should route calls to the local gateway in the event of WAN failure.

1.3.5.3.2.2 Branch-Site Resiliency Solutions

Branch-Site Resiliency Solutions

See Also

Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency > Planning for Branch-Site Voice Resiliency >

Topic Last Modified: *2012-09-23*

There are obvious advantages to providing branch-site resiliency to your organization. Specifically, if you lose the connection to the central site, branch site users will continue to have Enterprise Voice service and voice mail (if you configure voice mail rerouting settings; for details, see Branch-Site Resiliency Requirements). However, for sites with fewer than 25 users, a resiliency solution may not provide a sufficient return on investment.

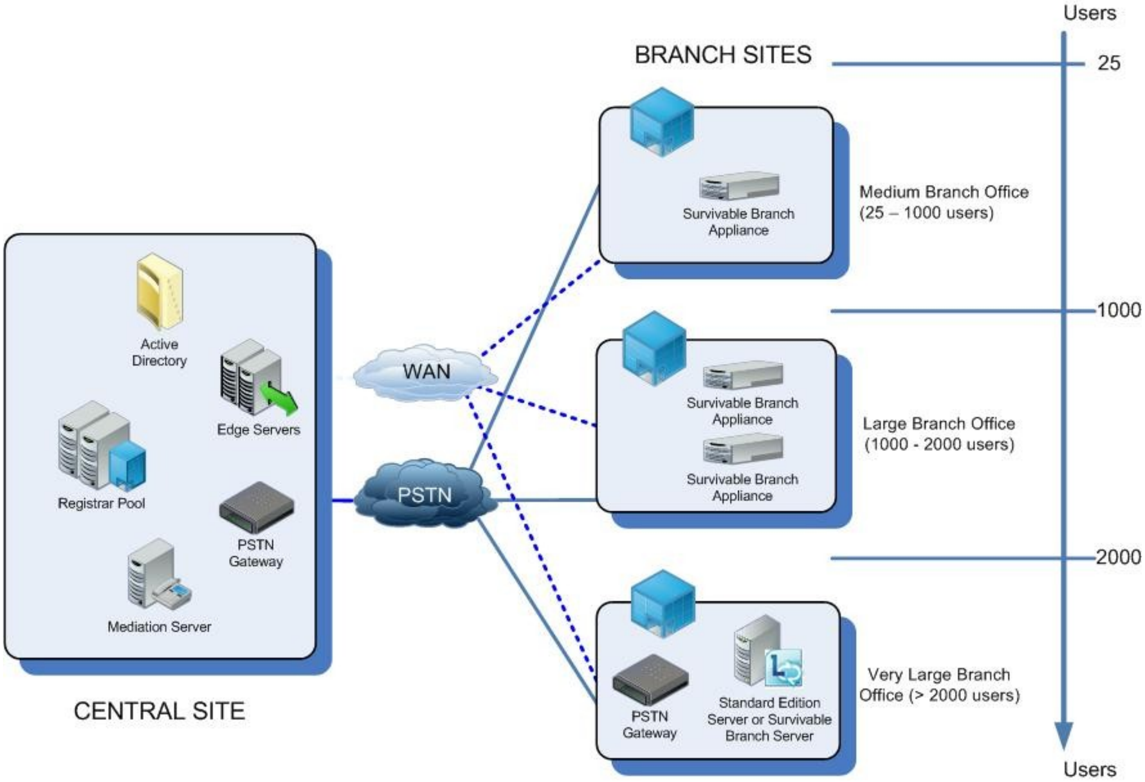
If you decide to provide branch-site resiliency, you have three options. The following table can help you determine the best option for your organization.

If you...	We recommend that you use a...
Host between 25 and 1000 users at your branch site, and if the return on investment does not support a full deployment or where local administrative support is unavailable	Survivable Branch Appliance The Survivable Branch Appliance is an industry-standard blade server with a Lync Server Registrar and Mediation Server running on Windows Server 2008 R2. The Survivable Branch Appliance also contains a public switched telephone network (PSTN) gateway. Qualified third-party devices (developed by Microsoft partners in the Survivable Branch Appliance (SBA) qualification/certification program) provide a continuous PSTN connection in the event of WAN failure, but this approach does not provide resilient presence and conferencing because these features depend on Front End Servers at the central site. For details about Survivable Branch Appliances, see "Survivable Branch Appliance Details," later in this topic. **Note:** If you decide to also use a SIP trunk with your Survivable Branch Appliance, contact your Survivable Branch Appliance vendor to learn about which service provider is best for your organization.
Host between 1000 and 2000 users at your branch site, lack a resilient WAN connection, and have trained Lync Server administrators available	Survivable Branch Server or two Survivable Branch Appliances. The Survivable Branch Server is a Windows Server meeting specified hardware requirements that has Lync Server Registrar and Mediation Server software installed on it. It must connect to either a PSTN gateway or a SIP trunk to a telephone service provider. For details about Survivable Branch Servers, see "Survivable Branch Server Details," later in this topic.
If you require presence and conferencing features in addition to voice features for up to 5000 users, and have trained Lync Server administrators available	Deploy as a central site with a Standard Edition server rather than as a branch site. A full-scale Lync Server deployment provides a continuous PSTN connection and resilient presence and conferencing in the event of WAN failure. For details about preparing for this solution, see Planning Primer: Planning for Your Organization, Determining Your System Requirements, Determining Your

	Infrastructure Requirements, and other relevant sections of the Planning documentation.

Resiliency Topologies

The following figure shows the recommended topologies for branch-site resiliency.


Users
BRANCH SITES
25
Survivable Branch Appliance
Medium Branch Office (25 – 1000 users)
1000
Survivable Branch Appliance
Survivable Branch Appliance
Large Branch Office (1000 - 2000 users)
2000
PSTN Gateway
Standard Edition Server or Survivable Branch Server
Very Large Branch Office (> 2000 users)
Users
WAN
PSTN
Active Directory
Edge Servers
Registrar Pool
PSTN Gateway
Mediation Server
CENTRAL SITE

Survivable Branch Appliance Details

The Lync Server Survivable Branch Appliance includes the following components:

- A Registrar for user authentication, registration and call routing
- A Mediation Server for handling signaling between the Registrar and a PSTN gateway
- A PSTN gateway for routing calls to the PSTN as a fallback transport in the event of a WAN outage
- SQL Server Express for local user data storage

The Survivable Branch Appliance also includes PSTN trunks, analog ports, and an Ethernet adapter.

If the branch site’s WAN connection to a central site becomes unavailable, internal branch users continue to be registered with the Survivable Branch Appliance Registrar and obtain uninterrupted voice service by using the Survivable Branch Appliance connection to the PSTN. Branch site users who connect from home or other remote locations will be able to register with a Registrar server at a central site if the WAN link to the branch site is unavailable. These users will have full unified communications functionality, with the one exception that inbound calls to the branch site will go to voice mail. When the WAN connection becomes available, full functionality should be restored to branch site users. Neither the failover to the Survivable Branch Appliance nor the restoration of service requires the presence of an IT administrator.

Lync Server supports up to two Survivable Branch Appliance at a branch site.

Survivable Branch Appliance Deployment Overview

The Survivable Branch Appliance is manufactured by original equipment manufacturers in partnership with Microsoft and deployed on their behalf by value-added retailers. This deployment should occur only after Lync Server has been deployed at the central site, a WAN connection to the branch site is in place, and branch site users are enabled for Enterprise Voice.

For details about these phases, see Deploying a Survivable Branch Appliance or Server in the Deployment documentation.

Phase	Steps	User Rights
Set up Active Directory Domain Services for the Survivable Branch Appliance	**At the central site:** 1. Create a domain user account (or enterprise identity) for the technician who will install and activate the Survivable Branch Appliance at the branch site. 2. Create a computer account (with the applicable fully qualified domain name (FQDN)) for Survivable Branch Appliance in Active Directory Domain Services. 3. In Topology Builder, create and publish the Survivable Branch Appliance.	The technician user account must be a member of RTCUniversalSBATechnicians. The Survivable Branch Appliance must belong to the RTCSBAUniversalServices group, which happens automatically when you use Topology Builder.
Install, and activate the Survivable Branch Appliance.	**At the branch site:** 1. Connect the Survivable Branch Appliance to an Ethernet port and PSTN port. 2. Start the Survivable Branch Appliance. 3. Join the Survivable Branch Appliance to the domain, using the domain user account created for the Survivable Branch Appliance at the central site. Set the FQDN and IP address to match the FQDN created in the computer account. 4. Configure the Survivable Branch Appliance using the OEM user interface. 5. Test PSTN connectivity.	The technician user account must be a member of RTCUniversalSBATechnicians.

Survivable Branch Server Details

In Topology Builder create the branch site, add the Survivable Branch Server to that site, and then run the Lync Server Deployment Wizard on the computer where you want to install the role.

⊟See Also

Other Resources

Deploying Lync Server 2013

1.3.5.3.2.3 Branch-Site Resiliency Requirements

Branch-Site Resiliency Requirements

Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency > Planning for Branch-Site Voice Resiliency >

Topic Last Modified: *2012-10-18*

This topic will help you to prepare users for branch-site resiliency and voice mail survivability, and also specifies the relevant hardware and software requirements.

Preparing Branch Users for Branch-Site Resiliency

Prepare users for branch-site resiliency by setting their Registrar pool as the Survivable Branch Appliance (SBA) or Survivable Branch Server.

Registrar Assignments for Branch Users

Regardless of which branch-site resiliency solution you choose, you will need to assign a primary Registrar to each user. Branch site users should always register with the Registrar at the branch site, regardless of whether that Registrar resides in the Survivable Branch Appliance, Survivable Branch Server, or stand-alone Lync Server 2013 Standard or Enterprise Edition server. A domain name system (DNS) service (SRV) resource record is required so that a client can discover its Registrar pool. If the Survivable Branch Appliance becomes unavailable, this is how branch site clients will automatically discover the backup Registrar.

If a branch site does not have a DNS server, there are two alternative ways to configure discovery of the Survivable Branch Appliance or Survivable Branch Server:

- Configure DHCP option 120 on the branch site’s Dynamic Host Configuration Protocol (DHCP) server to point to the fully qualified domain name (FQDN) of the Survivable Branch Appliance or Survivable Branch Server.
- Configure the Survivable Branch Appliance or Survivable Branch Server to respond to DHCP 120 queries.

Voice Routing for Branch Users

We recommend that you create a separate user-level Voice over Internet Protocol (VoIP) policy for users in a branch site. This policy should include a primary route that uses the Survivable Branch Appliance or branch server gateway, and one or more backup routes that use a trunk with a public switched telephone network (PSTN) gateway at the central site. If the primary route is unavailable, the backup route that uses one or more central site gateways is used instead. This way, regardless of where a user is registered—on the branch site Registrar or the backup Registrar pool at the central site—the user’s VoIP policy is always in effect. This is an important consideration for failover scenarios. For example, if you need to rename the Survivable Branch Appliance or reconfigure the Survivable Branch Appliance to connect to a backup Registrar pool at the central site, then you must move branch site users to the central site for the duration. (For details about renaming or reconfiguring a Survivable Branch Appliance, see Appendix B: Managing a Survivable Branch Appliance in the Deployment documentation.) If those users do not have user-level VoIP policies or user-level dial plans, when the users are moved to another site, the site-level VoIP policies and site-level dial plans of the central site apply to the users by default, instead of the branch site site-level VoIP policies and dial plans,.

In this scenario, unless the site-level VoIP policies and site-level dial plans used by the backup Registrar pool can also apply to the branch site users, their calls will fail. For example, if users from a branch site located in Japan are moved to a central site in Redmond, then a dial plan with normalization rules that prepend +1425 to all 7-digit calls is unlikely to appropriately translate calls for those users.

Important:

When you create a branch office backup route, we recommend that you add two PSTN phone usage records to the branch office user policy and assign separate routes to each one. The first, or primary, route would direct calls to the gateway associated with the Survivable Branch Appliance (SBA) or branch server; the second, or backup, route would direct calls to the gateway at the central site. In directing calls, the SBA or branch server will attempt all routes assigned to the first PSTN usage record before attempting the second usage record.

To help ensure that inbound calls to branch site users will reach those users when the branch gateway or the Windows component of the Survivable Branch Appliance site is unavailable (which would happen, for example, if the Survivable Branch Appliance or branch gateway were down for maintenance), create a failover route on the gateway (or work with your Direct Inward Dialing (DID) provider) to redirect incoming calls to the backup Registrar pool at the central site. From there, the calls will be routed over the WAN link to branch users. Be sure that the route translates numbers to comply with the PSTN gateway or other trunk peer's accepted phone number formats. For details about creating a failover route, see Configuring a Failover Route. Also create service-level dial plans for the trunk associated with the gateway at the branch site to normalize incoming calls. If you have two Survivable Branch Appliances at a branch site, you can create a site-level dial plan for both unless a separate service-level plan for each is necessary.

Note:

To account for the consumption of central site resources by any branch site users that rely on the central site for presence, conferencing, or failover, we recommend that you consider each branch site user as if the user were registered with the central site. There are currently no limits on the number of branch site users, including users registered with a Survivable Branch Appliance.

We also recommend that you create a user-level dial plan and voice policy, and then assign it to branch site users. For details, see Create a Dial Plan and Create the VoIP Routing Policy for Branch Users in the Deployment documentation.

Routing Extension Numbers

When preparing dial plans and voice policies for branch site users, be sure to include normalization rules and translation rules that match the strings and number format used in the msRTCSIP-line (or Line URI) attribute, so that Lync 2013 calls enabled between branch site users and central site users will be routed correctly—particularly when calls must be rerouted over the PSTN because the WAN link is unavailable. Additionally, there are special considerations for dialed numbers that include extension numbers, rather just phone numbers.

Normalization rules and translations rules that match Line URIs that contain an extension number, whether exclusively or in addition to a full E.164 phone number, have additional requirements. This section describes several example scenarios to route calls for Line URIs with an extension number.

If your organization does not have Direct Inward Dial (DID) phone numbers configured for individual users and the Line URI of each user is configured with *only* an extension number, internal users can call one another by dialing only an extension number. However, you must configure normalization rules that can apply to calls from a branch site user to a central site user, that match the extension numbers.

In a scenario where the WAN link between a branch site and a central site is available, calls from branch site users to central site users do not require the matching normalization rule to translate the number because the call is not routed over the PSTN. For example:

Rule name	Description	Number pattern	Translation	Example
5digitExtensions	Does not translate 5-digit numbers	^(\d{5})$	$1	10001 is not translated

You must also accommodate extension numbers for specific scenarios, such as when the WAN link between a branch site and central site is unavailable and a call from a branch site must be routed over the PSTN. During a WAN outage, if a branch site user calls a central site user only by dialing the central site user's extension, you must have an outbound translation rule that adds the central site user's full phone number. If a user's Line URI contains your organization's full phone number and the user's unique extension number instead of a full phone number that is unique to the user, then you must have an outbound translation rule that adds your organization's full phone number instead. For example:

Description	Matching pattern	Translation	Example
Translates 5-digit numbers to a user's phone number and extension	^(\d{5})$	+14255550123;ext=$1	10001 is translated to +14255550123;ext=10001
Translates 5-digit numbers to your organization's phone number and a user's extension	^(\d{5})$	+14255550100;ext=$1	10001 is translated to +14255550100;ext=10001

In this scenario, if the trunk peer that handles rerouting to the PSTN does not support extension numbers, then the outbound translation rule must also remove the extension number. For example:

Description	Matching pattern	Translation	Example
Removes extension from phone numbers with extensions	^\+(\d*);ext=(\d*)$	+$1	+14255550123;ext=10001 is translated to +14255550123

Whether or not a WAN link is available, if your organization does not have DID numbers configured for individual users and the Line URI for a user contains your organization's phone number and the user's unique extension number, then you must configure your organization's phone number Line URI with a number that is reachable by the trunk peer or PSTN gateway at the branch site. You must also configure your organization's phone number Line URI to include its own unique extension for calls to be routed to that number.

For details about calls from a central site user to a branch site user when the WAN link between the sites is unavailable, see "Preparing for Voice Mail Survivability" later in this topic. For details about dial plans and normalization rules, including other sample rules, see Dial Plans and Normalization Rules in the Planning documentation and Configuring Dial Plans in the Deployment documentation. For details about outbound translation rules, see Translation Rules in the Planning documentation and Defining Translation Rules in the Deployment documentation.

Preparing for Voice Mail Survivability

Exchange Unified Messaging (UM) is usually installed only at a central site and not at branch sites. A caller should be able to leave a voice mail message, even if the WAN link between branch site and central site is unavailable. As a result, configuring the Line URI for the Exchange UM Auto Attendant phone number that provides voice mail for branch site users requires special considerations, in addition to the voice policy, dial plan, and normalization rules applicable to that voice mail number.

Survivable Branch Appliances (SBAs) and Survivable Branch Servers provide voice mail survivability for branch users during a WAN outage. Specifically, if you are using a Survivable Branch Appliance or Survivable Branch Server and the WAN becomes unavailable, the SBA or Survivable Branch Server reroutes unanswered calls over the PSTN to Exchange UM at the central site. With a SBA or Survivable Branch Server, users can also retrieve voice mail messages through the PSTN during a WAN outage. Finally, during a WAN outage the Survivable Branch Appliance or Survivable Branch Server queues missed-call notifications and then uploads them to the Exchange UM server when the WAN is restored. To help ensure that voice mail rerouting is resilient, be sure that you add an entry for the central site pool's FQDN and an entry for the Edge Server FQDN to the hosts file on the Survivable Branch Server. Otherwise, DNS resolution can time out if you do not have a DNS server at the branch site.

We recommend the following configurations for voice mail survivability for branch site users:

- An Microsoft Exchange administrator should configure Exchange UM Auto Attendant (AA) to accept messages only. This configuration disables all other generic functionality, such as transfer to a user or transfer to an operator, and limits the AA to only accepting messages. Alternatively, the Exchange administrator can use a generic AA or an AA customized to route the call to an operator.
- The Lync Server administrator should take the AA phone number and use that phone number as the **exchange um auto attendant** number in the voice mail rerouting settings for the Survivable Branch Appliance or branch server.
- The Lync Server administrator should get the Exchange UM subscriber access phone number and use that number as the **subscriber access** number in the voice mail rerouting settings for the Survivable Branch Appliance or Survivable Branch Server.
- The Lync Server administrator should configure Exchange UM so that only one dial plan is associated with all branch users who need access to voice mail during a WAN outage.
- When the WAN link is unavailable, calls to branch site users can be routed to the user's Exchange Unified Messaging (UM) voice mailbox, but only if the voice policy applied to the call specifies a voice mail phone number that is unique and does not include an extension number.

Hardware and Software Requirements for Branch-Site Resiliency

The hardware and software requirements vary, depending on your resiliency solution.

Requirements for Survivable Branch Appliances

Required hardware and software is built into the Survivable Branch Appliance. However, we also recommend that each branch site deploy a DHCP server to obtain client IP addresses; otherwise, when the DHCP lease expires, clients will not have IP connectivity.

If the enterprise DNS servers are located only in central sites, branch site users will be unable to access them during a WAN outage, and therefore Lync Server discovery that uses DNS SRV (service (SRV) resource record) will fail. To assure prompt rerouting during a WAN outage, DNS records must be cached at the branch site. If the branch router supports it, turn on DNS caching. Or, you can deploy a DNS server at the branch. This can be a stand-alone server or a version of the Survivable Branch Appliance that supports DNS capabilities. For details, contact your Survivable Branch Appliance provider.

Note:
It is not necessary to have a domain controller at a branch site. The Survivable Branch Appliance authenticates clients by using a special certificate that it sends the client in response to the client's certificate request when it signs in.

Lync clients can discover the Lync Server by using DHCP Option 120 (SIP Registrar Option). This can be configured in one of two ways:

- Configure the DHCP server at the branch site to reply to DHCP 120 queries, which return the FQDN of the Registrar on the Survivable Branch Appliance or Survivable Branch Server.
- Turn on Lync Server DHCP. When this is turned on, the Lync Server Registrar responds to DHCP Option 120 queries. Note that the Registrar does not respond to any DHCP queries other than DHCP Options 120.

Additionally, for larger branch sites that have multiple subnets, DHCP relay agents should be enabled to forward DHCP Option 120 queries to the DHCP Server (configuration 1) or to the Registrar (configuration 2).

Finally, branch site users must be configured for Enterprise Voice and provisioned with an appropriate unified communications endpoint.

Requirements for Survivable Branch Servers

The requirements for Survivable Branch Servers are the same as the requirements for any Lync Server server role. For details, see Determining Your Infrastructure Requirements in the Planning documentation.

Requirements for Full-Scale Lync Server Branch-Site Deployments

For details, see Determining Your Infrastructure Requirements in the Planning documentation.

Configuring a Failover Route

Planning for Enterprise Voice Resiliency > Planning for Branch-Site Voice Resiliency > Branch-Site Resiliency Requirements >

Topic Last Modified: *2012-09-21*

The following example shows how an administrator can define a failover route for use if the Dallas-GW1 is down for maintenance or is otherwise unavailable. The following tables illustrate the required configuration change.

Table 1. User Policy

User policy	Phone usage
Default Calling Policy	Local GlobalPSTNHopoff
Redmond Local Policy	RedmondLocal
Dallas Calling Policy	DallasUsers GlobalPSTNHopoff

Table 2. Routes

Route name	Number pattern	Phone usage	Trunk	Gateway

Redmond Local Route	^\+1(425|206|253)(\d{7})$	Local RedmondLocal	Trunk1 Trunk2	Red-GW1 Red-GW2
Dallas Local Route	^\+1(972|214|469)(\d{7})$	Local	Trunk3	Dallas-GW1
Universal Route	^\+?(\d*)$	GlobalPSTNHopoff	Trunk1 Trunk2 Trunk3	Red-GW1 Red-GW2 Dallas-GW1
Dallas Users Route	^\+?(\d*)$	DallasUsers	Trunk3	Dallas-GW1

In Table 1, a phone usage of GlobalPSTNHopoff is added after the DallasUsers phone usage in the Dallas Calling Policy. This enables calls with the Dallas Calling policy to use routes that are configured for the GlobalPSTNHopoff phone usage if a route for the DallasUsers phone usage is unavailable.

1.3.5.4 Call Management Features for High Availability and Disaster Recovery

Call Management Features for High Availability and Disaster Recovery

See Also

Microsoft Lync Server 2013 > Planning > Planning for High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-21*

The following topics contain information about high availability and disaster recovery features for the call management features in Lync Server.

- Managing Response Groups During a Disaster
- Manage Call Park During Disaster Recovery
- Manage Announcements During Disaster Recovery

See Also

Other Resources

Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service

1.3.5.4.1 Managing Response Groups During a Disaster

Managing Response Groups During a Disaster

Planning > Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery >

Topic Last Modified: *2012-11-01*

Lync Server 2013 supports running response groups in the backup pool during disaster recovery. This section describes how to plan for response groups during an outage, how response groups work during the outage, and the steps required to fail over and fail back response groups.

- Planning for Response Group Disaster Recovery

- Response Group Experience During Pool Failure
- Response Group Disaster Recovery Procedures

1.3.5.4.1.1 Planning for Response Group Disaster Recovery

Planning for Response Group Disaster Recovery

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Managing Response Groups During a Disaster >

Topic Last Modified: *2012-11-01*

This section describes some ways to prepare response groups for disaster recovery and provides an overview of the disaster recovery process.

Preparing for Response Group Disaster Recovery

Keep the following in mind when you prepare for and carry out disaster recovery procedures.

Note:

In a coexistence environment, only the Lync Server 2013 response groups are supported for the disaster recovery procedures described in this document.

- Plan for disaster recovery when you do your capacity planning. For disaster recovery capacity, each pool in a paired pool should be able to handle the workloads of all the response groups in both pools. For details about Response Group capacity planning, see Capacity Planning for Response Group.
- Take regular backup copies of all the response group configurations in all the Front End pools where you deployed the Response Group application by using the export procedure described in this document. For details, see Response Group Disaster Recovery Procedures. Keep the backup copies in a safe location.
- Keep a separate backup copy of all the original audio files you used for the Response Group application, including any recordings and music-on-hold files. Keep the backup files in a safe location.
- For Lync Server 2013 disaster recovery, all Response Group settings must have unique names across your deployment. This requirement applies to workflows, queues, agent groups, holiday sets, and hours of business. You should verify that this requirement is met when the primary and backup pools are still active, and before you need to initiate any failover procedure. If you encounter name conflicts while importing response group data to the backup pool, the import fails. To complete the import and failover procedure, you need to resolve the name conflicts by renaming the response group object in the backup pool or by using the **Import-CsRgsConfiguration** cmdlet with the –ResolveNameConflicts parameter to automatically resolve the conflict by appending a unique identifying number to the response group object.
- In general, we recommend that you perform daily backups, but if you have a high volume of changes, you might want to schedule more frequent backups. The amount of information you can lose in the event of a disaster depends on the frequency of your backups, as well as the frequency and volume of changes.
- It is possible to import response groups to a backup pool before a disaster or failover operation occurs. Importing response groups in advance reduces downtime, because the Lync Server Response Group service can be restored in the backup pool as soon as calls are routed to the backup pool.

Note:
The Response Group application cannot reach any agents homed in an inactive pool until failover is complete. During this time, the Response Group application processes calls as if those agents are unavailable.

Response Group Disaster Recovery Process

In the event of a disaster, you can recover response groups by using either of the following recovery approaches:

- Fail over to a backup pool and then fail back to the original pool.
- Fail over to a backup pool, create a new pool with a different fully qualified domain name (FQDN), and then import the response groups to the new pool.

During the failover phase of disaster recovery, the response groups reside in multiple pools: in the primary pool (which is unavailable) and in the backup pool. The response groups in both pools have the same name and the same owner (the primary pool), but they have different parents.

When you recover by creating a new pool with a different FQDN, you need to assign the new pool as the owner of the response groups when you import them. Ownership of response groups remains with the original pool unless or until you explicitly reassign ownership by using the –OverwriteOwner parameter with the **Import-CsRgsConfiguration** cmdlet.

Note:
You also need to use the –OverwriteOwner parameter if you rebuilt the pool during the recovery (that is, the Response Group database is empty), whether or not you use the same FQDN. You do not need to use the –OverwriteOwner parameter if you did not rebuild the pool, but it is permissible to use this parameter whenever you import response groups back to the primary pool.

You can define only one set of application-level Response Group configuration settings per pool. These settings include the default music-on-hold configuration, the default music-on-hold audio file, the agent ringback grace period, and the call context configuration. To view these configuration settings, run the **Get-CsRgsConfiguration** cmdlet. For details about the **Get-CsRgsConfiguration** cmdlet, see Get-CsRgsConfiguration.

You can transfer these application-level settings from one pool to another by using the **Import-CsRgsConfiguration** cmdlet with the –ReplaceExistingSettings parameter, but doing so overrides the settings in the destination pool.

Important:
This constraint about transferring settings to another pool is true only for the application-level settings and the default music-on-hold audio file. It does not apply to agent groups, queues, workflows, business hours, and holiday sets.

If you don't want to replace the application-level settings in the backup pool during a disaster and the primary pool can't be recovered, the application-level settings from the primary pool will be lost. If you need to create a new pool to replace the primary pool during recovery, either with the same FQDN or with a different FQDN, you can't recover the original application-level settings. In this case, you need to configure the new pool with these settings and include the music-on-hold audio file.

If you decide to use the **Import-CsRgsConfiguration** cmdlet to transfer application-level settings from the primary pool to the backup pool during a disaster, you can then transfer the settings from the backup pool to the new pool during recovery in the same way that you transferred them from the primary pool to the backup pool.

The following table is an overview of the steps involved in recovering response groups.

For details about performing these steps, see Response Group Disaster Recovery Procedures.

Response Group Disaster Recovery Steps

Phase	Steps	Required groups and roles
Before outage	On a routine basis, run the **Export-CsRgsConfiguration** cmdlet to create backups of all Response Group configurations in all Front End pools where Response Group application is deployed.	RTCUniversalServerAdmins CsResponseGroupAdministrator
During outage	Run the **Import-CsRgsConfiguration** cmdlet to import the backed up Lync Server Response Group service configuration from the primary pool to the backup pool. **Note:** Use the –ReplaceExistingSettings parameter if you want to replace application-level Response Group settings in the backup pool with the settings from the primary pool. If you do not transfer the application-level settings from the primary pool to the backup pool, and the primary pool can't be recovered, you will lose the settings from the primary pool.	RTCUniversalServerAdmins CsResponseGroupAdministrator
After importing	Run Response Group cmdlets with either the –ShowAll parameter (to display all response groups) or the –Owner parameter (to display only imported response groups) to verify that all response group configurations were imported to the backup pool. **Important:** If you do not use either the –ShowAll parameter or the –Owner parameter, the response groups that you imported to the backup pool will not be listed in the results returned by the cmdlets. Run the following cmdlets: • **Get-CsRgsWorkflow** • **Get-CsRgsQueue** • **Get-CsRgsAgentGroup** • **Get-CsRgsHoursOfBusiness** • **Get-CsRgsHolidaySet**	RTCUniversalServerAdmins CsResponseGroupAdministrator
After failover	• Place a test call to a response group that was imported to the backup pool and verify that the call is	N/A

	handled correctly. • All formal agents must sign in again to their formal groups on backup pool. • Manage configuration changes: Response groups in the backup pool, whether imported to the backup pool or owned by the backup pool, can be modified as usual during the outage. **Important:** You must use Lync Server Management Shell to manage the response groups that you imported to the backup pool. You cannot use Lync Server Control Panel to manage these response groups while they are in the backup pool.	
After recovery, before failback	Run the **Export-CsRgsConfiguration** cmdlet specifying the -Source parameter as the backup pool and the –Owner parameter as the primary pool to export the response groups owned by the primary pool from the backup pool.	RTCUniversalServerAdmins CsResponseGroupAdministrator
After failback	• Run the **Import-CsRgsConfiguration** cmdlet to import the response groups back to the primary pool. **Note:** If the primary pool can't be recovered and you deploy a new pool to replace it, use the –ReplaceExistingSettings parameter to transfer the application-level settings from the backup pool to the new pool. If you do not transfer the settings from the backup pool, the new pool will use the default settings. • Run the following cmdlets with either the –ShowAll parameter (to display all response groups) or the –	RTCUniversalServerAdmins CsResponseGroupAdministrator

	Owner parameter (to display only imported response groups) to verify that all response group configurations were successfully imported back to the primary pool: - **Get-CsRgsWorkflow** - **Get-CsRgsQueue** - **Get-CsRgsAgentGroup** - **Get-CsRgsHoursOfBusiness** - **Get-CsRgsHolidaySet** - Place a test call to a response group that was imported back to the primary pool and verify that the call is handled correctly. - Optionally, run the **Export-CsRgsConfiguration** cmdlet on the backup pool with the –RemoveExportedConfiguration parameter to remove the response groups owned by the primary pool from the backup pool.	

1.3.5.4.1.2 Response Group Experience During Pool Failure

Response Group Experience During Pool Failure

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Managing Response Groups During a Disaster >

Topic Last Modified: *2012-10-30*

This section describes in detail how response group activity is affected in the following stages:

- An outage occurs in the primary pool, but failover is not yet initiated.
- Service is failed over to the backup pool.
- Service is failed back to the primary pool.

User Experience When Outage Occurs

When a pool or site outage occurs, but the administrator has not yet initiated failover, response group activity is handled as described in the following table.

Note:

During disaster recovery, calls behave differently depending on whether the primary pool response groups were imported to the backup pool during recovery. In the following table, references to imported response groups mean that primary pool response groups were imported to the backup pool during disaster recovery mode.

Outage Occurs

Type of call or user action	During outage

Calls connected to an agent	• Regular calls remain connected. • Anonymous calls are disconnected.
In progress calls not yet connected to an agent	Calls are disconnected.
New calls	• Calls are disconnected. • If response groups were imported, calls connect to backup pool, but agents homed in primary pool are unreachable.
Agent calls on behalf of response group	Feature is disabled during this stage.
Agent sign-in and agent information	• Agent groups owned by the primary pool can be viewed on agent console but agents cannot sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are not displayed on agent console.
Response group configuration	• Response groups owned by the primary pool can be viewed, depending on the availability of the primary pool's back-end database, but cannot be modified. • Response groups owned by the backup pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.

User Experience During Failover

When an administrator invokes failover to a backup pool, response group activity is handled during and after the failover as described in the following table. The first column describes the type of activity that might be taking place. The middle column describes how each activity is handled during the brief time that it takes to fail over to the backup pool. The last column describes how the activity is handled for the duration, after the failover process is complete and the backup pool is standing in for the primary pool.

Note:

During disaster recovery, calls behave differently depending on whether the primary pool response groups were imported to the backup pool during recovery. In the following table, references to imported response groups mean that primary pool response groups were imported to the backup pool during disaster recovery mode.

Failover Is Initiated

Type of call or user action	**During Failover**	**After Failover Completes**
Calls connected to an agent	• Regular calls remain connected. • Anonymous calls are disconnected.	• Regular calls remain connected. • For imported response groups, anonymous calls that have reached the backup pool remain connected.

In progress calls not yet connected to an agent	Calls are disconnected.	• If response groups were not imported, no calls are in this status. • For imported response groups, calls that have reached the backup pool remain connected.
New calls	• Calls are disconnected. • For imported response groups, calls connect to the backup pool, but agents homed in the primary pool are unreachable.	• If response groups were not imported, calls are disconnected. • For imported response groups, calls connect to the backup pool.
Agent calls on behalf of response group	Feature is disabled during this stage	• If response groups were not imported, calls fail. • For imported response groups, calls succeed.
Agent sign-in and agent information	• Agent groups owned by the primary pool can be viewed on agent console but agents cannot sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are displayed on agent console and agents can sign in.	• Agent groups owned by the primary pool can be viewed on agent console but agents cannot sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are displayed on agent console and agents can sign in.
Response group configuration	• Response groups owned by the primary pool can be viewed, depending on the availability of the primary pool's back-end database, but cannot be modified. • Response groups owned by the backup pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.	• Response groups owned by the primary pool can be viewed, depending on the availability of the back end database, but cannot be modified. • Response groups owned by the backup pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.

User Experience During Failback

When an administrator invokes failback to the primary pool, response group activity is handled during and after the failback as described in the following table.

Note:

During disaster recovery, calls behave differently depending on whether the primary pool response groups were imported to the backup pool during recovery. In the following table, references to imported response groups mean that primary pool response groups were imported to the backup pool during disaster recovery mode.

Call Handling in Failback

Type of call or user action	**During Failback**	**After Failback Completes**
Calls connected to an agent	• Regular calls remain connected. • If response groups were not imported, no anonymous calls are in this status. • For imported response groups, anonymous calls remain connected.	• Regular calls remain connected. • If response groups were not imported, no anonymous calls are in this status. • For imported response groups, anonymous calls remain connected.
In progress calls not yet connected to an agent	• If response groups were not imported, no calls are in this status. • For imported response groups, calls will be disconnected.	• If response groups were not imported, no calls are in this status. • For imported response groups, calls will be disconnected.
New calls	Calls connect to the primary pool, but agents homed in the primary pool are unreachable.	Calls connect to the primary pool.
Agent calls on behalf of response group	Feature is disabled during this stage.	Calls succeed.
Agent sign-in and agent information	• Agent groups owned by the primary pool can be viewed on agent console but agents cannot sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are displayed on agent console and agents can sign in.	• Agent groups owned by the primary pool can be viewed on agent console and agents can sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are not displayed on agent console.
Response group configuration	• Response groups owned by the primary pool can be viewed, depending on the availability of the primary pool's back-	• Response groups owned by the primary pool can be viewed and modified. • Response groups owned by the backup

	end database, but cannot be modified. • Response groups owned by the backup pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.	pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.

1.3.5.4.1.3 Response Group Disaster Recovery Procedures

Response Group Disaster Recovery Procedures

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Managing Response Groups During a Disaster >

Topic Last Modified: *2012-11-01*

During the failover phase of disaster recovery, the response groups reside in multiple pools: in the primary pool (which is unavailable) and in the backup pool. The response groups in both pools have the same name and the same owner (the primary pool), but they have different parents. During this time, Response Group cmdlets work a little differently. Be sure to use parameters as specified in the following procedure. For details about how cmdlets work during the failover phase, see NextHop blog article "Lync Server 2013: Recovering Response Groups During Disaster Recovery" at http://go.microsoft.com/fwlink/p/?LinkId=263957. This blog article also applies to the released version of Lync Server 2013.

Use the steps in the following procedure to prepare for and perform disaster recovery for Lync Server Response Group service.

To fail over and fail back Response Group

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Routinely perform backups. At the command line, type:

   ```
   Export-CsRgsConfiguration -Source "service:ApplicationServer:<primary
   ```

   For example:

   ```
   Export-CsRgsConfiguration -Source "service:ApplicationServer:primary.c
   ```

3. During an outage, after failover to the backup pool, import the response groups to the backup pool. At the command line, type:

   ```
   Import-CsRgsConfiguration -Destination "service:ApplicationServer:<bac
   ```

   If you want to replace the application-level settings in the backup pool with the settings from the primary pool, include the –ReplaceExistingSettings parameter. For example:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:back
```

Caution:
If you do not replace the settings in the backup pool and the primary pool can't be recovered, the primary pool settings will be lost. For details, see Planning for Response Group Disaster Recovery.

4. Verify that the import was successful by displaying the imported response groups. The imported response groups are still owned by the primary pool. Do the following:
   - Display all the workflows in the backup pool that are owned by the primary pool, and verify that all the primary pool workflows are included. At the command line, type:

     ```
     Get-CsRgsWorkflow -Identity "service:ApplicationServer:<back
     ```

     For example:

     ```
     Get-CsRgsWorkflow -Identity "service:ApplicationServer:backu
     ```

   - Display all the queues in the backup pool that are owned by the primary pool, and verify that all the primary pool queues are included. At the command line, type:

     ```
     Get-CsRgsQueue -Identity "service:ApplicationServer:<backup
     ```

     For example:

     ```
     Get-CsRgsQueue -Identity "service:ApplicationServer:backup.c
     ```

   - Display all the agent groups in the backup pool that are owned by the primary pool, and verify that all the primary pool agent groups are included. At the command line, type:

     ```
     Get-CsRgsAgentGroup -Identity "service:ApplicationServer:<ba
     ```

     For example:

     ```
     Get-CsRgsAgentGroup -Identity "service:ApplicationServer:bac
     ```

   - Display all the hours of business in the backup pool that are owned by the primary pool, and verify that all the primary pool hours of business are included. At the command line, type:

     ```
     Get-CsRgsHoursOfBusiness -Identity "service:ApplicationServe
     ```

     For example:

     ```
     Get-CsRgsHoursOfBusiness -Identity "service:ApplicationServe
     ```

   - Display all the holiday sets in the backup pool that are owned by the primary pool, and verify that all the primary pool holiday sets are included. At the command line, type:

     ```
     Get-CsRgsHolidaySet -Identity "service:ApplicationServer:<ba
     ```

     For example:

     ```
     Get-CsRgsHolidaySet -Identity "service:ApplicationServer:bac
     ```

   Alternatively, you can display all the response groups in the backup pool, including the ones owned by the primary pool and the ones owned by the backup pool by using the –ShowAll parameter instead of the –Owner parameter. For example:

   ```
   Get-CsRgsWorkflow -Identity "service:ApplicationServer:<backup pool FQ
   ```

   Important:
   You must use either the –ShowAll parameter or the –Owner parameter. If you do not use either of these parameters, the response groups that you imported to the backup pool will not be listed in the results returned by the cmdlets.

5. Verify that the import was successful by placing a call to an imported

response group and verifying that the call is handled correctly.

6. Request agents who are members of formal agent groups to sign in to their agent groups in the backup pool.
7. Manage and modify the imported response groups as usual.

> **Important:**
> While the response groups are in the backup pool, you need to use Lync Server Management Shell to manage them. You cannot use Lync Server Control Panel to manage the response groups that you imported to the backup pool.

8. After the primary pool is restored and failback is complete, export the primary pool response groups that were imported to the backup pool. At the command line, type:

```
Export-CsRgsConfiguration -Source ApplicationServer:<backup pool FQDN>
```

9. Import the response groups back to the primary pool. At the command line, type:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:<pri
```

For example:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:prim
```

> **Note:**
> If you rebuild a pool during recovery, whether with the same or a different fully qualified domain name (FQDN), you need to use the –OverwriteOwner parameter. As a rule of thumb, you can always use the –OverwriteOwner parameter when you import response groups back to the primary pool.

If you deployed a new pool (with the same or a different FQDN) to replace the primary pool, and you want to use the application-level settings from the backup pool for the new pool, include the –ReplaceExistingSettings parameter. At the command line, type:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:<new
```

For example:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:newp
```

> **Important:**
> If you don't want to replace the application-level settings and default music-on-hold audio file for the new pool with the settings from the backup pool, the new pool will use the default application-level settings.

10. Verify that the import back to the primary pool was successful by displaying the imported response group configuration. Do the following:
    - Display all the workflows in the primary pool, and verify that all the imported workflows are included. At the command line, type:

      ```
      Get-CsRgsWorkflow -Identity "service:ApplicationServer:<pri
      ```

      For example:

      ```
      Get-CsRgsWorkflow -Identity "service:ApplicationServer: prim
      ```

    - Display all the queues in the primary pool, and verify that all the imported queues are included. At the command line, type:

      ```
      Get-CsRgsQueue -Identity "service:ApplicationServer:<primary
      ```

      For example:

      ```
      Get-CsRgsQueue -Identity "service:ApplicationServer:primary.
      ```

    - Display all the agent groups in the primary pool, and verify that all the imported agent groups are included. At the command line, type:

      ```
      Get-CsRgsAgentGroup -Identity "service:ApplicationServer: <p
      ```

      For example:

```
Get-CsRgsAgentGroup -Identity "service:ApplicationServer:pri
```

- Display all the hours of business in the primary pool, and verify that all the imported hours of business are included. At the command line, type:

  ```
  Get-CsRgsHoursOfBusiness -Identity "service:ApplicationServe
  ```

  For example:

  ```
  Get-CsRgsHoursOfBusiness -Identity "service:ApplicationServe
  ```

- Display all the holiday sets in the primary pool, and verify that all the imported holiday sets are included. At the command line, type:

  ```
  Get-CsRgsHolidaySet -Identity "service:ApplicationServer:<p
  ```

  For example:

  ```
  Get-CsRgsHolidaySet -Identity "service:ApplicationServer:pri
  ```

11. Verify that the import was successful by placing a call to an imported response group and verifying that the call is handled correctly.
12. Optionally, remove the response groups owned by the primary pool from the backup pool. At the command line, type:

    ```
    Export-CsRgsConfiguration -Source "service:ApplicationServer:<backup p
    ```

    For example:

    ```
    Export-CsRgsConfiguration -Source "service:ApplicationServer:backup.co
    ```

    Note:
    This step creates a new file with the exported configuration, and then removes it from the backup pool.

1.3.5.4.2 Manage Call Park During Disaster Recovery

Manage Call Park During Disaster Recovery

Planning > Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-10*

Lync Server 2013 supports Call Park in the backup pool during disaster recovery. This section describes things to consider if you want to support Call Park during an outage and what happens to parked calls during the stages of an outage.

- Planning for Call Park Disaster Recovery
- Call Park Experience During Pool Failure

1.3.5.4.2.1 Planning for Call Park Disaster Recovery

Planning for Call Park Disaster Recovery

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Manage Call Park During Disaster Recovery >

Topic Last Modified: *2012-10-30*

This section describes some ways to prepare the Call Park application for disaster recovery and some considerations for the disaster recovery process.

Preparing for Call Park Disaster Recovery

Keep the following in mind when preparing for and carrying out disaster recovery procedures.

- Plan for disaster recovery when you do your capacity planning. For disaster recovery capacity, each pool in a paired pool should be able to handle the workloads of the Call Park services in both pools. For details about Call Park capacity planning, see Capacity Planning for Call Park.
- During disaster recovery, users who have been redirected to the backup pool as part of the failover process use the Call Park service running in the backup pool. Therefore, support for Call Park during disaster recovery requires the Call Park application to be deployed and enabled in both the primary pool and the backup pool.
- Each pool must have a valid range of orbit numbers for users who are homed in that pool to use for parking calls.
- Always keep a separate backup copy of any customized music on hold that has been uploaded for Call Park. These files are not backed up as part of the Lync Server 2013 disaster recovery process and will be lost if the files uploaded to the pool are damaged, corrupted, or erased.

Call Park Disaster Recovery Considerations

You can define only one set of Call Park application configuration settings and one customized music-on-hold audio file per pool. These settings include the timeout threshold, music on hold, maximum call pickup attempts, and timeout URI. To view these configuration settings, run the **Get-CsCpsConfiguration** cmdlet. For details about the **Get-CsCpsConfiguration** cmdlet, see Get-CsCpsConfiguration.

During disaster recovery, Call Park uses the Call Park application in the backup pool, so settings in the primary pool are not backed up. If the primary pool can't be recovered and you deploy a new pool to replace the primary pool, the settings from the primary pool are lost, and you need to reconfigure the Call Park settings and any customized music-on-hold audio files in the new pool.

If you deploy a new pool with a different fully qualified domain name (FQDN) to replace the primary pool, you need to reassign all the Call Park orbit ranges that were associated with the primary pool to the FQDN of the new pool. To reassign orbit ranges to the new pool, you can use either Lync Server Control Panel or the **Set-CsCallParkOrbit** cmdlet. For details about the **Set-CsCallParkOrbit** cmdlet, see Set-CsCallParkOrbit.

1.3.5.4.2.2 Call Park Experience During Pool Failure

Call Park Experience During Pool Failure

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Manage Call Park During Disaster Recovery >

Topic Last Modified: *2012-09-10*

When a Front End pool becomes unavailable due an unplanned incident, calls that have been parked but not yet retrieved are disconnected. During failover to a backup pool, users are redirected to the backup pool and are in resiliency mode. While in resiliency mode, users cannot park calls, but they can place calls on hold and transfer them. When failover is complete, calls can again be parked and retrieved as usual. During failback, users cannot park calls until they are out of resiliency mode.

During disaster recovery, users who have been redirected to the backup pool as part of the failover process use the Call Park application that is deployed in the backup pool.

Therefore, users who are redirected to the backup pool use the call park settings that are configured for the Call Park application in the backup pool.

The following table summarizes the Call Park experience through the phases of disaster recovery.

User Experience During Disaster Recovery

Call state	When outage occurs	During failover	During failback
Call not yet parked	Call remains connected, but cannot be parked.	• During failover, call cannot be parked while users are in resiliency mode, but can be put on hold and transferred. • When failover completes, call can be parked and retrieved.	• During failback, call cannot be parked while users are in resiliency mode, but can be put on hold and transferred. • When failback completes, call can be parked and retrieved.
Call parked, but not yet retrieved	Call is disconnected.	No calls in this state.	Call remains parked.
Parked call already retrieved	Call remains connected.	Call remains connected.	Call remains connected.

1.3.5.4.3 Manage Announcements During Disaster Recovery

Manage Announcements During Disaster Recovery

Planning > Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery >

Topic Last Modified: *2013-02-23*

Lync Server 2013 supports announcements for calls to unassigned numbers during outages. Restoring announcement functionality during an outage is optional. If you choose to restore announcements during an outage, you need recreate your announcement configuration in the backup pool. This section describes what you need to do if you choose to restore announcements during disaster recovery.

This section applies to unassigned number ranges that use the Announcement application. This section does not apply to unassigned number ranges that use Exchange Unified Messaging (UM) Auto Attendant.

Before an Outage

Regardless of whether you choose to use announcements during outages, you should take separate backups of any customized audio files that you configured for the Announcement application. Customized announcements are not backed up as part of the Lync Server disaster recovery process. If you do not take separate backups of the files and the files that you uploaded to the server or pool are damaged, corrupted, or erased, the files will be lost.

If you do not have backup copies of customized audio files, and the original audio files are no longer available, you can find the audio files that you configured for an Announcement application by looking in the File Store for the server or pool where you originally imported the files. You can copy all the audio files that you configured for the Announcement application from the File Store.

To copy audio files from the file store

1. At the command line, run:

   ```
   Xcopy <Source: Pool Announcement Service File Store path> <Destination
   ```

   For example:

   ```
   Xcopy "<Pool File Store Path>\X-ApplicationServer-X\AppServerFiles\RGS
   ```

   Where X-ApplicationServer-X refers to the service ID of the Application Server of the pool (for example, 1-ApplicationServer-1")

During an Outage

To use the Announcement application during an outage, you need to recreate the announcement configuration in the backup pool by performing the tasks described in this section.

> **Note:**
> We recommend that you perform these tasks after you fail over to the backup pool, because as soon as you perform step 2, the backup pool takes ownership of the unassigned number ranges.

> **Note:**
> These steps are not required for number ranges that use an Exchange UM Auto Attendant phone number.

To recreate the announcement configuration in the backup pool

1. Recreate the announcements that you deployed in the primary pool in the backup pool by doing the following:
   1.a. Import any audio files used in the primary pool to the backup pool by using the **Import-CsAnnouncementFile** cmdlet and specifying the backup pool for the Parent parameter.
   1.b. Recreate each announcement by using the **New-CsAnnouncement** cmdlet and specifying the backup pool for the Parent parameter.

   > **Note:**
   > For details about using these parameters to create announcements in the backup pool, see Create an Announcement.

2. After all announcements are recreated in the backup pool, redirect all the unassigned number ranges that use announcements in the primary pool to the recreated announcements in the backup pool.

   For each unassigned number range that uses an announcement in the primary pool, run the following:

   ```
   Set-CsUnassignedNumber -Identity "<name of number range>" -Announcemen
   ```

After the Outage

When the primary pool becomes available, you need to redirect the unassigned number ranges that you changed for the outage back to the primary pool.

> **Note:**
> These steps are not required for number ranges that use an Exchange UM Auto Attendant phone number.

To restore announcements in the primary pool

1. If you had to rebuild the primary pool during the recovery, you need to recreate the announcements in the primary pool by importing the audio files and creating announcements, just as you did in the backup pool, except that you specify the primary pool for the Parent parameter. For details, see "During an Outage" earlier in this topic.
2. For each unassigned number range that you changed for the outage, run the following:

   ```
   Set-CsUnassignedNumber [-Identity "<name of number range>"] -Announcem
   ```

3. Optionally, remove the announcements that you recreated in the backup pool. Get a list of announcements for the backup pool Announcement application. At the command line, run:

   ```
   Get-CsAnnouncement -Identity "<Service:service ID>"
   ```

   For example:

   ```
   Get-CsAnnouncement -Identity "ApplicationServer:redmond.contoso.com
   ```

   In the resulting list, locate the announcements you want to remove and copy the GUIDs. For each announcement you want to remove, run:

   ```
   Remove-CsAnnouncement -Identity "<Service:service ID/guid>"
   ```

   For example:

   ```
   Remove-CsAnnouncement -Identity "ApplicationServer:redmond.contoso.com
   ```

1.3.5.5 Configuring Persistent Chat Server for High Availability and Disaster Recovery

Configuring Persistent Chat Server for High Availability and Disaster Recovery

Microsoft Lync Server 2013 > Planning > Planning for High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-01*

The Lync Server 2013, Persistent Chat Server services use a *stretched pool* configuration for disaster recovery. A stretched pool is a pool that has computers that are distributed between two physical data centers, but are within a single logical Lync Server site.

In This Section

- Required Resources
- Using Topology Builder to Configure High Availability and Disaster Recovery
- Using a Stretched Persistent Chat Server Pool for Disaster Recovery
- SQL Server Mirroring
- Setting Up SQL Server Log Shipping for the Persistent Chat Server Primary Database
- Setting Up SQL Server Log Shipping between the Primary Mirror and the Log Shipping Secondary Database

1.3.5.5.1 Required Resources

Required Resources

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-01*

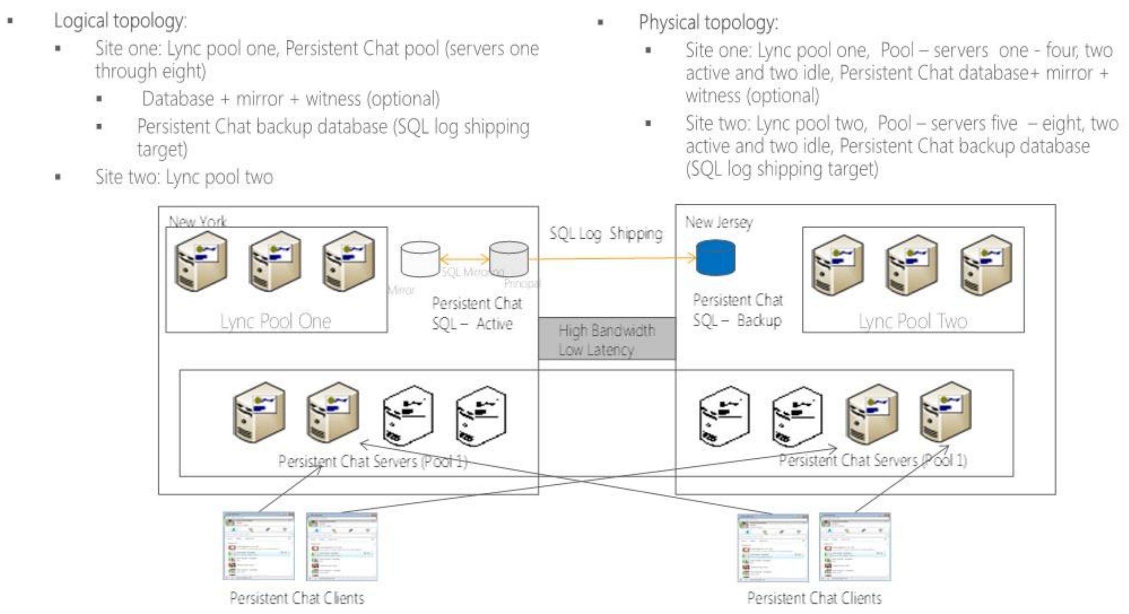
High availability and disaster recovery for Persistent Chat Server requires additional resources beyond what is typically needed for full operation. Before configuring Persistent Chat Server for high availability and disaster recovery, ensure that you have the following resources in addition to what is required for standard Persistent Chat Server operation. For additional configuration information, see Configuring Persistent Chat Server.

- One dedicated database instance located in the same physical data center in which the home front end of the Persistent Chat Server service is located. This database will serve as the SQL Server mirror for the primary Persistent Chat database. Optionally, designate an additional SQL Server to serve as the mirroring witness if you want an automated failover to the mirror database.
- One dedicated database instance located in the other physical data center. This database will serve as the SQL Server Log Shipping secondary database for the database in the primary data center.
- One dedicated database instance to serve as the SQL Server mirror for the secondary database. Optionally, designate an additional SQL Server to server as the mirroring witness. Both of these must be located in the same physical data center as the secondary database.
- If Persistent Chat Server compliance is enabled, an additional three dedicated database instances are required. Their distribution is the same as those previously outlined for the Persistent Chat database. While it is possible for the compliance database to share the same SQL Server instance as the Persistent Chat database, we recommend standalone instances for high availability and disaster recovery.
- A file share must also be created and designated for the SQL Server Log Shipping transaction logs. This share must have read/write privileges to all the SQL Server services that are running the Persistent Chat databases in both data centers. This share is not defined as part of a FileStore role.
- A file share on the secondary database server to serve as the destination folder for the SQL Server transaction logs that are copied from the primary server file share.

The following figures provide examples about how the entire Persistent Chat Server pool can be configured in the two different stretched pool topologies:

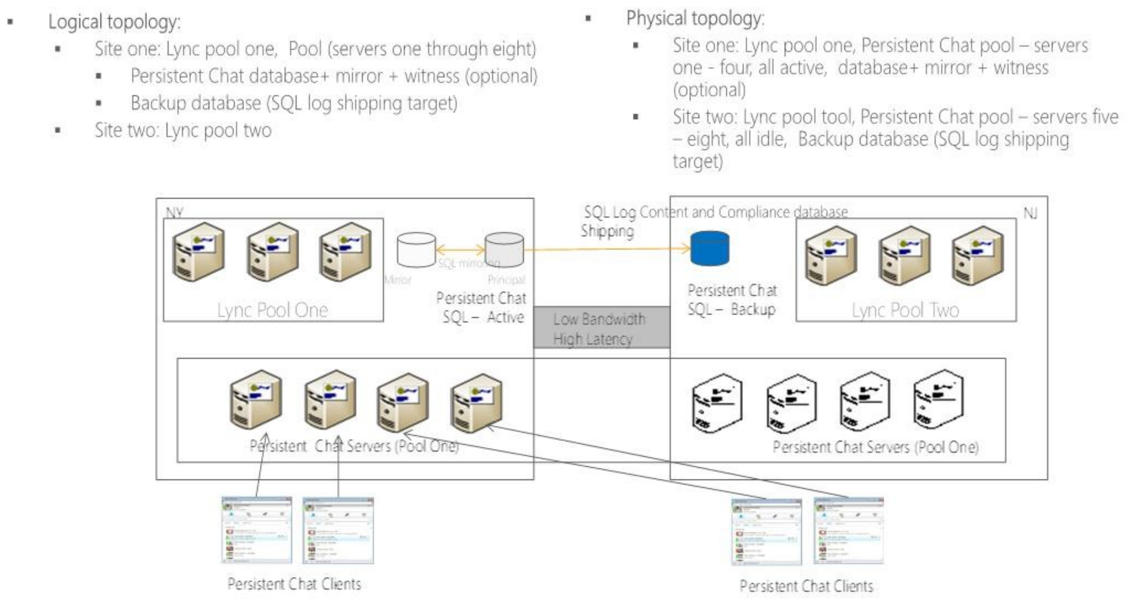
- Stretched Persistent Chat Server pool when data centers are geo-located with high bandwidth/low latency.
- Stretched Persistent Chat Server pool when data centers are geo-located with low bandwidth/high latency.

The following figure shows a stretched Persistent Chat Server pool topology where data centers are geo-located with high bandwidth/low latency.



- Logical topology:
  - Site one: Lync pool one, Persistent Chat pool (servers one through eight)
    - Database + mirror + witness (optional)
    - Persistent Chat backup database (SQL log shipping target)
  - Site two: Lync pool two
- Physical topology:
  - Site one: Lync pool one, Pool – servers one - four, two active and two idle, Persistent Chat database+ mirror + witness (optional)
  - Site two: Lync pool two, Pool – servers five – eight, two active and two idle, Persistent Chat backup database (SQL log shipping target)

The following figure shows a stretched Persistent Chat Server pool topology where data centers are geo-located with low bandwidth/high latency.



- Logical topology:
  - Site one: Lync pool one, Pool (servers one through eight)
    - Persistent Chat database+ mirror + witness (optional)
    - Backup database (SQL log shipping target)
  - Site two: Lync pool two
- Physical topology:
  - Site one: Lync pool one, Persistent Chat pool – servers one - four, all active, database+ mirror + witness (optional)
  - Site two: Lync pool tool, Persistent Chat pool – servers five – eight, all idle, Backup database (SQL log shipping target)

1.3.5.5.2 Using Topology Builder to Configure High Availability and Disaster Recovery

Using Topology Builder to Configure High Availability and Disaster Recovery

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-06*

Perform the following steps within Topology Builder to configure high availability and disaster recovery for Persistent Chat Server.

1. Add the mirror databases and the log shipping secondary database SQL Server stores.
2. Edit the Persistent Chat Server service properties to:
   2.a. Enable mirroring for the primary database.
   2.b. Add the primary mirror SQL Server store.
   2.c. Enable the SQL Server Log Shipping database.
   2.d. Add the SQL Server Log Shipping secondary SQL Server store.
   2.e. Add the SQL Server store mirror for the secondary database.
   2.f. Publish the topology.

1.3.5.5.3 Using a Stretched Persistent Chat Server Pool for Disaster Recovery

Using a Stretched Persistent Chat Server Pool for Disaster Recovery

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-06*

The disaster recovery solution for Persistent Chat Server is built on a stretched Persistent Chat Server pool. This is similar to metropolitan site resiliency in Lync Server 2010; however, there is no requirement for a stretched virtual local area network (VLAN). By stretching Persistent Chat Server pool, you essentially configure one pool in the topology logically, but you physically place the servers in the pool in two different data centers. Configure SQL Server mirroring for the database in the same way, and deploy the database and the mirror in the same data center. You need to configure a backup database in the secondary data center (with an optional mirror to provide high availability during disaster recovery). This is the backup database used for failover during disaster recovery.

For details about how to configure SQL Server mirroring for high availability, see SQL Server Mirroring. For details about failing over the database for disaster recovery, see Setting Up SQL Server Log Shipping for the Persistent Chat Server Primary Database and Setting Up SQL Server Log Shipping between the Primary Mirror and the Log Shipping Secondary Database.

1.3.5.5.4 SQL Server Mirroring

SQL Server Mirroring

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-29*

Establish the SQL Server mirroring session between the primary Persistent Chat database and its mirror. For information about how to deploy SQL Server mirroring, see Deploying SQL Mirroring for Back End Server High Availability.

1.3.5.5.5 Setting Up SQL Server Log Shipping for the Persistent Chat Server Primary Database

Setting Up SQL Server Log Shipping for the Persistent Chat Server Primary Database

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-11-12*

Using SQL Server Management Studio, connect to the Persistent Chat Server secondary Log Shipping database instance, and be sure that SQL Server Agent is running.

Using SQL Server Management Studio connected to the Persistent Chat primary database instance, perform the following steps:

1. Be sure that the SQL Server Agent is running.
2. Right-click the mgc database, and then click **Properties**.
3. Under **Select a page**, click **Transaction Log Shipping**.
4. Select the **Enable this as a primary database in a log shipping configuration** check box.
5. Under **Transaction log backups**, click **Backup Settings**.
6. In the **Network path to the backup folder** box, type the network path to the share that you created for the transaction log backup folder.
7. If the backup folder is located on the primary server, type the local path to the backup folder in the **If the backup folder is located on the primary server, type a local path to the folder (example: c:\backup)** box. (If the backup folder is not on the primary server, you can leave this box empty.)

   > **Important:**
   >
   > If the SQL Server service account on your primary server runs under the local system account, you must create your backup folder on the primary server and specify a local path to that folder.

8. Configure the **Delete files older than** and **Alert if no backup occurs within** parameters.
9. Look at the backup schedule listed in the **Schedule** box under **Backup job**. To customize the schedule for your installation, click **Schedule**, and adjust the SQL Server Agent schedule as required.
10. Under **Compression**, select **Use the default server setting**, and then click **OK**.
11. Under **Secondary server instances and databases**, click **Add**.
12. Click **Connect** and connect to the instance of SQL Server that you have configured as your secondary server.
13. In the **Secondary Database** box, select the **mgc** database from the list.
14. On the **Initialize Secondary database** tab, choose the option **Yes, generate a full backup of the primary database and restore it into the secondary database (and create the secondary database if it doesn't exist)**.
15. On the **Copy Files** tab, in the **Destination folder for copied files** box, type the path of the folder into which the transaction logs backups should be copied. This folder is often located on the secondary server.
16. Note the copy schedule listed in the **Schedule** box under **Copy job**. To customize the schedule for your installation, click **Schedule**, and adjust the SQL Server Agent schedule as required. This schedule should be approximately the same as the backup schedule.
17. On the **Restore** tab, under **Database state when restoring backups**, choose the **No recovery mode** option.
18. Under **Delay restoring backups at least:**, select **0 minutes**.
19. Choose an alert threshold under **Alert if no restore occurs within**.
20. Look at the restore schedule listed in the **Schedule** box under **Restore job**.

To customize the schedule for your installation, click **Schedule**, adjust the SQL Server Agent schedule as required, and click **OK**. This schedule should be approximately the same as the backup schedule.

21. On the **Database Properties** dialog box, click **OK** to begin the configuration process.

1.3.5.5.6 Setting Up SQL Server Log Shipping betw een the Primary Mirror and the Log Shipping Secondary Database

Setting Up SQL Server Log Shipping between the Primary Mirror and the Log Shipping Secondary Database

See Also

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2013-02-21*

Perform the following steps for log shipping to continue if the primary Persistent Chat database is failed over to its mirror database.

1. Manually fail over the primary Persistent Chat database to the mirror. This is done by using the Lync Server Management Shell and the **Invoke-CsDatabaseFailover** cmdlet. For details, see "Using Lync Server Management Shell Cmdlets" in Deploying SQL Mirroring for Back End Server High Availability.
2. Using the SQL Server Management Studio, connect to the primary Persistent Chat Server mirror instance.
3. Be sure that the SQL Server Agent is running.
4. Right-click the mgc database, and then click **Properties**.
5. Under **Select a page**, click **Transaction Log Shipping**.
6. Select the **Enable this as a primary database in a log shipping configuration** check box.
7. Under **Transaction log backups**, click **Backup Settings**.
8. In the **Network path to the backup folder** box, type the network path to the share you created for the transaction log backup folder.
9. If the backup folder is located on the primary server, type the local path to the backup folder in the **If the backup folder is located on the primary server, type a local path to the folder** box. (If the backup folder is not on the primary server, you can leave this box empty.)

◆**Important:**
If the SQL Server service account on your primary server runs under the local system account, you must create your backup folder on the primary server and specify a local path to that folder.

10. Configure the **Delete files older than** and **Alert if no backup occurs within** parameters.
11. Look at the backup schedule listed in the **Schedule** box under **Backup job**. To customize the schedule for your installation, click **Schedule**, and adjust the SQL Server Agent schedule, as required.

◆**Important:**
Use the same settings that you used for the primary database.

12. Under **Compression**, select **Use the default server setting**, and click **OK**.
13. Under **Secondary server instances and databases**, click **Add**.
14. Click **Connect**, and connect to the instance of SQL Server that you have configured as your secondary server.
15. In the **Secondary Database** box, select the **mgc** database from the list.
16. On the **Initialize Secondary database** tab, select the option **No, the**

secondary database is initialized.

17. On the **Copy Files** tab, in **Destination folder for copied files**, type the path of the folder into which the transaction logs backups should be copied, and click **OK**. This folder is often located on the secondary server.
18. Open the **Script Configuration** drop-down list, and select **Script Configuration to New Query Window**.
19. In the new query window, in **Database Properties**, click **OK** to begin the configuration process.
20. Select and run the first half of the query (see step 18) up to the line: -- ****** End: Script to be run at Primary: ******.

◆**Important:**
Manually running this script is necessary because SQL Server Management Studio does not support multiple primary databases in a SQL Server Log Shipping configuration.

21. Select **Cancel** to close the Log File shipping configuration panel and to establish a working setup that correctly implements the log file shipping for both the primary and mirrored database (in case of failover).
22. Manually fail back the primary Persistent Chat database to the primary. This is done by using the Lync Server Management Shell, and the **Invoke-CsDatabaseFailover** cmdlet. For details, see "Using Lync Server Management Shell Cmdlets" in Deploying SQL Mirroring for Back End Server High Availability.

Concepts

Deploying SQL Mirroring for Back End Server High Availability
Deploying SQL Mirroring for Back End Server High Availability

1.3.5.6 Lync Server 2010 Metropolitan Site Resiliency

Lync Server 2010 Metropolitan Site Resiliency

Microsoft Lync Server 2013 > Planning > Planning for High Availability and Disaster Recovery >

Topic Last Modified: *2013-01-15*

The metropolitan site resiliency solution supported for Lync Server 2010 is not supported for Lync Server 2013. This solution involved spanning a single Front End pool across two data centers in the same metropolitan area.

1.3.6 Planning for Manageability and Virtualization

Planning for Manageability and Virtualization

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-10-18*

This section includes topics on planning for simple management of your Lync Server 2013 deployment.

- Planning for Role-Based Access Control
- Planning for Simple URLs
- Running Lync Server on Virtual Servers

⊟Related Sections

1.3.6.1 Planning for Role-Based Access Control

Planning for Role-Based Access Control

Microsoft Lync Server 2013 > Planning > Planning for Manageability and Virtualization >

Topic Last Modified: *2012-09-14*

To enable you to delegate administrative tasks while maintaining high standards for security, Lync Server 2013 offers role-based access control (RBAC). With RBAC, administrative privilege is granted by assigning users to administrative roles. Lync Server 2013 includes a rich set of built-in administrative roles, and also enables you to create new roles and specify a custom list of cmdlets for each new role. You can also add scripts of cmdlets to the allowed tasks of both predefined and custom RBAC roles.

Better Server Security and Centralization

With RBAC, access and authorization is based precisely on a user's Lync Server role. This enables use of the security practice of "least privilege," granting administrators and users only the rights that are necessary for their job.

Important:

RBAC restrictions work only on administrators working remotely, using either the Lync Server Control Panel or Lync Server Management Shell. A user sitting at a server running Lync Server is not restricted by RBAC. Therefore, physical security of your Lync Server is important to preserve RBAC restrictions.

Roles and Scope

In RBAC, a *role* is enabled to use a list of cmdlets, designed to be useful for a certain type of administrator or technician. A *scope* is the set of objects which the cmdlets defined in a role can operate on. The objects that scope affects can be either user accounts (grouped by organizational unit) or servers (grouped by site).

The following table lists the predefined roles in Lync Server, and gives a general overview of the types of tasks each can do. The fourth column shows the similar Microsoft Exchange Server role for each Lync Server role, if there is one.

Predefined Administrative Roles

Role	Tasks allowed	Underlying Active Directory group	Exchange equivalent
CsAdministrator	Can perform all administrative tasks and modify all settings, including creating roles and assigning users to roles. Can expand a deployment by adding new sites, pools, and services.	CS Administrators	Organization Management
CsUserAdministrator	Can enable and disable users for Lync Server, move users and assign existing policies to users.	CS User Administrators	Mail Recipients

	Cannot modify policies.		
CsVoiceAdministrator	Can create, configure, and manage voice-related settings and policies.	CS Voice Administrators	Not applicable
CsServerAdministrator	Can manage, monitor, and troubleshoot servers and services. Can prevent new connections to servers, stop and start services, and apply software updates. Cannot make changes with global configuration impact.	CS Server Administrators	Server Management
CsViewOnlyAdministrator	Can view the deployment, including user and server information, in order to monitor deployment health.	CS View-Only Administrators	View-Only Organization Management
CsHelpDesk	Can view the deployment, including user's properties and policies. Can run specific troubleshooting tasks. Cannot change user properties or policies, server configuration, or services.	CS HelpDesk	HelpDesk
CsArchivingAdministrator	Can modify archiving configuration and policies.	CS Archiving Administrators	Retention Management, Legal Hold
CsResponseGroupAdministrator	Can manage the configuration of the Response Group application within a site.	CS Response Group Administrators	Not applicable
CsLocationAdministrator	Lowest level of rights for Enhanced 9-1-1 (E9-1-1) management, including creating E9-1-1 locations and network identifiers, and associating these with each other. This role is always assigned with a	CS Location Administrators	Not applicable

	global scope.		
CsResponseGroupManager	Can manage specific response groups.	CS Response Group Managers	Not applicable
CsPersistentChatAdministrator	Can manage the Persistent Chat feature and specific Persistent Chat rooms.	CS Persistent Chat Administrators	Not applicable

All predefined roles shipped in Lync Server have a global scope. To follow least privilege practices, you should not assign users to roles with global scope if they are going to administer only a limited set of servers or users. To accomplish this, you can create roles which are based on an existing role, but with a more limited scope.

Creating a Scoped Role

When you create a role with limited scope (a scoped role), you specify the scope, along with the existing role it is based on and the Active Directory group to be assigned the role. The Active Directory group you specify must already be created. The following cmdlet is an example of a creating a role which has the privileges of one of the pre-defined administrative roles, but with limited scope. It creates a new role called `Site01 Server Administrators`. The role has the abilities of the predefined CsServerAdministrator role, but only for the servers located in the Site01 site. For this cmdlet to work, the Site01 site must already be defined, and a security group named `Site01 Server Administrators` must already exist.

```
New-CsAdminRole -Identity "Site01 Server Administrators" -Template CsServerAdmini
```

After this cmdlet runs, all users who are members of the `Site01 Server Administrators` group will have server administrator privileges for the servers in Site01. Additionally, any users who are later added to this security group also gain the privileges of this role. Note that both the role itself, and the security group it is assigned to are called `Site01 Server Administrators`.

The following example limits user scope instead of server scope. It creates a `Sales Users Administrator` role to administer the user accounts in the Sales organizational unit. The SalesUsersAdministrator security group must already be created for this cmdlet to work.

```
New-CsAdminRole -Identity "Sales Users Administrator " -Template CsUserAdministra
```

Creating a New Role

To create a role that has access to a set of cmdlets not in one of the predefined roles, or to a set of scripts or modules, you again start by using one of the predefined roles as a template. Note that scripts and modules that roles are to be able to run must be stored in the following locations:

- The Lync module path, which is by default C:\Program Files\Common Files \Microsoft Lync Server 2013\Modules\Lync
- The user script path, which is by default C:\Program Files\Common Files \Microsoft Lync Server 2013\AdminScripts

To make a new role, you use the **New-CsAdminRole** cmdlet. Before running **New-CsAdminRole**, you must first create the underlying security group that will be associated with this role.

The following cmdlets serve as an example of a creating a new role. They create a new role type called `MyHelpDeskScriptRole`. The new role has the abilities of the predefined CsHelpDesk role, and can additionally run the functions in a script named “testscript”.

```
New-CsAdminRole -Identity "MyHelpDeskScriptRole" -Template CsHelpDesk -ScriptModu
```

For this cmdlet to work, you must have first created the security group MyHelpDeskScriptRole.

After this cmdlet runs, you can assign users directly to this role (in which case they have global scope), or create a scoped role based on this role, as explained in Creating a Scoped Role, previously in this document.

Assigning Roles to Users

Each Lync Server role is associated with an underlying Active Directory security group. Any users who you add to the underlying group gain the abilities of that role.

The examples in the preceding sections both created a new role and assigned an existing security group to the new role. To assign an existing role to one or more users, add those users to the group associated with the role. You can add both individual users and security groups to these groups.

For example, the **CsAdministrator** role is automatically granted to the **CS Administrators** security group in Active Directory. This security group is created in Active Directory when you deploy Lync Server. To grant a user or group this privilege, you can simply add them to the **CS Administrators** group.

A user can be given multiple RBAC roles by being added to the underlying Active Directory groups that correspond to each role.

Note that when you create a role, users who are later added to the underlying Active Directory group gain the abilities of that role.

Modifying the Abilities of a Role

You can modify the list of cmdlets and scripts that a role can run. You can modify both the cmdlets and scripts that custom roles can run, but you can modify only the scripts for predefined roles. Each cmdlet you type can add, remove, or replace cmdlets or scripts.

To modify a role, use the **Set-CsAdminRole** cmdlet. The following cmdlet both removes one script from the role.

```
Set-CsAdminRole -Identity "MyHelpDeskScriptRole" -ScriptModules @{Remove="testScr
```

Planning for RBAC

For each person who is to be given any kind of administrative rights for your Lync Server deployment, consider exactly which tasks they need to perform, then assign them to roles with the least privilege and scope necessary for their job. If necessary, you can use the **Set-CsAdminRole** cmdlet to create a new role with only the cmdlets necessary for this person’s tasks.

Users who have the CsAdministrator role can create all types of roles, including roles based on CsAdministrator, and assign users to them. The best practice is to assign the CsAdministrator role to a very small set of trusted users.

1.3.6.2 Planning for Simple URLs

Planning for Simple URLs

See Also

Microsoft Lync Server 2013 > Planning > Planning for Manageability and Virtualization >

Topic Last Modified: *2013-02-21*

Simple URLs make joining meetings easier for your users, and make getting to Lync Server administrative tools easier for your administrators.

Lync Server supports three simple URLs:

- **Meet** is used as the base URL for all conferences in the site or organization. An example of a Meet simple URL is https://meet.contoso.com. A URL for a particular meeting might be https://meet.contoso.com/*username*/7322994. With the Meet simple URL, links to join meetings are easy to comprehend, and easy to communicate and distribute.
- **Dial-in** enables access to the Dial-in Conferencing Settings webpage. This page displays conference dial-in numbers with their available languages, assigned conference information (that is, for meetings that do not need to be scheduled), and in-conference DTMF controls, and supports management of personal identification number (PIN) and assigned conferencing information. The Dial-in simple URL is included in all meeting invitations so that users who want to dial in to the meeting can access the necessary phone number and PIN information. An example of the Dial-in simple URL is https://dialin.contoso.com.
- **Admin** enables quick access to the Lync Server Control Panel. From any computer within your organization's firewalls, an admin can open the Lync Server Control Panel by typing the Admin simple URL into a browser. The Admin simple URL is internal to your organization. An example of the Admin simple URL is https://admin.contoso.com

Simple URL Scope

You can configure your simple URLs to have global scope, or you can specify different simple URLs for each central site in your organization. If both a global simple URL and a site simple URL are specified, the site simple URL has precedence.

In most cases, we recommend that you set simple URLs only at the global level, so that a user's Meet simple URL does not change if they move from one site to another. The exception would be organizations that need to use different telephone numbers for dial-in users at different sites. Note that if you set one simple URL (such as the Dial-in simple URL) at a site to be a site-level simple URL, you must also set the other simple URLs at that site to be site-level as well.

You can set global simple URLs in Topology Builder. To set a simple URL at the site level, you must use the Set-CsSimpleURLConfiguration cmdlet.

Naming Your Simple URLs

There are three recommended options for naming your simple URLs. Which option you choose has implications for how you set up your DNS A records and certificates which support simple URLs. In each option, you must configure one Meet simple URL for each SIP domain in your organization.

You always need just one simple URL in your whole organization for Dial-in, and one for Admin, no matter how many SIP domains you have.

For details about the necessary DNS A records and certificates, see DNS Requirements for Simple URLs and Certificate Requirements for Internal Servers in the Planning documentation.

In Option 1, you create a new SIP domain name for each simple URL.

If you use this option, you need a separate DNS A record for each simple URL, and each Meet simple URL must be named in your certificates.

Simple URL Naming Option 1

Simple URL	Example
Meet	https://meet.contoso.com, https://meet.fabrikam.com, and so on (one for each SIP domain in your organization)
Dial-in	https://dialin.contoso.com
Admin	https://admin.contoso.com

With Option 2, simple URLs are based on the domain name lync.contoso.com. Therefore, you need only one DNS A record which enables all three types of simple URLs. This DNS A record references lync.contoso.com. Additionally, you still need separate DNS A records for other SIP domains in your organization.

Simple URL Naming Option 2

Simple URL	Example
Meet	https://lync.contoso.com/Meet, https://lync.fabrikam.com/Meet, and so on (one for each SIP domain in your organization)
Dial-in	https://lync.contoso.com/Dialin
Admin	https://lync.contoso.com/Admin

Option 3 is most useful if you have many SIP domains, and you want them to have separate Meet simple URLs but want to minimize the DNS record and certificate requirements for these simple URLs.

Simple URL Naming Option 3

Simple URL	Example
Meet	https://lync.contoso.com/contosoSIPdomain/Meet https://lync.contoso.com/fabrikamSIPdomain/Meet
Dial-in	https://lync.contoso.com/Dialin
Admin	https://lync.contoso.com/Admin

Simple URL Naming and Validation Rules

Topology Builder and the Lync Server Management Shell cmdlets enforce several validation rules for your simple URLs. You are required to set simple URLs for Meet and Dialin, but setting one for Admin is optional. Each SIP domain must have a separate Meet simple URL, but you need only one Dialin simple URL and one Admin simple URL for your whole organization.

Each simple URL in your organization must have a unique name, and cannot be a prefix of another simple URL (for example, you could not set lync.contoso.com/Meet as your Meet simple URL and lync.contoso.com/Meet/Dialin as your Dialin simple URL). Simple URL names cannot contain the FQDN of any of your pools, or any port information (for example, https://FQDN:88/meet is not allowed). All simple URLs must start with the https:// prefix.

Simple URLs can contain only alphanumeric characters (that is, a-z, A-Z, 0-9, and the period (.). If you use other characters, the simple URLs might not work as expected.

Changing Simple URLs after Deployment

If you change a simple URL after initial deployment, you must be aware of how the change impacts your DNS records and certificates for simple URLs. If the base of a simple URL changes, then you must change the DNS records and certificates as well. For example, changing from https://lync.contoso.com/Meet to https://meet.contoso.com changes the base URL from lync.contoso.com to meet.contoso.com, so you would need to change the DNS records and certificates to refer to meet.contoso.com. If you changed the simple URL from https://lync.contoso.com/Meet to https://lync.contoso.com/Meetings, the base URL of lync.contoso.com stays the same, so no DNS or certificate changes are needed.

Whenever you change a simple URL name, however, you must run **Enable-CsComputer** on each Director and Front End Server to register the change.

⊟See Also

Concepts

DNS Requirements for Simple URLs

1.3.6.3 Running Lync Server on Virtual Servers

Running Lync Server on Virtual Servers

Microsoft Lync Server 2013 > Planning > Planning for Manageability and Virtualization >

Topic Last Modified: *2012-09-10*

Lync Server 2013 supports virtualization topologies that support all Lync Server workloads, including instant messaging (IM) and presence, conferencing, Enterprise Voice, Monitoring, Archiving, and Persistent Chat. Running on virtualized servers requires Windows Server 2012 or Windows Server 2008 R2. Lync Server 2013 virtualization supports the Hyper-V virtualization platform.

Recommended Host Server Configurations

The following table shows the recommended base hardware for a host server.

Component	Recommendation
Server	Enterprise-grade server, with a minimum of two CPU sockets
CPU	Enterprise-class CPU which can support at least 24 virtual cores.
Network adapter	Two or more 1GbE or 10 GbE adapters. For best performance, we recommend using Windows Server 2012 on a host server that supports Single Root I/O Virtualization (SR-IOV).
Storage	Two or more serial advanced technology

	attachment (SATA) or serial attached SCSI (SAS) hard disk drive, 10k rpm or higher direct attach storage (DAS), or equivalent storage. RAID 1 or equivalent SSD.
Memory	At least 32 GB. Each host server should have 4 GB for the host, as well as enough memory to support each virtual server it will run, according to the amount of memory required by each server role as listed in Server Hardware Platforms.

Both the physical host servers and all virtual servers must run one of the following operating systems. Lync Server virtualization supports a mix of operating systems. For example, a host server running Windows Server 2012 that runs virtual servers that run Windows Server 2008 R2 is supported.

- Windows Server 2012. This is the recommended operation system for both host servers and virtual servers, to enable the best performance.
- Windows Server 2008 R2 with the software update described in Microsoft Knowledge Base article 981836, "Network connectivity for a Windows Server 2003-based Hyper-V virtual machine is lost temporarily in Windows Server 2008 R2," at http://go.microsoft.com/fwlink/p/?linkId=201212.

Note:
You must run this update on both the physical host server and all virtual machines, even though the Microsoft Knowledge Base article states otherwise.

Supported Topologies

You can mix physical and virtual servers in your deployment, with only the following restrictions:

- You cannot mix different types of servers within the same pool. All servers within the same pool must either be physical or virtual. For these purposes, Front End Servers and SQL Servers running the back-end database are considered to be separate, meaning that you can have virtual Front End Servers using a physical back-end database, or physical Front End Servers and a virtual back-end database. Note however that the back-end database has a real-time requirement for presence updates, which is unlike many SQL Server applications. If you run a virtual back-end database you must be aware of performance issues, especially if the host of the virtual back-end database is running other applications.
  This is the only limitation to mixing physical and virtual servers. You could have some Front End pools of physical servers and others of virtual servers. And you can deploy different types of pools and servers as either physical or virtual in any combination.
- All servers within one pool should provide about the same performance. For example, if you have virtual Front End Servers in one pool being hosted on different host servers, you should make sure each virtual Front End Server is capable of a similar level of performance.

If you are deploying a large amount of virtualized servers across different host servers, you should consider spreading out the members of one pool across different host servers. For example, in a pool of eight virtual Front End Servers, deploy four on one physical host and four on another. While this is not a true high-availability solution, it does provide some protection if a single host server fails.

Lync Server supports the use of virtual clustered storage. However, live migration (and other types of migration) of virtual servers running Lync Server is not supported. As with physical servers, Lync Server 2013 virtual servers do not support SQL clustering.

Networking Considerations

Lync Server provides real-time communications, and depends on fast and efficient networking. If a packet is delayed by as little as a few milliseconds, users might detect an audio glitch, experience a delayed call, or frozen video. To improve the network performance of your virtualized topology, you should do the following:

- The host must have at least one network adapter dedicated to the virtual machines running Lync Server roles. Sharing a network adapter with the host or with a storage area network (SAN) is not recommended.
- Note that a Lync Server workload that includes media can reach a peak network utilization of more than 500 Mbps.
- If one host server is running multiple guest virtual servers that each run Lync Server media workloads, ensure that the host network adapter can handle the traffic. To prevent bottlenecks, consider a higher speed network adapter (such as 10 GbE) or multiple network adapters using link aggregation.
- For best performance, use the Single Root I/O Virtualization (SR-IOV) capabilities of Windows Server 2012 Hyper-V. With SR-IOV, the virtual function of a physical network adapter is assigned directly to a virtual machine. This increases network throughput and reduces network latency while also reducing the host CPU overhead that is required for processing network traffic. To take advantage of SR-IOV, you must use a host server which has BIOS which supports SR-IOV, as well as use network adapters that support SR-IOV. Additionally, you must run Windows Server 2012 on both the host server and all virtual servers.
- Enable virtual LAN (VLAN) tagging on the network adapter, and implement multiple VLANs on the virtual servers to optimize network traffic.
- Implement multi-path I/O (MPIO) to your back-end database.

Managing Your Virtual Environment

We recommend you use Microsoft System Center Virtual Machine Manager (VMM) to manage your virtualized Lync Server topology.

By using VMM, you do not need to use Terminal Services or Remote Desktop Services for the virtual machine management. Additionally, by using VMM you can view and manage performance, and other components such as disk space. You can also save a virtual machine as a template for creating new instances.

VMM uses Windows PowerShell, so you can create VMM Windows PowerShell scripts that integrate with Lync Server Management Shell to manage Lync Server.

For details about VMM, see the System Center Virtual Machine Manager website at http://go.microsoft.com/fwlink/p/?linkId=202887.

Getting Started Using VMM

To get started using VMM to manage your virtualized Lync Server topology, do the following:

1. In VMM, create a new host group named `LS 2013`.
2. In the **Actions** pane, click **Add Host**.
3. If your virtual environment is part of your Active Directory domain, select that option. Otherwise, select the Windows Server-based host on a perimeter network, and click **Next**.
4. Install a VMM Agent on the host server. If the host server is on a perimeter network, you must create a security key, which must then be available to the

VMM Administrative Console.

5. Go back to the VMM Administrative Console and click **Add Host**.
6. Specify the machine name and the domain/machine name and security key, making sure that VMM can find the host, and then click **Next**.
7. After the host has been added, the four virtual machines should be available. In the VMM Administrative Console, click the **Virtual Machines** button.
8. You will now see the Virtual Machines view, with the four virtual machines running Lync Server listed.

1.3.7 Planning for Front End Servers, Instant Messaging, and Presence

Planning for Front End Servers, Instant Messaging, and Presence

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-13*

Front End Servers provide much of the Lync Server functionality and are included in every Lync Server deployment. Instant messaging (IM) and presence are core capabilities of Lync Server and are automatically deployed and enabled in every Lync Server installation. The following sections provide more details about Front End Servers, IM and presence.

- Features and Functionality of Front End Servers, Instant Messaging, and Presence
- Defining Your Requirements for Front End Servers, Instant Messaging, and Presence
- Topologies and Components for Front End Servers, Instant Messaging, and Presence
- Technical Requirements for Front End Servers, Instant Messaging, and Presence

1.3.7.1 Features and Functionality of Front End Servers, Instant Messaging, and Presence

Features and Functionality of Front End Servers, Instant Messaging, and Presence

Microsoft Lync Server 2013 > Planning > Planning for Front End Servers, Instant Messaging, and Presence >

Topic Last Modified: *2012-09-25*

Front End Servers provide most Lync Server functionality. There are two editions available: Lync Server Enterprise Edition, which is designed primarily for larger organizations, and Lync Server Standard Edition, which is designed primarily for smaller organizations which want a smaller hardware investement and do not require high availability. Both editions support all Lync Server workloads including IM, presence, conferencing, and Enterprise Voice.

Instant messaging (IM) enables your users to communicate with each other in real time on their computers using text-based messages. Both two-party and multiparty IM sessions are supported. A participant in a two-party IM conversation can add a third participant to the conversation at any time. When this happens, the Conversation window changes to support conferencing features.

Presence provides information to users about the status of other on the network. A user’s presence status provides information to help others decide whether they should try to contact the user and whether to use instant messaging, phone, or email. Presence encourages instant communication when possible, but it also provides information about whether a user is in a meeting or out of the office, indicating that instant communication is not possible. This presence status is displayed as a presence icon in Lync and other presence-aware applications, including the Microsoft Outlook messaging and collaboration client, Microsoft SharePoint technologies, Microsoft Word, and Microsoft Excel spreadsheet software. The presence icon represents the user's current availability and willingness to communicate.

1.3.7.2 Defining Your Requirements for Front End Servers, Instant Messaging, and Presence

Defining Your Requirements for Front End Servers, Instant Messaging, and Presence

Microsoft Lync Server 2013 > Planning > Planning for Front End Servers, Instant Messaging, and Presence >

Topic Last Modified: *2013-01-11*

The main task of planning for instant messaging (IM) and presence is ensuring that you have enough Front End Servers for your users.

Enabling Communication with External Users

You can greatly increase the benefits of your investment in Lync Server by enabling your users to communicate with external users. External users can include:

- **Remote users** Your organization's own users, when they are working outside your firewalls and are using their laptops or other Lync Server devices.
- **Federated users** Users from companies you work with who also run Lync Server. To enable your users to easily contact these users, you create federated relationships with these companies.
- **Public users** Users of public IM services, such as IM services provided by the Windows Live network of Internet services, Yahoo!, and AOL, and users of providers and servers that use Extensible Messaging and Presence Protocol (XMPP), such as Google Talk.

Note:

Note that a separate license might be required for public IM connectivity with Windows Live, AOL, and Yahoo!

Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation

with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

To enable any or all of these scenarios, you need to deploy an Edge Server to help enable secure communications between your Lync Server deployment and external users. Your organization's remote users and users at federated organizations will be able to see each other's presence and communicate using IM. For details about enabling communication with external users, see Planning for External User Access in the Planning documentation.

Archiving IM Content

Lync Server provides features you can use if your organization must follow compliance regulations. You can use Archiving to archive the content of IM messages for all users in your organization or for only certain users that you specify. For details, see Planning for Archiving in the Planning documentation.

If you also have Microsoft Exchange Server 2013 deployed, you can integrate the archiving of Exchange data with the archiving of Lync Server data, and use a single tool to search both types of archived data. For more information, see Configuring Microsoft Lync Server 2013 to Use Microsoft Exchange Server 2013 Archiving.

1.3.7.3 Topologies and Components for Front End Servers, Instant Messaging, and Presence

Topologies and Components for Front End Servers, Instant Messaging, and Presence

Microsoft Lync Server 2013 > Planning > Planning for Front End Servers, Instant Messaging, and Presence >

Topic Last Modified: *2012-11-02*

The only components required for instant messaging (IM) and presence are:

- Your organization's Front End Servers or Standard Edition servers. IM and presence capabilities are always enabled on these servers.
- A load balancer, if you have an Enterprise Edition Front End pool. For more information, see Load Balancing Requirements.

Planning for the Deployment of Front End Pools

In Lync Server 2013, Front End pool architecture has changed, and these changes affect how you should plan and maintain your Front End pools.

We recommend that all your Enterprise Edition Front End pools include at least three Front End Servers. In Lync Server, the architecture of Front End pools uses a distributed systems model, with each user's data kept on three Front End servers in the pool. For more information about this new architecture, see Topology Changes.

If you do not want to deploy three Enterprise Edition Front End Servers and want high availability and disaster recovery, we recommend you use Lync Server Standard Edition and create two pools with a paired backup relationship. This will provide the best high availability and disaster recovery solution with only two servers. For more information, on high availability and disaster recovery topologies and features, see Planning for High Availability and Disaster Recovery.

Planning for the Management of Front End Pools

For pools that contain three or more Front End Servers, follow these guidelines:

- When you start the pool for the first time, be sure to start at least three of the Front End Servers.
- When you move users to the pool for the first time, be sure at least three of the Front End Servers are running.
- If you establish a pairing relationship between this pool and another pool for disaster recovery purposes, then after establishing that relationship you must be sure this pool has three Front End Servers running simultaneously at some time to properly synchronize data with the backup pool. For more information on pool pairing and disaster recovery features, see Planning for High Availability and Disaster Recovery.

For a Front End pool to be functional, a certain number of Front End Servers in the pool need to be up and running, as shown in the table later in this section. When you plan upgrade and maintenance of a pool, you must keep this in mind. Overall, for upgrades of Front End Servers, we recommend you upgrade one server at a time. Bring one server down, apply the upgrade, then bring that server back up before upgrading another server. For detailed instructions for upgrading a Front End Server, see Upgrade or Update Front End Servers.

Total number of Front End Servers in the pool	Number of servers that must be running for pool to be functional
1-2	1
3-4	2
5-6	3
7-8	4
9-10	5
11-12	6

If the number of servers running falls below the functional level as shown in this table, the remaining servers in the pool go into survivability mode, and you will see the following message in the event log: `Local Pool Manager has been disconnected from Pool Fabric Manager. (Id: 32163)`. After five minutes, if the number of running servers is still below the threshold level, the remaining servers in the pool will stop all Lync Server services, and the following messages will be in the event log: `Pool Manager failed to connect to Fabric Pool Manager (id: 32170) Server is being shutdown because fabric pool manager could not be initialized (id: 32173)`

Changing a Front End Pool's Configuration

Whenever you add Front End Servers to a pool, or remove them from the pool, and then publish the new topology, follow these guidelines:

- After the new topology has been published, you must restart each Front End Server in the pool. Restart them one at a time.
- If the entire pool has been down during the configuration change, then run the following cmdlet after the new topology is published:

```
Reset-CsPoolRegistrarState -PoolFQDN <PoolFQDN> -ResetType ServiceReset
```

If a Front End Server fails and is unlikely to be replaced for a few days or more, remove the server from the topology. Add the new Front End Server to the topology when it is available again.

Front End Pools with Two Front End Servers

We do not recommend deploying a Front End pool that contains only two Front End Servers. If you do ever need to deploy such a pool, follow these guidelines:

- If one of the two Front End Servers goes down, you should try to bring the failed server back up as soon as you can. Similarly, if you need to upgrade one of the two servers, bring it back online as soon as the upgrade is finished.
- If for some reason you need to bring both servers down at the same time, do the following when the downtime for the pool is finished:
  - The best practice is to restart both Front End Servers at the same time.
  - If the two servers cannot be restarted at the same time, you should bring them back up in the reverse order of the order they went down.
  - If you cannot bring them back up in that order, then use the following cmdlet before bringing the pool back up:.

```
Reset -CsPoolRegistrarState -ResetType QuorumLossRecovery -Po
```

1.3.7.4 Technical Requirements for Front End Servers, Instant Messaging, and Presence

Technical Requirements for Front End Servers, Instant Messaging, and Presence

Microsoft Lync Server 2013 > Planning > Planning for Front End Servers, Instant Messaging, and Presence >

***Topic Last Modified:** 2012-09-18*

Instant messaging (IM) and presence always run on Enterprise Edition Front End pools and Standard Edition servers. For information on supported hardware, operating systems, and database software, see the following:

- Supported Hardware
- Server Software and Infrastructure Support

Supported Collocation

The Front End Server role can be collocated with Mediation Server. You can also run Monitoring and Archiving on Front End Servers. Front End Server cannot be collocated with Edge Server or Director.

1.3.8 Planning for Conferencing

Planning for Conferencing

Microsoft Lync Server 2013 > Planning >

***Topic Last Modified:** 2013-01-29*

Lync Server 2013 offers a rich set of conferencing capabilities:

- Web conferencing, which includes document collaboration, application sharing, and desktop sharing. Lync Server 2013 uses Office Web Apps and the Office Web Apps Server to handle sharing and rendering of PowerPoint presentations. For details about installing and configuring the Office Web Apps Server, see Configuring Integration with Office Web Apps Server and Lync Server 2013.
- Audio/video (A/V) conferencing, which enables users to have real-time audio or video conferences without the need for external services such as the Microsoft Live Meeting service or a third-party audio bridge.
- Dial-in conferencing, which allows users to join the audio portion of a Lync Server 2013 conference by using a public switched telephone network (PSTN) phone without requiring a third-party audio conferencing provider.
- Instant messaging (IM) conferencing, in which more than two parties communicate in a single IM session. For details about IM conferencing, see Planning for Front End Servers, Instant Messaging, and Presence.

Lync Server 2013 supports both scheduled conferences and impromptu conferences.

When you deploy Lync Server 2013, Front End Server, you can choose whether to also deploy the web conferencing, A/V conferencing, and dial-in conferencing capabilities. IM conferencing capabilities are always automatically deployed along with IM conversation capabilities on Lync Server 2013 Front End Servers.

Note:

If your deployment includes meetings organized using Office Communicator 2007 R2 clients (including the Live Meeting console or Conferencing Add-in for Microsoft Office Outlook), the meetings will have the following limitations after they are migrated to Lync Server 2013:

- Users in the meeting will not be able to use data collaboration features, including document collaboration, application sharing, and desktop sharing.
- Stability issues may arise since Office Communicator 2007 R2 clients are not supported with Lync Server 2013.

To avoid these issues, reschedule any meeting organized using Office Communicator 2007 R2 clients with Outlook 2010 or Outlook 2013 using either the Online Meeting Add-in for Lync 2010 or Online Meeting Add-in for Lync 2013.

The following sections describe what is required to deploy the various types of conferencing capabilities, including the planning process, components, hardware and software requirements, and the deployment process.

- Overview of Conferencing
- Defining Your Requirements for Conferencing
- Components and Topologies for Conferencing
- Technical Requirements for Conferencing
- Deployment Checklist for Conferencing
- Support for Large Meetings

1.3.8.1 Overview of Conferencing

Overview of Conferencing

Microsoft Lync Server 2013 > Planning > Planning for Conferencing >

Topic Last Modified: *2012-09-30*

When you deploy conferencing, you can choose to enable and use both web conferencing and A/V conferencing, or just web conferencing. Dial-in conferencing is a subset of audio conferencing and requires additional configuration.

With all forms of conferencing enabled, your users can enjoy the richest possible conferencing environment with any combination of instant messaging (IM), audio, video, desktop sharing, slide presentations, sharing attachments, and sharing applications. Conferences can be scheduled or unscheduled, and users can easily add forms of communication to a conference while it happens. For example, starting with IM, adding document collaboration, and then adding voice or video. New participants can also be added to ongoing conferences in real time.

The following topics provide an overview of the specific features and capabilities provided by web conferencing, A/V conferencing, and dial-in conferencing.

- Common Conferencing Concepts
- Web Conferencing Overview
- A/V Conferencing Overview
- Dial-In Conferencing Overview

1.3.8.1.1 Common Conferencing Concepts

Common Conferencing Concepts

Planning > Planning for Conferencing > Overview of Conferencing >

Topic Last Modified: *2012-09-19*

Several concepts are common to all types of conferencing. These are described in the following sections.

Policies and Bandwidth Management

Lync Server 2013 enables administrators to set policies for the types of meetings that users can organize. This helps you enforce your organization’s policies and control bandwidth usage. You can define a wide variety of meeting policies, and assign them to individual users and groups of users. You can also set policies that govern peer-to-peer conversations. For details about setting conferencing policies, see Conferencing Policies in the Operations documentation. For details about bandwidth management, see Overview of Call Admission Control and Configuring Video Bandwidth in Lync Server 2013.

Archiving and Compliance Features

Lync Server 2013 provides features you can use if your organization must follow compliance regulations. You can use the archiving abilities to archive content presented in meetings, and also the content of instant messaging (IM) conversations and IM conferences. For details, see Planning for Archiving in the Planning documentation. You can use compliance features of Persistent Chat Server to archive multiparty, topic-based conversations that persist over time. For details, see Planning for Persistent Chat Server in the Planning documentation.

Monitoring Feature

The Monitoring Server feature can capture call detail records (CDRs), which you can use to track which users talk to which other users using Lync Server 2013. For details about deploying and configuring monitoring, see Deploying Monitoring.

Enabling External Participation in

Conferences

You can greatly increase the benefits of your investment in Lync Server 2013 conferencing by enabling external users to also participate in conferences when invited. External users can include:

- **Remote Users** Your organization's own users, when they are working outside your firewalls and are using their laptops or other Lync Server 2013 devices.
- **Federated Users** Users from companies you work with who also run Lync Server 2013. To enable your users to easily contact these users, you create federated relationships with these companies.
- **Anonymous Users** Any other external users who are invited specifically by your users to join specific conferences. A meeting organizer in your company can send an email invitation for a conference to an external user. The email includes a link that the outside user can click to join the conference.

To enable any or all of these scenarios, you need to deploy an Edge Server to help enable secure communications between your Lync Server 2013 deployment and external users. The Lync Server 2013 solution using Edge Servers provides higher quality media than other solutions such as a virtual private network (VPN). For details, see Planning for External User Access.

Additionally, whether or not you deploy Edge Servers, you can enable users (that is, either inside or outside your organization) to dial in from standard PSTN phones to join on-premises audio conferences. This is accomplished by deploying Lync Server 2013 dial-in conferencing.

Compatibility Among Meeting Types and Client Versions

If you are going to have Lync Server 2013 interoperate with previous versions of Office Communications Server and its clients, you must be aware of the following issues:

- Users using Lync Server 2013 cannot schedule Live Meeting conferences, or modify any migrated meetings of this type.
- Users using Lync Server 2013 who need to attend Live Meeting conferences hosted on servers running Office Communications Server 2007 R2 must have the Live Meeting client installed on their computer (in addition to Lync Server 2013) to attend these meetings.
- When Live Meeting conferences are migrated to Lync Server 2013, meeting content does not migrate. If this content is needed, it must be uploaded again.

1.3.8.1.2 Web Conferencing Overview

Web Conferencing Overview

Planning > Planning for Conferencing > Overview of Conferencing >

Topic Last Modified: *2012-09-30*

With web conferencing, users can share and collaborate on documents, such as PowerPoint presentations, during their conferences. Additionally, users can share all or part of their desktops with each other in real time, making it seem as though the people in the conference were gathered around the same table in the meeting.

Whiteboard and Annotations

A whiteboard is a blank canvas that can be used for collaboration, with text, ink, drawings and images. Annotations made on whiteboards can be seen by all meeting participants. The whiteboard feature enhances collaboration by enabling meeting participants to discuss ideas, brainstorm, take notes, and so on.

Polling

The polling feature enhances collaboration by enabling presenters to quickly determine participants' preferences. During online meetings and conversations, presenters can use polling to gather anonymous responses from participants. All presenters can see the results and can either hide the results or show them to all attendees.

Application Sharing and Desktop Sharing

During a conference you can share your entire desktop, an individual application, or individual monitors in a multi-monitor environment. Aside from just viewing the content, other participants in the conference can also request control of your screen and, with the permission, interact with the content (including scrolling and editing).

Note:

Participants who are viewing the conference can also take over and start sharing content during the meeting

PowerPoint Sharing

In Lync 2010 PowerPoint presentations were viewed in one of two ways. For users running Lync 2010, PowerPoint presentations were displayed using the PowerPoint 97-2003 format and were viewed using an embedded copy of the PowerPoint viewer. For users running Lync Web App, PowerPoint presentations were converted to dynamic HTML files then viewed using a combination of those customized DHTML files and Silverlight. Although generally effective, this approach did have some limitations:

- The embedded PowerPoint Viewer (which provided the optimal viewing experience) is only available on the Windows platform.
- Many mobile devices (including some of the more popular mobile phones) do not support Silverlight.
- The PowerPoint Viewer and the DHTML/Silverlight approach do not support all of the features (such slide transitions and embedded video) that are found in the more recent editions of PowerPoint.

To help address these issues, and to improve the overall experience of users presenting or viewing PowerPoint presentations, Lync Server 2013 employs Office Web Apps and the Office Web Apps Server to handle PowerPoint presentations. Among other advantages, this new approach enables:

- Higher-resolution displays and better support for PowerPoint capabilities, such as animations, slide transitions, and embedded video.
- Additional mobile devices to access these presentations. That's because Lync Server 2013 uses standard DHTML and JavaScript to broadcast PowerPoint presentations instead of customized DHTML and Silverlight.
- Users with the appropriate privileges to scroll through a PowerPoint presentation independent of the presentation itself. For example, while Ken Myer is presenting his slide show, Pilar Ackerman can look at any slide she wants to, and without affecting Ken's presentation.

1.3.8.1.3 A/V Conferencing Overview

A/V Conferencing Overview

Planning > Planning for Conferencing > Overview of Conferencing >

Topic Last Modified: *2012-10-13*

A/V conferencing enables real-time audio and video communications between your users. When you deploy conferencing, you can choose to enable and use both web conferencing and A/V conferencing, or just web conferencing.

To plan for A/V conferencing, you need to understand the network bandwidth required by the type of conferencing media that your organization requires. This could include audio, video, and panoramic video.

Before you enable users for A/V conferencing, ensure that your network can handle the resulting load. Without sufficient network bandwidth, the user experience may be severely degraded. You can use call admission control (CAC) to manage the network bandwidth used by A/V Conferencing. This is important for restricted networks, such as limited bandwidth links between central and branch sites. For details, see Overview of Call Admission Control. For details about media bandwidth requirements, see Network Bandwidth Requirements for Media Traffic.

If you deploy audio conferencing in your network, your users will need audio devices such as headsets to participate in an audio conference. If you deploy video conferencing, you need to deploy video devices, such as webcams for users. We recommend that you use unified communications (UC) devices that are certified by Microsoft for all device types, to ensure an optimal user experience. For details about UC-certified devices, see "Phones and Devices for Lync" at http://go.microsoft.com/fwlink/p/?LinkId=263861. For either audio or video devices, device deployment, and user training are important steps for you to consider and plan for.

The following sections describe the features for audio and video conferencing, including information about managing bandwidth and selecting the appropriate clients.

Audio Conferencing Features

Lync Server 2013 provides several features that you can use to configure the audio conferencing experience for the user, including the following:

- **Audience mute** The presenter can use this setting to mute all the audio participants in the conference and put the conference in a state where non-presenters cannot unmute themselves.
- **Conferencing Entry/Exit Announcements** If you have enabled dial-in conferencing, presenters can use this setting to turn entry and exit announcements on or off to minimize distractions while a conference is in progress.
- **Adding a user by dialing out** Presenters and attendees that have been given permission, can add PSTN numbers to the conferences and have the conference dial-out to those numbers.

Video Conferencing Features

Lync Server 2013 provides several features that you can use to configure the video conferencing experience for the user, including the following:

- **Gallery View** In video conferences that have more than two people, users automatically see everyone in the conference. If the conference has more than five participants, the video of the most active participants appear in the top row and only the photo appears for the other participants. Multiparty video is turned on by default. For details about configuring or turning off multiparty video, see Configuring Video Bandwidth in Lync Server 2013.

- **Panoramic Video** If a RoundTable video conferencing device is installed in the conferencing room, this feature provides a full 360 degree view of the conference room. The panoramic video strip is only available with RoundTable devices.
- **Presenter only video mode** Presenters can configure the meeting so that only the video from the presenter is shown. This prevents distractions in large meetings when multiple video streams are available and locking to different sources. This mode also applies to video captured and provided by RoundTable devices.
- **HD video** Users can experience resolutions up to HD 1080P in two-party calls and multiparty conferences.
- **Video Spotlight** Presenters can configure the meeting so that only the video from a selected participant who is a video source is seen by the other participants in the conference. This mode also applies to video captured and provided by RoundTable devices for panoramic video.

1.3.8.1.4 Dial-In Conferencing Overview

Dial-In Conferencing Overview

Planning > Planning for Conferencing > Overview of Conferencing >

Topic Last Modified: *2012-09-30*

If your organization has users who need to attend Lync Server 2013 on-premises conferences when they are out of the office or do not have access to a computer, you can deploy dial-in conferencing so that they can join the conference by using a public switched telephone network (PSTN) phone.

Dial-in conferencing is an optional feature that you can configure when you deploy Lync Server 2013 conferencing. Although dial-in conferencing uses some of the same Lync Server 2013 components that Enterprise Voice uses, you can deploy dial-in conferencing even if you do not deploy Enterprise Voice.

Note:

If you deploy dial-in conferencing, you must deploy it in every pool where you deploy Lync Server 2013 conferencing. You do not need to assign access numbers in every pool, but you must deploy the dial-in feature in every pool. This requirement supports the recorded name feature when a user calls an access number from one pool to join a Lync Server 2013 conference in a different pool.

Conferences must be enabled for dial-in access in meeting policy. By default, conferences that are enabled for dial-in access include the following information in the conference invitation:

- A numeric conference ID that identifies the conference.
- One or more PSTN access numbers.
- A link to a Dial-in Conferencing Settings page, which contains a complete list of access numbers with their associated languages; a place to create, reset, or unblock personal identification numbers (PINs); and other information, such as dual-tone multi-frequency (DTMF) controls.

Dial-in conferencing supports both enterprise and anonymous users. Enterprise users have Active Directory Domain Services (AD DS) credentials and Lync Server 2013 accounts within their organization. Anonymous users do not have enterprise credentials within your organization. In the dial-in conferencing context, a user in a federated partner's organization who uses the PSTN to connect to a conference is treated like an anonymous user. For dial-in conferencing, unlike other contexts, federated users are not authenticated.

Enterprise users or conference leaders who join a conference that is enabled for dial-in access dial one of the conference access numbers and then are prompted to enter the conference ID. If a leader has not yet joined the meeting, users can either enter their unified communications (UC) extension (or full phone number) and PIN or wait to be admitted by a leader. The Meeting organizer can join the meeting as a leader by entering just their PIN. The Front End Server uses the combination of full phone number or extension, and PIN, to uniquely map enterprise users to their Active Directory credentials. As a result, enterprise users are authenticated and identified by name in the conference. Enterprise users can also assume a conference role predefined by the organizer.

Note:

Enterprise users who dial in from an office IP phone or from Lync Server 2013 or Lync 2010 Attendant are not prompted for their phone number because they are already authenticated.

Anonymous users who want to join a dial-in conference dial one of the conference access numbers and then they are prompted to enter the conference ID. Unauthenticated anonymous users are also prompted to record their name. The recorded name identifies unauthenticated users in the conference. Anonymous users are not admitted to the conference until at least one leader or authenticated user has joined, and they cannot be assigned a predefined role.

Note:

Enterprise users who choose not to enter their phone number and PIN are not authenticated. They are prompted to record their name and are treated as anonymous users in the conference.

At schedule time, the meeting organizer can choose to restrict access to the meeting by making the meeting closed or locked. In this case, dial-in users are requested to authenticate. If dial-in users fail or choose not to authenticate, they are transferred to the lobby. They wait in the lobby until a leader accepts or rejects them, or they time out and are disconnected. Dial-in users hear music if they are waiting to be admitted to the conference. After they are admitted to a conference, dial-in users can participate in the audio portion of the conference and can exercise dual-tone multi-frequency (DTMF) commands by using the phone keypad. Dial-in leaders can exercise DTMF commands to turn participants' ability to unmute on or off, lock or unlock the conference, admit people from the lobby, and turn entry and exit announcements on or off. Leaders can also use a DTMF command to admit everyone from the lobby, which changes the permissions of the meeting to allow anyone who subsequently joins. All dial-in participants can exercise DTMF commands to hear Help, listen to the conference roster, and mute themselves.

Dial-in participants (that is, whether or not they dial from the PSTN), hear personal announcements during the conference, such as whether they have been muted or unmuted, the meeting is being recorded, or someone is waiting in the lobby.

Note:

Participants who join the conference by clicking a link instead of dialing in do not hear personal announcements.

1.3.8.2 Defining Your Requirements for Conferencing

Defining Your Requirements for Conferencing

See Also

Microsoft Lync Server 2013 > Planning > Planning for Conferencing >

Topic Last Modified: *2012-09-30*

When you are determining which conferencing capabilities to deploy, you need to consider the features that you want available to your users and your network bandwidth capabilities. The following list of questions guides you through the conferencing planning process to determine what features of conferencing you should deploy, based on your organization's requirements.

- **Do you want to enable web conferencing, which includes document collaboration and application sharing?**

  If so, you must enable conferencing for your Front End pool in the Microsoft Lync Server 2013, Planning Tool or in Topology Builder. When you enable conferencing, you enable both web conferencing and A/V conferencing.

  Application sharing requires and uses more network bandwidth than document collaboration. Lync Server 2013 provides a throttling mechanism to control each application sharing session. By default, this is set to 1.5 KB/second for each session.

  If you do not want to enable application sharing but you do want document collaboration, you can enable conferencing and use meeting policies to disable application sharing. For details about configuring meeting policies, see Conferencing Policies.

  To enable users to share PowerPoint presentations, you need to configure Office Web Apps Server. For details about configuring Office Web Apps Server, see Configuring Integration with Office Web Apps Server and Lync Server 2013.
- **Do you want to enable A/V conferencing?**

  If so, you must enable conferencing for your Front End pool in the Lync Server 2013, Planning Tool or in Topology Builder. When you enable conferencing, you enable both web conferencing and A/V conferencing.

  A/V conferencing requires and uses more network bandwidth than web conferencing (which includes document collaboration and application sharing).

  If you do not want to enable A/V conferencing but you do want to enable web conferencing, you can enable conferencing and use meeting policies to disable A/V conferences.

  If you do want to enable audio conferences but not video conferences, you can enable A/V conferencing and use meeting policies to prevent video conferences. Alternatively, you can enable A/V conferencing and enable only certain users to start or participate in A/V conferences.

  > **Note:**
  >
  > Enterprise Voice is not required for you to use A/V conferencing. If you enable A/V conferencing, your users can add audio to their conferences if they have audio devices, even if you use a PBX for your telephone solution.
- **Do you want to enable users to join the audio portion of conferences when using a PSTN phone?**

  If so, deploy and enable dial-in conferencing. Invited users, both inside and outside your organization, can then join the audio portion of conferences by using a PSTN phone.
- **Do you want to enable external users with Lync Server 2013 clients to join the types of conferences that you have enabled?**

  If so, you should deploy Edge Servers. By allowing external participation in meetings, you maximize your investment in Lync Server 2013. For example, users with laptops with Lync Server 2013 can join conferences from wherever they are—at home, in the airport, or at customer sites.

  Additionally, with Edge Servers deployed you can create federated relationships with other organizations-such as your customers or vendors-and users from those organizations can more easily collaborate with your users.

  For details about deploying Edge Servers, see Planning for External User Access and Deploying External User Access. For details about enabling external access for Office Web Apps Server, see Publishing Office Web Apps Server Using a Reverse Proxy Server.
- **Do you want to control the clients that can join Lync Server 2013**

meetings?
If so, you should configure the meeting join page so that only the client options that you want to support are available. Each time a user clicks a link to join a scheduled meeting, Lync Server 2013 detects whether a client is already installed on the computer. It then starts the default client and opens the meeting join page, which contains links for alternate clients. The meeting join page always contains the option to use Microsoft Lync Web App. In addition to this option, you can decide whether to include links for Attendee and previous versions of Communicator. For details, see Configuring the Meeting Join Page.

- Web Conferencing Requirements
- A/V Conferencing Requirements
- Dial-In Conferencing Requirements

⊟See Also

Other Resources

Planning for Conferencing
Deployment Checklist for Conferencing

1.3.8.2.1 Web Conferencing Requirements

Web Conferencing Requirements

See Also

Planning > Planning for Conferencing > Defining Your Requirements for Conferencing >

Topic Last Modified: *2013-01-30*

If you have chosen to enable web conferencing, you need to plan for the following:

- Access to the file store, which is used for storing web conferencing content.
- Integration with Office Web Apps Server, which is necessary in order to share PowerPoint files during a conference.

File Store

The Lync Server 2013 web conferencing service stores content shared during meetings in the file store. As part of deployment, you must specify a file share to be used as the file store for the either Standard Edition server or Enterprise Edition Front End pool. You can use an existing file share for the file store or you can specify a new file share by specifying the fully qualified domain name (FQDN) of the file server on which the file share is to be located and a folder name for the new file share. For more information, see Topology Builder – Define the File Store for the Front End. The web conferencing service encrypts the content before it stores the content in the file store.

Lync Server 2013 supports using file shares on either direct attached storage (DAS) or a storage area network (SAN), including Distributed File System (DFS) and on a redundant array of independent disks (RAID) for file stores. After the Lync Server Deployment Wizard has defined the location of the file share, Lync Server creates a folder structure within the file share similar to:

- 1-ApplicationServer-1
- 1-CentralMgmt-1
- 1-WebServices-1
  - CollabContent
  - CollabMetadata
  - DataConf

The web conferencing service then stores content such as PowerPoint slides, whiteboards, polls, and attachments in the CollabContent and CollabMetadata folders, located in the WebServices folder.

The administrator must set permissions on the file share so that RTC groups have the necessary read and write access.

⚠**Warning:**

If you encounter any errors with the permissions, open Topology Builder, download and republish the existing topology. Publishing the topology will verify the file share permissions and reset them if needed.

You can use the following settings to manage how content is stored for a meeting:

- **ContentGracePeriod**, located in Set-CsConferencingConfiguration, sets how long web conferencing content will remain on the server after the meeting has ended.
- **MaxContentStorageMb**, located in Set-CsConferencingConfiguration, sets the maximum amount of file space allowed for the storage of content during a single meeting.

MaxUploadFileSizeMb does not limit the file upload setting for Lync Web App. The file size upload limit for Lync Web App is set to approximately 30MB and is controlled by the IIS web.config file: /DataCollabWeb/Int[Ext]/Handler/web.config. To configure the file size upload limit for Lync Web App, update `maxRequestLength` and `maxAllowedContentLength` in the web.config file as shown below.

```
<system.web>
    <!--
        Since this handler is used to upload files to DMCU the request size (in k
        has to fit max allowed file size uploaded by Lync Web App client.
        The timeout has to reflect the min client bandwidth. Timeout of 600 secs
        and 512 Kbits of *client* bandwidth would result into aproximately 30 Mby
        for Lync Web App upload size limit.
    -->
      <httpRuntime maxRequestLength="500000" executionTimeout="600" />
                <security>
                <requestFiltering>
                           <requestLimits maxAllowedContentLength="524288000" />
                </requestFiltering>
                </security>
```

You must update the web.config file for each Front End Server.

Office Web Apps Server

In order to use these new capabilities administrators must install Office Web Apps Server and they must configure Lync Server 2013 to communicate with Office Web Apps Server. This documentation provides information on how to configure Lync Server 2013 to work with Office Web Apps Server. What this documentation does not provide is information about how to install Office Web Apps Server. For installation details, see the Microsoft Office Web Apps Deployment website at http://go.microsoft.com/fwlink/p/?linkid=257525. That guide includes complete prerequisite information for Office Web Apps Server. Note that Office Web Apps Server should be installed on a stand-alone computer that is not running Lync Server, SQL Server, or any other server application. (You must not have any version of Office installed on that computer.) Any computer used to run Office Web Apps Server must also have a specific set of software installed (including .NET Framework 4.5 and Windows PowerShell 3.0). These requirements, along with information about configuring certificates and Internet Information Services (IIS), are discussed in detail in the Microsoft Office Web Apps Deployment website at http://go.microsoft.com/fwlink/p/?linkid=257525.

⊟See Also

Concepts

Web Conferencing Overview
Deployment Checklist for Web Conferencing

1.3.8.2.2 A/V Conferencing Requirements

A/V Conferencing Requirements

See Also

Planning > Planning for Conferencing > Defining Your Requirements for Conferencing >

Topic Last Modified: *2012-09-30*

Lync Server 2013 infrastructure requirements for conferencing are the same as for deployment of Lync Server 2013. For details, see Determining Your Infrastructure Requirements in the Planning documentation.

It is important that you have the necessary Media bandwidth to handle media traffic generated by conferencing. For details that you can use to calculate your needed bandwidth, see Network Bandwidth Requirements for Media Traffic. For details about limiting the bandwidth, see Creating or Modifying Bandwidth Policy Profiles. For details about infrastructure requirements, see Network Infrastructure Requirements.

In order to use the conferencing features, Lync Server 2013 requires that certain ports are open. For details about Port Requirements, see Ports and Protocols for Internal Servers. For details about configuring ports, see Configuring Port Ranges for Your Conferencing, Application, and Mediation Servers.

Concepts

A/V Conferencing Overview
Deployment Checklist for A/V Conferencing

1.3.8.2.3 Dial-In Conferencing Requirements

Dial-In Conferencing Requirements

See Also

Planning > Planning for Conferencing > Defining Your Requirements for Conferencing >

Topic Last Modified: *2012-09-30*

Before you start the Lync Server 2013 deployment process you need to plan for the following:

- The configuration to use for connecting to the public switched telephone network (PSTN)
- Your strategy for assigning dial-in conferencing regions to dial-in access numbers
- Your strategy for creating conference directories

Planning for Dial-in PSTN Connectivity

Dial-in conferencing requires at least one Mediation Server and at least one PSTN gateway.

You can deploy a Mediation Server in a central site or in a branch site. In a central site, you can collocate a Mediation Server on a Front End pool or Standard Edition server, or you can deploy it on a stand-alone server or pool. In a branch site, you can deploy a Mediation Server on a stand-alone server or as a component of the Survivable Branch Appliance.

You can deploy a PSTN gateway in a central site or in a branch site. In a branch site, the PSTN gateway can be stand-alone or a component of the Survivable Branch Appliance.

Note:

Dial-in conferencing does not use media bypass because A/V Conferencing Server do not support media bypass.

For details about planning your configuration for Mediation Server and PSTN gateways for dial-in conferencing, see Components and Topologies for Mediation Server in the Planning documentation.

Planning for Dial-in Conferencing Regions

During dial-in configuration, you create dial plans and dial-in conferencing access numbers. Dial plans are sets of normalization rules that specify the number and pattern of digits in a phone number and translate the phone number into the standard E.164 format for call routing. Dial-in conferencing access numbers are the numbers participants call to join a conference.

Every dial-in conferencing access number must be associated with at least one dial plan. Dial-in conferencing regions associate a dial-in conferencing access number with its dial plans. When you set up a dial plan, you specify the dial-in conferencing region that applies to the dial plan. When you create the dial-in access number, you select the regions that associate the access number with the appropriate dial plans.

When you create a dial plan, you specify the scope of the dial plan: user scope, pool scope, or site scope. Every user is assigned the dial plan from the narrowest scope that applies to the user. For example, a user is assigned a user-level dial plan, if one applies. If a user-level dial plan does not apply, the user is assigned a pool-level dial plan. If a pool-level dial plan does not apply, the user is assigned a site-level dial plan. If a site-level dial plan does not apply, the user is assigned the global dial plan.

Before you configure the dial plans, is it important to plan how you want to name and use regions. The following considerations apply to dial-in conferencing regions:

- A region is typically a geographical area that is associated with an office or group of offices.
- Languages are associated with dial-in access numbers. If you support geographical areas that have multiple languages, you should decide how you want to define regions to support the multiple languages. For example, you might define multiple regions based on a combination of geography and language, or you might define a single region based on geography and have a different dial-in access numbers for each language.
- When a user schedules a meeting, by default the meeting uses the region specified by that user's dial plan.
- By default, the all of the dial-in access numbers for the region are included in the meeting invitation.
- It is important to name regions so that they are clearly recognizable. The user can use the names of the regions to change a meeting's region so that different access numbers are included in the invitation. (When users use Outlook to schedule a meeting, the user uses the Online Meeting Add-in for Lync 2013 to change the region).
- Regions should be designed so that any invitee who wants to dial into a

conference can see a local access number in the conference invitation.

- You can configure the order in which access numbers within a region appear on the Dial-in Conferencing Settings page (and, therefore, the order in which they appear in the conference invitation) by using Lync Server Management Shell cmdlets.
- Any user from any location can call any dial-in access number to join a conference.

Planning for Conference Directories

Conference directories maintain a mapping between the alphanumeric meeting ID that a participant uses to join a conference when using Lync 2013, and the numeric-only conference ID that a dial-in conferencing participant uses to join the conference. The format of the conference ID is as follows:

```
      <housekeeping digit (1 digit)><conference directory (usually 1-2 digits)><c
```

Creating multiple conference directories will ensure that conference IDs will stay short until a significant amount of conferences have been created. In an organization with a typical number of conferences per user, we recommend that you create one conference directory for every 999 users in the pool. Using this guideline the conference IDs can generally be kept small. However, once the number of conference directories (across the pools) exceed 9, the Conference ID number will grow to support additional conferences.

See Also

Concepts

Mediation Server Component
Dial Plans and Normalization Rules

1.3.8.3 Components and Topologies for Conferencing

Components and Topologies for Conferencing

Microsoft Lync Server 2013 > Planning > Planning for Conferencing >

Topic Last Modified: *2013-02-04*

When you select conferencing in Topology Builder, conferencing is deployed as part of the Front End Server or Standard Edition server. Dial-in conferencing and PowerPoint sharing requires additional components and configuration. The following sections describe the supported components and topologies for web conferencing, A/V conferencing, and dial-in conferencing.

Supported Components

The only components web conferencing and A/V conferencing require are your organization's Front End Servers or Standard Edition servers. For a list of hardware and software requirements for the Front End Servers and Standard Edition servers, see Supported Hardware and Server Software and Infrastructure Support.

Lync Server 2013 uses Office Web Apps and the Office Web Apps Server to handle sharing and rendering of PowerPoint presentations. For details about installing and configuring the Office Web Apps Server, see Configuring Integration with Office Web Apps Server and Lync Server 2013.

In addition to the requirements for web conferencing and A/V conferencing, dial-in conferencing uses the following Lync Server 2013 components:

- **Application service** Application service provides a platform for deploying, hosting, and managing unified communications (UC) applications. Dial-in conferencing uses two UC applications that require Application service: Conferencing Attendant and Conferencing Announcement. Application service is installed and activated by default on every Front End Server in a Front End pool and on every Standard Edition server when you deploy a Conferencing workload and select the dial-in conferencing option.
- **Conferencing Attendant application** Conferencing Attendant application is a unified communications application that accepts public switched telephone network (PSTN) calls, plays prompts, and joins the calls to an A/V conference. Conferencing Attendant application is installed and activated by default when you deploy a Conferencing workload and select the dial-in conferencing option.
- **Conferencing Announcement application** Conferencing Announcement application is a unified communications application that plays tones and prompts to PSTN participants on certain actions, such as when participants join or leave a conference, participants are muted or unmuted, someone enters the conference lobby, or the conference is locked or unlocked. Conferencing Announcement application also supports dual-tone multifrequency (DTMF) commands from the phone keypad. Conferencing Announcement application is automatically installed and activated by default when you deploy a Conferencing workload and select the dial-in conferencing option.
- **Dial-in Conferencing Settings page** The Dial-in Conferencing Settings page displays conference dial-in numbers with their available languages, assigned conference information (that is, for meetings that do not need to be scheduled), and in-conference DTMF controls, and supports management of personal identification number (PIN) and assigned conferencing information. The Dial-in Conferencing Settings page is automatically installed as part of Web Services.
- **Lync Server 2013, Mediation Server and PSTN gateway** Dial-in conferencing requires a Mediation Server to translate signaling (and media, in some configurations) between Lync Server 2013 and the PSTN gateway, and a PSTN gateway to translate signaling and media between the Mediation Server and the PSTN gateway. For dial-in conferencing, you must deploy at least one Mediation Server and at least one of the following:
  - PSTN gateway
  - IP-PBX
  - Session Border Controller (SBC) (for an Internet telephony service provider to which you connect by configuring a SIP trunk)

  Note:

  If you are also deploying Enterprise Voice, Mediation Server and PSTN gateways are part of the Enterprise Voice deployment. If you are not deploying Enterprise Voice, you need to deploy at least one Mediation Server and at least one PSTN gateway, IP-PBX, or SBC for dial-in conferencing.
- **File store** File store is used for recorded name audio files. File Store is a standard component in every Enterprise Edition or Standard Edition deployment.
- **User store** User store is used to store user Lync Server 2013 PINs. PINs are hashed. The User store is a standard component in every Enterprise Edition or Standard Edition deployment.
- **Lync Server Control Panel** Some dial-in settings can be configured by using Lync Server Control Panel.
- **Lync Server Management Shell** All dial-in settings can be configured by using Lync Server Management Shell cmdlets. Lync Server Management Shell cmdlets are available for deploying, configuring, running, monitoring, and troubleshooting Conferencing Attendant application and Conferencing Announcement application. For details about specific cmdlets, see Lync Server Management Shell documentation.

Supported Topologies

In Lync Server 2013, the server running conferencing services is always collocated with the Front End Servers or Standard Edition servers. During your initial deployment, Topology Builder gives you the option to include conferencing in your topology. You can also use Topology Builder to add conferencing to an existing deployment. For details, see Defining and Configuring the Topology.

Dial in Conferencing Toplogies

You can deploy dial-in conferencing in the following topologies and configurations:

- Lync Server 2013 Standard Edition
- Lync Server 2013 Enterprise Edition
- With or without Enterprise Voice

You can deploy Application service, Conferencing Attendant application, and Conferencing Announcement application in a central site, but not in a branch site.

Note:

If you deploy dial-in conferencing, you must deploy it in every pool where you deploy Lync Server 2013 conferencing. You do not need to assign access numbers in every pool, but you must deploy the dial-in conferencing feature in every pool. This requirement supports the recorded name feature when a user calls an access number from one pool to join a Lync Server 2013 conference in a different pool.

Supported Topologies for Lync Server 2013 and Office Web Apps

Lync Server 2013 provides the following ways to configure Office Web Apps Server. Depending on your needs you can:

- **Install both Lync Server 2013 and Office Web Apps Server on-premises behind your organization’s firewall, and in the same network zone.** With this topology, external access to Office Web Apps Server will be provided through your reverse proxy server. Both Lync Server 2013 and Office Web Apps Server (or an Office Web Apps Server farm) are installed on-premises and behind your organization's firewall. Ideally, you should install Office Web Apps Server in the same network zone as Lync Server.
  External Lync clients can connect to Lync Server 2013 and to Office Web Apps Server by using a reverse proxy server, which is a server that takes requests from the Internet and forwards them to the internal network. (Internal clients do not need to use the reverse proxy server because they can connect to Office Web Apps Server directly.) This topology works best if you want to use a dedicated Office Web Apps Server farm that is only used by Lync Server 2013.
- **Using an externally deployed Office Web Apps Server**
  In this topology, Lync Server 2013 is deployed on-premises, and uses an Office Web Apps Server that is deployed outside of Lync Server network zone. This may happen when Office Web Apps Server is shared across multiple applications in the corporation and is deployed in a network requiring Lync Server to use the external interface of Office Web Apps Server and vice versa. You do not need to install a reverse proxy server; instead, all the requests from the Office Web Apps Server to Lync Server 2013 are routed through your Edge Server. Both your internal and your external Lync clients connect to Office Web Apps Server using the external URL.
  If the Office Web Apps Server is deployed outside your internal firewall, then select the option **Office Web Apps Server is deployed in an external network (that is, perimeter/Internet)** in Topology Builder. For more details see Configuring Integration with Office Web Apps Server and Lync Server 2013.

Regardless of the topology you select, it is critical that the correct firewall ports be opened. You must make sure that DNS names, IP addresses, and ports are not blocked by firewalls on the Office Web Apps Server, the load balancer, or Lync Server.

Note:
Another option for providing external access to Office Web Apps Server is to deploy the server in the perimeter network. If you elect to do this, keep in mind that Office Web Apps Server setup requires the server computer to be a member of your Active Directory domain. Unless your network policy allows computers in the perimeter network to be Active Directory domain members, it is recommended that you do not install Office Web Apps Server in the perimeter network. Instead, you should install Office Web Apps Server in the internal network and provide external user access through your reverse proxy server.

1.3.8.4 Technical Requirements for Conferencing

Technical Requirements for Conferencing

Microsoft Lync Server 2013 > Planning > Planning for Conferencing >

Topic Last Modified: *2012-09-11*

For Lync Server 2013, dial-in conferencing, A/V conferencing, instant messaging (IM) conferencing and web conferencing capabilities always run on Front End Servers.

This section details the hardware and software requirements for these servers, along with the supported collocation.

Dial-in conferencing is a feature that includes a variety of components. Some of the components are specific to dial-in conferencing and some are Enterprise Voice components. This section describes the requirements for the components that are specific to dial-in conferencing. For details about Mediation Server and public switched telephone network (PSTN) gateway requirements, see Mediation Server Component and Components and Topologies for Mediation Server in the Planning documentation.

Hardware Requirements

Because web conferencing and A/V conferencing are collocated with the Front End Server, the server hardware requirements are the same as for the Front End Servers. For details about hardware requirements, see Server Hardware Platforms in the Supportability documentation. The following components required for dial-in conferencing also have the same hardware requirements as Front End Servers:

- Application service
- Conferencing Attendant application
- Conferencing Announcement application

The hardware requirements for Front End Server are the same as for many other server roles in Lync Server 2013 are outlined in the following table.

Software Requirements

Because web conferencing and A/V conferencing are collocated with the Front End Server, the server software requirements are the same as for the Front End Servers. For details about software requirements, see Server and Tools Operating System Support in the Supportability documentation.

For web conferencing, Lync Server 2013 also requires Office Web Apps and the Office Web Apps Server (formerly known as WAC Server) to handle PowerPoint presentations. For details, see Configuring Integration with Office Web Apps Server and Lync Server 2013.

For dial-in conferencing, Application service, Conferencing Attendant application, and Conferencing Announcement application have the same operating system requirements as Front End Servers. For details about software requirements, see Server and Tools Operating System Support in the Supportability documentation.

Conferencing Attendant application and Conferencing Announcement application require that Windows Media Format Runtime is installed on Front End Servers. The Windows Media Format Runtime is required to play Windows Media audio (WMA) files that are used for music on hold, recorded names, and prompts. Except for Windows Server 2012, the Windows Media Format Runtime is installed automatically as part of the Windows Desktop Experience when you run Setup, but you might need to restart the computer. Therefore, we recommend that you install as part of the Windows Desktop Experience, which includes Windows Media Format Runtime before you run Setup. Windows Server 2012 requires Microsoft Media Foundation.

Port Requirements for dial-in conferencing

The following table describes the ports that are used by dial-in conferencing. If you use a load balancer, ensure that the load balancer is configured for the ports used by any applications that will run in the pool.

These ports are default settings that you can change by using the **Set-CsApplicationServer** cmdlet. For details about this cmdlet, see the Lync Server Management Shell documentation.

Note:
All instances of the same application in a pool use the same SIP listening port.

Ports used by dial-in conferencing

Port number	Description
5072	Used by Conferencing Attendant application for SIP listening requests
5073	Used by Conferencing Announcement application for SIP listening requests

Supported Clients for Dial-In Conferencing

You can use the following client to schedule on-premises conferences that support dial-in access:

- Online Meeting Add-in for Lync 2013 (installed automatically when you install Lync 2013 or Attendee)

Dial-in Conferencing Settings page Requirements

The Dial-in Conferencing Settings page supports the combinations of operating systems and web browsers described in the following table.

Important:
The Dial-in Conferencing Settings page is not supported on 64-bit browsers.

Note:
32-bit and 64-bit versions of the operating systems are supported.

Supported Operating Systems and Web Browsers

Operating system	Web browser
Windows 7	Internet Explorer 9 Internet Explorer 8 Internet Explorer 7 Firefox 9.x
Windows Vista with Service Pack 2	Internet Explorer 9 Internet Explorer 8 Internet Explorer 7 Firefox 9.x
Windows XP with Service Pack 2 (SP2) or latest service pack	Internet Explorer 9 Internet Explorer 8 Internet Explorer 7 Firefox 9.x
Windows Server 2008 R2	Internet Explorer 9 Internet Explorer 8 Internet Explorer 7
Windows Server 2008 with SP2	Internet Explorer 9 Internet Explorer 8 Internet Explorer 7
Windows Server 2003 (except on Intel Architecture 64-bit [IA-64])	Internet Explorer 9 Internet Explorer 8 Internet Explorer 7
Mac OS 10.4.8 and later versions (Intel based)	Firefox 3.x Safari 5.x Safari 4.x

Audio File Requirements for dial-in conferencing

Lync Server 2013 does not support customization of voice prompts and music for dial-in conferencing. However, if you have a strong business need that requires you to change the default audio files, see Microsoft Knowledge Base article 961177, "How to customize voice prompts or music files for dial-in audio conferencing in Microsoft Office Communications Server 2007 R2," available at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=961177.

Conferencing Attendant application and Conferencing Announcement application have the following requirements for music on hold, recorded name, and audio prompt files:

- Windows Media Audio (WMA) file format
- 16-bit mono
- 48 kbps 2-pass CBR (constant bit rate)
- Speech level at -24DB

User Requirements for Dial-In Conferencing

Dial-in conferencing users must have a unique phone number or extension assigned to their account. This requirement supports authentication during dial-in conferencing. Enterprise users (that is, users who have Active Directory Domain Services (AD DS) credentials and Lync Server accounts within your organization) enter their phone number (or extension) and a personal identification number (PIN) to dial in to conferences as an authenticated user.

1.3.8.5 Deployment Checklist for Conferencing

Deployment Checklist for Conferencing

Microsoft Lync Server 2013 > Planning > Planning for Conferencing >

Topic Last Modified: *2012-09-30*

The following topics provide a checklist for deploying and configuring web conferencing, A/V conferencing, and dial-in conferencing.

- Deployment Checklist for Web Conferencing
- Deployment Checklist for A/V Conferencing
- Deployment Checklist for Dial-In Conferencing

1.3.8.5.1 Deployment Checklist for Web Conferencing

Deployment Checklist for Web Conferencing

Planning > Planning for Conferencing > Deployment Checklist for Conferencing >

Topic Last Modified: *2012-09-30*

As with deployment of your other Lync Server 2013 components, deployment of web conferencing requires that you use Topology Builder to create and publish a topology that incorporates conferencing.

Deployment Sequence

You can deploy conferencing at the same time that you deploy your initial topology or after you have deployed at least one Front End pool or Standard Edition server.

Conferencing Deployment Process

The following table provides an overview of the steps required to deploy conferencing into an existing topology.

Phase	Steps	Roles and group memberships	Documentation
Install prerequisite hardware and software	Conferencing runs on Front End Servers in a Front End pool and Standard Edition servers. It has no additional hardware or software requirements beyond what is required to install those servers. **Note:** Lync Server 2013 uses Office Web Apps and the Office Web Apps Server to handle sharing and rendering of PowerPoint presentations. For information about installing and configuring the Office Web Apps Server, see Configuring Integration with Office Web Apps Server and Lync Server 2013.	Domain user who is a member of the local Administrators group	Supported Hardware in the Supportability documentation Server Software and Infrastructure Support in the Supportability documentation Determining Your System Requirements in the Planning documentation. Technical Requirements for Archiving in the Planning documentation.
Create the appropriate internal topology to support conferencing	Run Topology Builder to add conferencing to the topology, and then publish the topology.	To define a topology, an account that is a member of the local Users group To publish the topology, an account that is a member of the Domain Admins group and RTCUniversalServerAdmins group, and that has full control permissions (read/write/modify) on the file share to be used for the Lync Server 2013 file store (so that Topology Builder can configure the required DACLs)	Define and Configure a Topology in Topology Builder in the Deployment documentation.
Configure conferencing policies and support	Use the Lync Server 2013 Control Panel or Lync Server	RTCUniversalServerAdmins group (Windows	Conferencing Policies in the Operations documentation.

	Management Shell to configure conferencing settings.	PowerShell only) or assign users to the [] or CSAdministrator role	

Lync Server 2013 now includes the **MaxUploadFileSizeMb** setting, which limits the size of files that can be uploaded during a meeting. The default value for this setting is 500 MB. You can adjust **MaxUploadFileSizeMb** using the **Set-CsConferencingConfiguration** cmdlet.

MaxUploadFileSizeMb does not limit the file upload setting for Lync Web App. The file size upload limit for Lync Web App is set to approximately 30MB and is controlled by the IIS web.config file: /DataCollabWeb/Int[Ext]/Handler/web.config. To configure the file size upload limit for Lync Web App, update `maxRequestLength` and `maxAllowedContentLength` in the web.config file as shown below.

```
<system.web>
    <!--
        Since this handler is used to upload files to DMCU the request size (in k
        has to fit max allowed file size uploaded by LWA client.
        The timeout has to reflect the min client bandwidth. Timeout of 600 secs
        and 512 Kbits of *client* bandwidth would result into aproximately 30 Mby
        for LWA upload size limit.
    -->
      <httpRuntime maxRequestLength="500000" executionTimeout="600" />
                <security>
                <requestFiltering>
                           <requestLimits maxAllowedContentLength="524288000" />
                </requestFiltering>
                </security>
```

You must update the web.config file for each Front End Server.

1.3.8.5.2 Deployment Checklist for A/V Conferencing

Deployment Checklist for A/V Conferencing

See Also

Planning > Planning for Conferencing > Deployment Checklist for Conferencing >

Topic Last Modified: *2012-09-30*

As with deployment of your other Lync Server 2013 components, deployment of A/V conferencing requires that you use Topology Builder to create and publish a topology that incorporates conferencing.

Deployment Sequence

You can deploy conferencing at the same time that you deploy your initial topology or after you have deployed at least one Front End pool or Standard Edition server.

Conferencing Deployment Process

The following table provides an overview of the steps required to deploy conferencing into an existing topology.

Phase	Steps	Roles and group memberships	Documentation
Install prerequisite hardware and software	Conferencing runs on Front End Servers of a Front End pool and Standard Edition servers. It has no additional hardware or software requirements beyond what is required to install those servers. **Note:** Lync Server 2013 uses Office Web Apps and the Office Web Apps Server to handle sharing and rendering of PowerPoint presentations. For details about installing and configuring the Office Web Apps Server, see Configuring Integration with Office Web Apps Server and Lync Server 2013.	Domain user who is a member of the local Administrators group	Supported Hardware in the Supportability documentation Server Software and Infrastructure Support in the Supportability documentation Determining Your System Requirements in the Planning documentation. Technical Requirements for Archiving in the Planning documentation.
Create the appropriate internal topology to support conferencing	Run Topology Builder to add conferencing to the topology, and then publish the topology.	To define a topology, an account that is a member of the local Users group To publish the topology, an account that is a member of the Domain Admins group and RTCUniversalServerAdmins group, and that has full control permissions (read/write/modify) on the file share to be used for the Lync Server 2013 file store (so that Topology Builder can configure the required DACLs)	Define and Configure a Topology in Topology Builder in the Deployment documentation.
Configure conferencing policies and support	Use the Lync Server 2013 Control Panel or Lync Server Management Shell to configure conferencing settings.	RTCUniversalServerAdmins group (Windows PowerShell only) or assign users to the [] or CSAdministrator role	Conferencing Policies in the Operations documentation.

See Also

Other Resources

Overview of Conferencing
Defining Your Requirements for Conferencing

1.3.8.5.3 Deployment Checklist for Dial-In Conferencing

Deployment Checklist for Dial-In Conferencing

Planning > Planning for Conferencing > Deployment Checklist for Conferencing >

Topic Last Modified: *2013-02-25*

The components required for dial-in conferencing are deployed when you deploy the conferencing workload. Before you can configure dial-in conferencing, you need to deploy either Enterprise Voice or a Mediation Server and a public switched telephone network (PSTN) gateway.

All the steps in the following table must be performed before users can dial in from the PSTN to join an audio/video conference.

Note:
If you are migrating from Office Communications Server 2007 R2, you must apply the latest updates to your Office Communications Server 2007 R2 environment before deploying dial-in conferencing.

Dial-in Conferencing Deployment Process

Phase	Steps	Permissions	Deployment documentation
Create a topology that includes the Conferencing workload, including a Mediation Server and PSTN gateway, and deploy the Front End pool or Standard Edition server	1. Run Topology Builder to configure your topology. While configuring the topology, select the dial-in conferencing option. 2. Publish the topology and deploy the Front End pool or Standard Edition server. 3. If necessary, create a stand-alone Mediation Server and associate it with a PSTN gateway. **Note:** This step is required only if you do not deploy Enterprise Voice and do not	Domain Admins RTCUniversalServerAdmins Administrator	- Deploying Lync Server 2013 - To create a stand-alone Mediation Server pool: Deploying Mediation Servers and Defining Peers

	collocate the Mediation Server with the Enterprise Edition Front End Server or Standard Edition server. If you deploy Enterprise Voice, you install and configure Mediation Servers and PSTN gateways as part of the Enterprise Voice deployment. If you collocate the Mediation Server, you install and configure the Mediation Server as part of the Front End pool or Standard Edition server deployment.		
Configure dial plans	A dial plan is a set of phone number normalization rules that translate phone numbers dialed from a specific location to a single standard (E.164) format for purposes of phone authorization and call routing. The same phone number dialed from different locations can, based on the respective dial plans, resolve to different E.164 numbers, as appropriate to each location. If you deploy Enterprise Voice, you set up dial plans as part of that deployment, and you need to make sure that the dial plans also accommodate dial-in conferencing. If you do not deploy Enterprise Voice, you need to set up dial plans for dial-in conferencing. Use the Lync Server 2013 Control Panel or Lync Server Management Shell to set up dial plans as follows:	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Configure Dial Plans for Dial-in Conferencing

	1. Create one or more dial plans for routing dial-in access phone numbers. 2. Assign a default dial plan to each pool. Set the **Dial-in conferencing region** to the geographic location to which the dial plan applies. The region associates the dial plan with dial-in access numbers.		
Make sure that dial plans are assigned regions	Run the **Get-CsDialPlan** and **Set-CsDialPlan** cmdlets to make sure that all dial plans have a region assigned.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Make Sure Dial Plans Have Assigned Regions
(Optional) Verify or modify user personal identification number (PIN) requirements	Use Lync Server 2013 Control Panel or Lync Server Management Shell to view or modify the Conferencing **PIN Policy**. You can specify minimum PIN length, maximum number of logon attempts, PIN expiration, and whether common patterns are allowable.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	(Optional) Verify PIN Policy Settings
Configure conferencing policy to support dial-in conferencing	Use Lync Server 2013 Control Panel or Lync Server Management Shell to configure **Conferencing Policy** settings. Specify whether: • PSTN conference dial-in is enabled. • Users can invite anonymous participants. • Unauthenticated users can join a conference by using dial-out phoning. With dial-out phoning,	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	Configure Conferencing Policy for Dial-in

	the conference server calls the user, and the user answers the phone to join the conference.		
Configure dial-in access numbers	Use Lync Server 2013 Control Panel or Lync Server Management Shell to set up dial-in access numbers that users call to dial in to a conference, and specify the regions that associate the access number with the appropriate dial plans. The first three access numbers for the region specified by the organizer's dial plan are included in the conference invitation. All access numbers are available on the Dial-in Conferencing Settings page. 📝**Note:** After you create dial-in access numbers, you can use the **Set-CsDialInConferencingAccessNumber** cmdlet to modify the display name of the Active Directory contact objects so that users can more easily identify the correct access number.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	Configure Dial-in Conferencing Access Numbers
(Optional) Verify dial-in conferencing settings	Use the **Get-CsDialinConferencingAccessNumber** cmdlet to search for dial plans that have a dial-in conferencing region that is not used by any access number and for access numbers that have no region assigned.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator CsViewOnlyAdministrator CsHelpDesk	(Optional) Verify Dial-in Conferencing Settings
(Optional) Modify key mapping of DTMF commands	Use the **Set-CsDialinConferencingDtmfConfiguration** cmdlet to modify the keys used for dual-tone multifrequency (DTMF) commands, which participants can use to control conference settings (such as mute and unmute or lock and unlock).	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	(Optional) Modify Key Mapping for DTMF Commands

(Optional) Modify conference join and leave announcement behavior	Use the **Set-CsDialinConferencingConfiguration** to change how announcements work when participants join and leave conferences.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	(Optional) Enable and Disable Conference Join and Leave Announcements
(Optional) Verify dial-in conferencing	Use the **Test-CsDialInConferencing** cmdlet to test that the access numbers for the specified pool work correctly.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	(Optional) Verify Dial-in Conferencing
Deploy the Online Meeting Add-in for Lync 2013	Deploy the Online Meeting Add-in for Lync 2013 so that users can schedule conferences that support dial-in conferencing. The Online Meeting Add-in for Lync 2013 is installed automatically when you install Lync 2013.	Administrators	Deploy the Online Meeting Add-in for Lync 2013
Configure user account settings	Use Lync Server 2013 Control Panel or Lync Server Management Shell to configure the telephony **Line URI** as a unique, normalized phone number (for example, tel:+14255550200).	RTCUniversalServerAdmins CsAdministrator CsUserAdministrator	Configure User Account Settings
(Optional) Welcome users to dial-in conferencing and set the initial PIN	Use the **Set-CsPinSendCAWelcomeMail** script to set users' initial PINs and send a welcome email that contains the initial PIN and a link to the Dial-in Conferencing Settings page.	RTCUniversalServerAdmins	(Optional) Welcome Users to Dial-in Conferencing

1.3.8.6 Support for Large Meetings

Support for Large Meetings

Microsoft Lync Server 2013 > Planning > Planning for Conferencing >

Topic Last Modified: *2012-10-01*

Lync Server 2013 can support meetings with up to 1000 participants using audio/video (A/V) conferencing, including sharing PowerPoint presentations. This support requires a dedicated pool configured to support large meetings and managed in a way that ensures hosting of only a single large meeting at a time.

This section describes how to support large meetings using a dedicated Lync Server 2013 pool. It describes scalability considerations and the implementation requirements for a dedicated pool, including topology, hardware, software, and configuration requirements. It also provides a set of best practice recommendations for supporting large meetings, a summary of the test methods and results of server scalability testing conducted by the Lync Server engineering team, and the answers to frequently asked questions about support for large meetings.

- Overview of Lync Server 2013 Conferencing Scalability
- Supporting Large Meetings Using Lync Server 2013
- Lync Server 2013 Large Meeting Support FAQ

1.3.8.6.1 Overview of Lync Server 2013 Conferencing Scalability

Overview of Lync Server 2013 Conferencing Scalability

Planning > Planning for Conferencing > Support for Large Meetings >

Topic Last Modified: *2012-10-01*

The maximum size of a conference hosted on Lync Server 2013 in a shared pool (that is, a pool that hosts all Lync Server 2013 workloads including instant messaging (IM) and presence, conferencing, and Enterprise Voice) is 250 users.

Before we discuss using Lync Server to support larger meetings, let’s look at the scalability testing methodology we use and how we determine the 250-user model for shared pool testing.

- Scalability Testing
- The Conferencing User Model
- Conferencing Load Distribution

1.3.8.6.1.1 Scalability Testing

Scalability Testing

Planning for Conferencing > Support for Large Meetings > Overview of Lync Server 2013 Conferencing Scalability >

Topic Last Modified: *2012-10-01*

Lync Server 2013 provides the server infrastructure for all Lync Server real-time communications, including instant messaging (IM) and presence, conferencing, and Enterprise Voice. This includes any features that use the hardware resources of a Lync Server 2013 pool and, therefore, affect performance and scale. All organizations do not use all features equally.

For example, some organizations might use video in conferences very heavily while others might have little or no video usage. Some organizations prefer PowerPoint slide sharing to application sharing, while others prefer the opposite. Those organizations that deploy Enterprise Voice might or might not use the Response Group application heavily. Most organizations deploy Monitoring Servers, but not many of them deploy Archiving Servers. Additionally, organizations do not all have the same infrastructures, including hardware capacities, network capacities, and the number of pools and size of pools deployed. The diversity of features and infrastructures poses a challenge to scalability testing – it is not possible to simulate all possible combinations of features and infrastructures.

To determine scalability support for Lync Server, we conduct testing by using all Lync Server features concurrently, based on an average usage model (user model). To determine an appropriate user model for Lync Server workloads, we analyze many data points, including customer surveys, feedback from the Microsoft customer experience improvement program, Lync Server usage data from the internal IT department at Microsoft, and data mined from our Live Meeting Service. In many cases, the user model has a bias towards heavier loads to provide a comfortable margin for usage within an organization.

In our scalability tests, we set up Lync Server 2013 pools according to the recommended hardware and software specifications, including infrastructure components, such as Active Directory Domain Services (AD DS), hardware load balancers, and firewalls. We set up Lync Server environments as closely as possible to typical real-world environments. We then use the Lync Server 2013 Stress and Performance Tool to simulate Lync Server 2013 loads (based on our user model). .

We do multiple iterations of scalability tests (including multiple three-week test runs). We use the results of all tests to help with performance tuning and to verify support for the scalability numbers in our user model.

1.3.8.6.1.2 The Conferencing User Model

The Conferencing User Model

Planning for Conferencing > Support for Large Meetings > Overview of Lync Server 2013 Conferencing Scalability >

Topic Last Modified: *2012-10-22*

A critical part of the Lync Server conferencing user model is meeting size. After collecting data from the multiple data points (as described in the previous section), we determined the following:

- Most meetings are actually small collaborative meetings with an average of four to six participants
- Approximately 80 percent of meetings have fewer than 20 participants.
- 99.98 percent of meetings have fewer than 100 participants.

In addition to meeting size, the conferencing user model also takes into account a variety of factors, such as:

- **Concurrent meetings** How many users are expected to be in meetings at the same time?
- **Media mix** What types of media are available and expected to be used by users in meetings?
- **User types** Are users internal users, remote users, federated users, or anonymous users?
- **Meeting ramp up time** How long does it take for all users of a meeting to join a meeting?

For details about the user model, see Lync Server 2013 User Models.

To determine the number of meetings and users to use for testing, we did the following:

- Took the total number of users in an organization (for example, 80,000 users) and multiplied it by the meeting concurrency rate (for example, 5% of all users) to determine the total number of users expected to be in meetings at the same time (in this example, 4000 users).
- Divided the total number of users by the number of Lync Server 2013, Front End Servers in the deployment (for example, 8 servers) to determine the estimated number of meeting participants per Front End Server (in this example, 500 users per Front End Server).
- Divided the number of users per Front End Server by the average meeting size (for example, 4 users) to determine the estimated average number of meetings per Front End Server (in this example, 125 meetings per Front End

Server).
- To get the per media load on each Front End Server, we estimated the media mix. For example, assuming that 75% of the meetings require more than just audio support and 50% of those meetings require application sharing, an average of 47 meetings and 188 users connect concurrently to each Front End Server for application sharing.
- Tested a variety of meeting sizes (based our user model of up to 250 users in a shared pool) to ensure server scalability.

1.3.8.6.1.3 Conferencing Load Distribution

Conferencing Load Distribution

Planning for Conferencing > Support for Large Meetings > Overview of Lync Server 2013 Conferencing Scalability >

Topic Last Modified: *2012-10-22*

Unlike some other dedicated conferencing solutions, Lync Server architecture is a shared-hardware model. This means that the same hardware is shared by many software components, each of which supports different real-time communications. Each type of real-time communications places specific loads on the servers. For example, the Front End Server can run the Session Initiation Protocol (SIP) routing components, web applications (such as Address Book search), Web Conferencing service, A/V Conferencing service, Enterprise Voice applications (for example, Conferencing Attendant application and Response Group application), and Mediation Server. A set of databases on the Front End Server also provide storage and processing for user, contact, presence, conferencing, and voice routing data. With this hardware sharing, components, services, and processes compete for CPU and memory resources, so non-conferencing workloads have a direct impact on server scaling.

Compared to other hardware port-based conferencing solutions, Lync Server conferencing architecture is a no-reservation model. When a user schedules a meeting, Lync Server creates a record in the conferencing database, which stores conferencing data, but does not reserve any hardware resources for the scheduled meeting ahead of time. Instead, Lync Server has built-in load balancing logic to dynamically allocate conferencing resources on Front End Servers in a way that distributes loads equally across all Front End Servers in the pool. This effectively provisions and utilizes hardware resources, but makes it challenging to support very large meetings (especially without appropriate planning). For example, when a Lync Server 2013 pool is running close to its top capacity, each Front End Server might host approximately 125 average-size meetings. Adding another small meeting would not be a problem, but adding a meeting for 1000 users would be a problem because the Front End Servers would probably not be able to support such a large meeting at the same time as the other 125 meetings.

1.3.8.6.2 Supporting Large Meetings Using Lync Server 2013

Supporting Large Meetings Using Lync Server 2013

Planning > Planning for Conferencing > Support for Large Meetings >

Topic Last Modified: *2012-10-03*

Large meetings do not follow the test model described in the previous section because they have the following characteristics:

- The meeting format is a one-to-many presentation.
- One or a few users are presenters, and everyone else participates only as attendees.

- PowerPoint presentation sharing is the main data collaboration activity.
- Audio is required and video may also be used.
- A dedicated person, generally either the meeting organizer or an assistant to the organizer sets up the meeting well in advance.
- Dedicated staff (not the presenters) runs the meeting, including connecting to an online meeting, verifying that audio, video, and slide sharing work, managing lobby and user roles, muting and unmuting participants, taking questions, and managing recordings, as appropriate.

Supporting large meetings of up to 1000 users requires addressing the issues related to both the shared hardware model and the no-reservation model.

To have sufficient CPU and memory resources for meetings of up to 1000 users, the hosting Front End Servers should not host any other instant messaging (IM) and presence or Enterprise Voice workloads. It should also not host any other meetings, regardless of the size of the other meetings. This means that hosting meetings of up to 1000 users requires setting up a separate Lync Server pool that is dedicated to hosting large meetings of up to 1000 users.

A Lync Server pool that is dedicated to hosting large meetings should host one and only one meeting of up to 1000 users at the same time, so meeting times need to be reserved in advance via an out of band scheduling process to ensure dedicated support from the Front End Servers. To support more than one large meeting at the same time, we recommend setting up multiple dedicated large-meeting pools.

We recommend that a dedicated person run and monitor the online portion of a large meeting. This person might be the organizer, delegate of the organizer or presenter, or a member of the dedicated large meeting support team, depending on the organization’s preferences.

In the following sections, we describe how to implement a dedicated pool for large meetings, including best practices for using Lync Server 2013 to support large meeting scenarios.

- Setting Up Support for Large Meetings
- Managing Large Meetings

1.3.8.6.2.1 Setting Up Support for Large Meetings

Setting Up Support for Large Meetings

Planning for Conferencing > Support for Large Meetings > Supporting Large Meetings Using Lync Server 2013 >

Topic Last Modified: *2012-10-05*

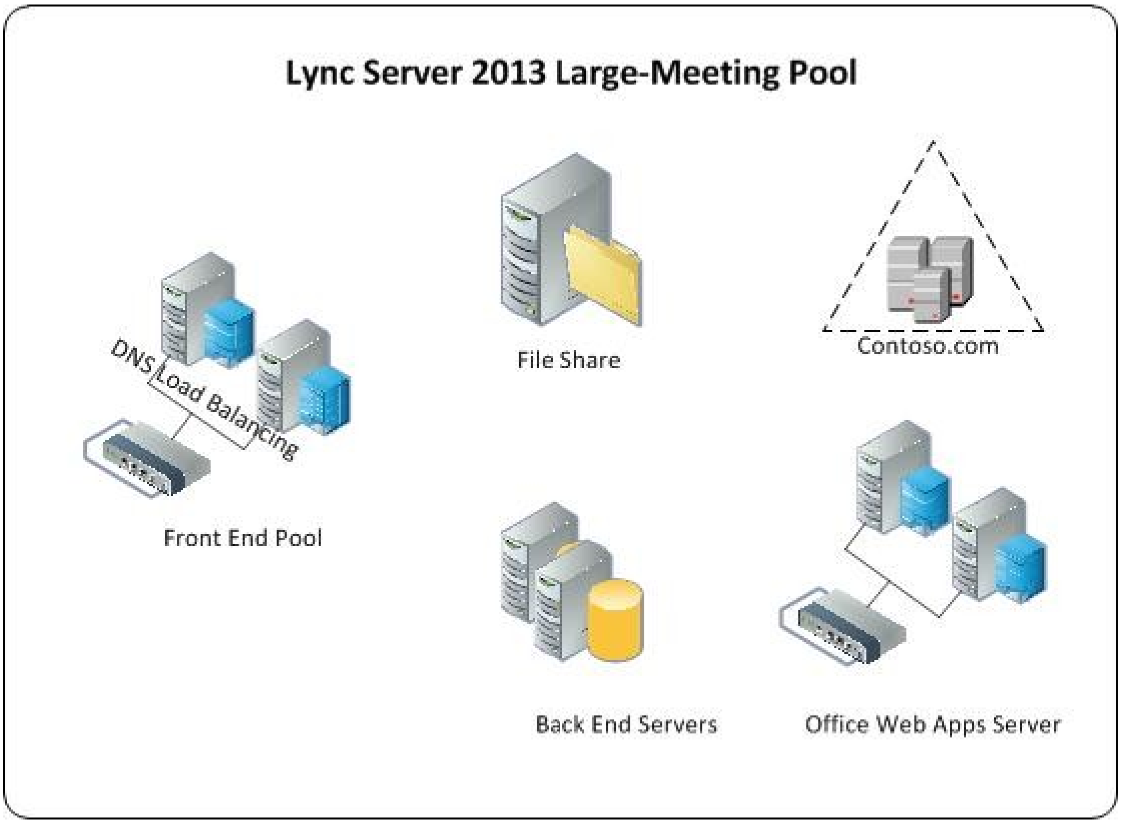
Supporting large meetings of up to 1000 users requires creating an appropriate topology, meeting hardware and software prerequisites, and configuring the environment appropriately.

Topology Requirements

A single large meeting requires at least one Front End Server and one Back End Server. However, to provide high availability, we recommend a two Front End Server pool with mirrored Back End Servers.

The user who hosts the large meetings must have their user account homed in this pool. However, we do not recommend that you host other user accounts in this pool. Instead, use it only for the large meetings. The best practice is to create a special user account in this pool to be used only to host large meetings. Managing a pool with exactly two Front End Servers requires some special considerations. For more information, see Topologies and Components for Front End Servers, Instant Messaging, and Presence.

Additionally, if you want to optionally provide disaster recovery backup and failover for the pool used for large meetings, you can pair it with a similarly set up dedicated pool in a different data. For details, see Planning for High Availability and Disaster Recovery.



Additional notes about the topology include:

- A file share is required for storing meeting content and, if Archiving Server is deployed and enabled, for storing the archiving files. The file share can be dedicated to the pool or can be the same file share used by another pool at the site in which the pool is deployed. For details about configuring the file share, see Configure File Storage.
- A Office Web Apps Server is required for enabling the PowerPoint presentation functionality in large meetings. The Office Web Apps Server can be dedicated to the large meeting pool or, it can be the same Office Web Apps Server used by other pools at the site in which the dedicated pool is deployed.
- Load balancing of the Front End Servers requires hardware load balancing for the HTTP traffic (such as meeting content download). DNS load balancing is recommended for SIP traffic. For details see Load Balancing Requirements.
- If you want to use Monitoring Server for the dedicated large-meeting pool, we recommend using the Monitoring Server and its database that are shared across all of the Front End Server pools in your Lync Server deployment.

Hardware and Software Requirements

The hardware requirements for servers in a dedicated large-meeting pool are the same as for your other Lync Server 2013 servers. For details about hardware requirements, see

"Server Hardware Platforms.

Servers in a dedicated large-meeting pool must meet all Lync Server 2013 software requirements. For details about software requirements, please see the following documentation:

- Server and Tools Operating System Support
- Database Software Support
- Additional Software Requirements

Additionally, both Lync Server 2013 and all Lync Server 2013 clients must have the latest updates.

Configuration Requirements

We recommend creating a new conferencing policy specifically for large meetings, and then assigning the conferencing policy to the users who are homed on the dedicated large-meeting pool. Configure the conferencing policy using the following settings:

- Set the **MaxMeetingSize** option to **1000**. (The default is **250**.)
- Set the **AllowLargeMeetings** option to **True**.
- Set the **EnableAppDesktopSharing** option to **None**.
- Set the **AllowUserToScheduleMeetingsWithAppSharing** option to **False**.
- Set the **AllowSharedNotes** option to **False**.
- Set the **AllowAnnotations** option to **False**.
- Set the **DisablePowerPointAnnotations** option to **True**.
- Set the **AllowMultiview** option to **False**.
- Set the **EnableMultiviewJoin** option to **False**.

Note:

The support for 1000 user large meetings in Lync Server 2013 requires the **AllowLargeMeetings** setting in the conferencing policy for the meeting scheduler to be set to true. When this setting is set to true, the Lync experience will be optimized for extra large meetings when users joins such meeting. Specifically, in a large meeting, Lync will not show the initial or update of the full meeting participant list, which is a performance bottleneck for both the client and Lync Server 2013. Instead, Lync will only show information about the user and the list of presenters of the meeting. Lync will still properly shows total number of participants available in the large meetings.

Except for the **Maximum meeting size** setting, all the other conferencing policy settings specified here are required in order to disable conferencing capabilities that are not necessary in large meetings.

Additionally, you need to configure the dedicated large-meeting pool so that each Lync Server 2013 user that is homed on the pool and responsible for managing the meeting schedule has the appropriate permissions. To do this, do the following:

- Set the **Designate as presenter** option to **None**. Typically, one or just a few users of all the participants of a large meeting are presenters, so participants should not be automatically admitted to large meetings as presenters. Instead, the presenters should be explicitly designated at meeting scheduling time, or be explicitly promoted during the large meeting.
- Make sure that the **Assigned conference type by default** check box is not selected. This setting controls whether the Online Meeting Add-in for Lync 2013 always schedules conferences using the organizer’s assigned conference, which means that scheduled meetings have the same join URL and audio information. In small group collaboration scenarios, having such assigned conference type works well because everyone has their own individual assigned conference, and the constant join URL and audio information helps to facilitate faster meeting joining. However, in the large-meeting scenario, the large meeting support staff schedules the large

meetings using a single set of user credentials, and then provides join URLs and audio information to the meeting requesters. In this case, using a different URL to join each meeting works better.
- Ensure that the **Admit anonymous users by default** check box is not selected, unless it is required. This setting affects the default meeting access type scheduled by the Online Meeting Add-in for Lync 2013 when not using an assigned conference. The appropriate option for this setting depends on your organization’s needs. If most large meetings for your organization are internal meetings, do not select this option. If most large meetings require that external users be able to join, select this option.

1.3.8.6.2.2 Managing Large Meetings

Managing Large Meetings

Planning for Conferencing > Support for Large Meetings > Supporting Large Meetings Using Lync Server 2013 >

Topic Last Modified: *2012-10-01*

After setting up a dedicated pool for large conferences, you can take steps to help ensure that large meetings hosted in the pool provide the best user experience. The topics in this section provide details about how to organize and manage large meetings.

- Dedicated Organizers
- Separate Large-Meeting Calendar
- Large-Meeting Scheduling Process
- Scheduling Details
- Running Large Meetings

Dedicated Organizers

Support for Large Meetings > Supporting Large Meetings Using Lync Server 2013 > Managing Large Meetings >

Topic Last Modified: *2012-10-01*

To minimize the real-time communications traffic in the large-meeting pool, we do not recommend hosting users who regularly sign in using Lync clients and participate in instant messaging (IM), presence, conferencing, and voice sessions. Instead, we recommend doing one of the following:

- Create one or more dedicated user accounts just for scheduling large meetings, or
- Home the user accounts of the staff responsible for scheduling large meetings on a large-meeting pool.

In either case, the user accounts that are homed on the large-meeting pool should not be used to regularly sign in to Lync, other than to schedule meetings.

Separate Large-Meeting Calendar

Support for Large Meetings > Supporting Large Meetings Using Lync Server 2013 > Managing Large Meetings >

Topic Last Modified: *2012-10-01*

For each large-meeting pool, you should maintain a separate a calendar of large meetings scheduled on that pool. For example, you can home a single user account on the large-meeting pool and use Outlook with Exchange and Online Meeting Add-in for Lync 2013 to maintain a separate calendar. If you use multiple user accounts to enable a support staff to create large meetings, you can set up a separate calendar that aggregates all large meetings created by the members of the support staff.

Maintaining a separate large meeting calendar helps to prevent conflicts and ensure that only one large meeting is active at any time.

Large-Meeting Scheduling Process

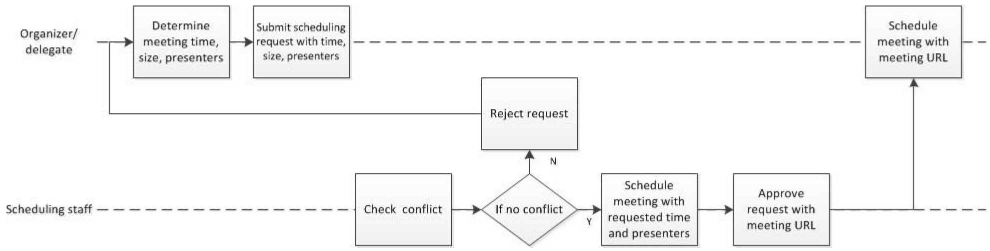
Support for Large Meetings > Supporting Large Meetings Using Lync Server 2013 > Managing Large Meetings >

***Topic Last Modified:** 2012-10-22*

Because only one large meeting at a time is supported on the dedicated large meeting pool, we recommend implementing a large meeting scheduling process to help prevent large meeting conflicts. The purpose of such the scheduling process is to facilitate setting up large meetings. Such capability is not provided directly by Lync Server or Lync Server clients. One way to implement such a process is to use your organization’s support team’s ticketing system, if available.

For organizers of large meetings, scheduling a large meeting involves completing the following steps:

1. The meeting organizer or delegate determines the time, duration, and size of an upcoming meeting, in addition to the list of presenters. If the anticipated meeting size exceeds 250 users or to ensure the best user experience for a meeting of fewer than 250 users, the organizer or the delegate submits a request for a large meeting.
2. The scheduling staff checks to see whether the requested date and time is available. Since we support only a single large meeting on the dedicated pool at a time, the scheduling staff needs to check the large-meeting calendar to determine whether there is another meeting scheduled for the requested date and time. If the requested time is available, the staff approves the meeting request.
3. If the request is approved, the scheduling staff (using credentials on the dedicated pool) uses Online Meeting Add-in for Lync 2013 with Outlook to set up a meeting on the dedicated large-meeting pool. The URL to be used to join the meeting is provided to the requester as part of the approval notice.
4. The meeting organizer or delegate uses Outlook to schedule the upcoming meeting, adding the URL for joining the meeting to the meeting invitation. The meeting organizer or delegate then specifies the users to be invited and sends out the meeting invitation.
   The following figure illustrates a typical request and approval workflow for scheduling large meetings.


Organizer/ delegate
Determine meeting time, size, presenters
Submit scheduling request with time, size, presenters
Schedule meeting with meeting URL
Reject request
N
Scheduling staff
Check conflict
If no conflict
Y
Schedule meeting with requested time and presenters
Approve request with meeting URL

Scheduling Details

Support for Large Meetings > Supporting Large Meetings Using Lync Server 2013 > Managing Large Meetings >

Topic Last Modified: *2012-10-04*

After checking to ensure that no other meeting is scheduled at the requested time, the large meeting support staff that handles the request schedules the meeting on the large-meeting pool. Use the Online Meeting Add-in for Lync that is installed with the Lync Server 2013 client to perform this task, using the credentials of a user enabled for Lync Server in the dedicated large-meeting pool.

To ensure the best user experience, it is important to schedule the large meeting with the right access levels and meeting settings that are appropriate to the meeting organizer's needs. We recommend the following scheduling settings configured in Lync Meeting options:

- Use a new meeting space for each large meeting instead of reusing the dedicated meeting space.
- Specify the meeting access level as follows:
  - If at least one invitee is external to the organization, set the meeting access type to **Anyone (no restrictions**. This enables you to avoid having to manage a potentially large lobby when the meeting is in progress.
  - If the meeting is an internal-only meeting, set the meeting access type to **Anyone from my organization**.

> **Note:**
> Avoid setting the meeting access type to **People I invite from my company** because when you use this setting, organizers must add all user email addresses to the invitee list and you cannot invite a distribution group.
> Avoid setting the meeting access type to **Only me, the meeting organizer** because this setting requires that every meeting participant, including presenters, must be put in the lobby at meeting run time. The person responsible for running the large meeting must then constantly monitor the lobby roster and admit new users who are in the lobby.

- Allow users who dial-in from phones to enter the meeting automatically by checking the **Callers get in directly** setting.
- Explicitly invite the following users:
  - Meeting organizer and delegate (requester)
  - The list of presenters provided by a meeting requester

> **Note:**
> If the meeting access type is set to **People I choose**, you need to explicitly add each participant of a large meeting as an invitee of the meeting.

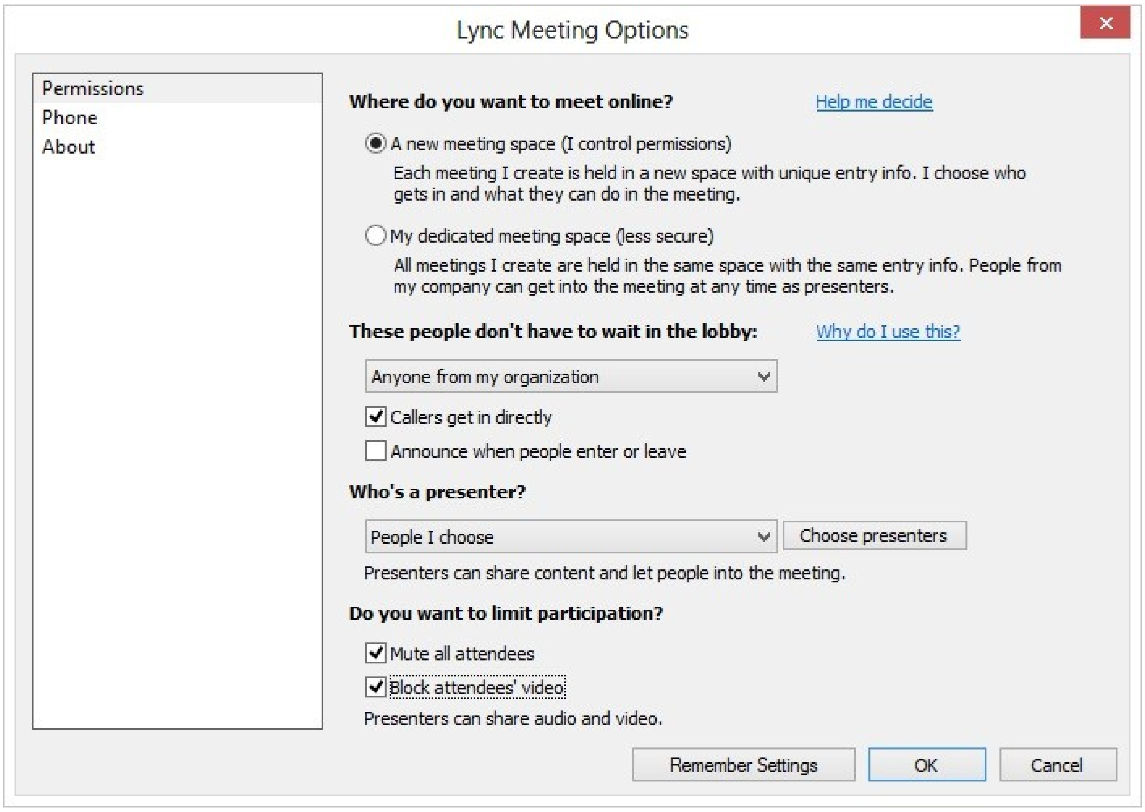
- Explicitly manage presenters, instead of setting the presenter option to one of the auto-promote values. Be sure to add the following users as presenters:
  - Meeting organizer and delegate (requester)
  - The list of presenters provided by large meeting requesters

> **Note:**
> By explicitly managing presenters, you can control the number of presenters, so that you can limit presenters to a small enough number to make it possible to have an effective large meeting. If the majority of meeting participants have the attendee role, it helps reduce the chance of people accidentally taking control of the presentation, deleting a PowerPoint presentation, muting/unmuting presenters, and other disruptions to the meeting.

- Check the **Mute all attendees** setting to make sure that only presenters can broadcast audio into the meeting.

- Check the **Block attendees' video** setting to make sure only presenters can broadcast video into the meeting.

The following figure shows the recommended settings for the Online Meeting Add-in for Lync.



Lync Meeting Options

Where do you want to meet online?

● A new meeting space (I control permissions)

Each meeting I create is held in a new space with unique entry info. I choose who gets in and what they can do in the meeting.

○ My dedicated meeting space (less secure)

All meetings I create are held in the same space with the same entry info. People from my company can get into the meeting at any time as presenters.

These people don't have to wait in the lobby:

Anyone from my organization

☑ Callers get in directly

□ Announce when people enter or leave

Who's a presenter?

People I choose

Presenters can share content and let people into the meeting.

Do you want to limit participation?

☑ Mute all attendees

☑ Block attendees' video

Presenters can share audio and video.

Running Large Meetings

Support for Large Meetings > Supporting Large Meetings Using Lync Server 2013 > Managing Large Meetings >

Topic Last Modified: *2012-10-01*

With serveral hundred to a thousand users in a meeting, it is a good pratice to have a dedicated person moderate the online session of a large meeting. This dedicated person can be a delegate of the meeting organizer or a member of the organization's large-meeting support staff. It is important to add the dedicated meeting moderator as a presenter at the time that the meeting is scheduled, although it is possible to promote an online meeting attendee to the presenter role while the meeting is in progress.

The meeting moderator can use all presenter functionalities of Lync Server 2013 clients to manage the large meeting. Those functionalities include:

1. Monitoring the lobby and admitting or rejecting users in the lobby.
2. Removing any users from the meeting who should not be in the meeting.
3. Changing meeting access types.
4. Changing participant roles.
5. Inviting additional participants during the meeting using Lync drag and drop functionality, phone dial out, or e-mail.
6. Muting and unmuting the audience or individidual users.
7. Managing meeting content, including uploading content, deleting content,

and switching active content.

1.3.8.6.3 Lync Server 2013 Large Meeting Support FAQ

Lync Server 2013 Large Meeting Support FAQ

Planning > Planning for Conferencing > Support for Large Meetings >

Topic Last Modified: *2012-10-22*

The following sections provide answers to common questions for creating and running large meetings.

Q: How many users can participate in a large meeting?

The Lync Server user model specifies limits of 250 users in a shared pool or 1000 users in a pool dedicated to large meetings, but these numbers only represent the number of users we tested and only for the specific set of hardware that we used in our testing. Based on our testing, we recommend those limits for maximum sizes. However, you control the actual number of participants allowed in meetings in your organization by configuring one or more conferencing policies (which you configure using Windows PowerShell cmdlets in the Lync Server Management Shell or using the Lync Server Control Panel). The number that you specify in a conferencing policy can be any 32-bit whole number between 1 and 4,294,967,295, but the recommended size is between 2 and 250 participants, inclusive; and the default value is 250.

Q: How many meetings or other workloads can I have in a pool that is dedicated to large meetings?

To ensure the best user experience in large meetings of up to 1000 participants, we recommend hosting only a single large meeting at a time on a pool that is dedicated to large meetings. We also recommend not allowing any other workloads to run on that pool when the large meeting is in progress.

Q: Should the organizers of large meeting be homed on the dedicated pool?

No. We recommend not homing any users other than the dedicated staff that manages scheduling of large meetings on the dedicated pool. This prevents other real-time communications traffic from causing problems with large meetings that are hosted in the pool. You should schedule large meetings on the dedicated pool using a user account of the large meeting scheduling staff. You should add the user account of the meeting organizer (the user who requests a large meeting) as a presenter for the large meeting.

Q: What media modalities can I use in a large meeting?

Large meetings with up to 1000 users can include audio, video, PowerPoint sharing, whiteboards, and presence polling.

Q: Can I use group instant messaging (IM) in large meetings?

Yes. However, large numbers of instant messages, especially when sent by a large number of meeting participants, can affect the user experience due to problems with fast text scrolling in the IM window. Delivering a large amount of instant messages to up to 1000 users can also introduce significant server loads, which can affect performance. Generally, IM is only required for questions and answers (Q&As).

Can users join large meetings by dialing in from a phone?

Yes. If the Lync Server 2013 pool is properly deployed and enabled for dial-in conferencing, users will be able to join the large meetings by dialing in. Our testing has shown that up to 15% of the 1000 users can join the large meeting over a 10 minute period.

Q: Can I host large meetings in a virtual topology?

We have not tested large meetings in a virtual topology, so we do not support the use of virtual machines to host a dedicated pool for large meetings.

1.3.9 Planning for External User Access

Planning for External User Access

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2013-01-19*

Communications in most organizations involve services and users that are not inside your internal network. These services and users include employees who are temporarily or permanently offsite, employees of customer or partner organizations, people who use public instant messaging (IM) services, and potential customers, partners and anonymous users whom you invite to meetings and presentations. In this documentation, these people are collectively referred to as *external users*.

With Microsoft Lync Server 2013, users in your organization can use IM and presence to communicate with external users, and they can participate in audio/video (A/V) conferencing and web conferencing with your offsite employees and other types of external users. You can also support external access from mobile devices and over Enterprise Voice. External users who are not members of your organization can participate in Lync Server 2013 meetings, allowing anonymous attendees.

To support communications across your organization’s firewall, you deploy Lync Server 2013 Edge Server in your perimeter network (also known as DMZ, demilitarized zone, and screened subnet). The Edge Server controls how users outside the firewall can connect to your internal Lync Server 2013 deployment. It also controls communications with external users that originate within the firewall.

Depending on your requirements, you can deploy one or more Edge Servers in one or more locations. This section describes scenarios for external user access in Lync Server 2013, and it explains how to plan your edge and reverse proxy topology.

Note:

Although you need an Edge Server to support Enterprise Voice and external user access, this section focuses on support for IM, presence, A/V conferencing, federation, web conferencing, and Lync Mobile. For details about support for Enterprise Voice, see Planning for Enterprise Voice in the Planning documentation.

- Changes in Lync Server 2013 That Affect Edge Server Planning
- System Requirements for External User Access Components
- Overview of External User Access
- Understanding Autodiscover
- Choosing a Topology
- Data Collection
- Determine DNS Requirements
- Determine External A/V Firewall and Port Requirements
- Plan for Edge Server Certificates
- Scenarios for External User Access

1.3.9.1 Changes in Lync Server 2013 That Affect Edge Server Planning

Changes in Lync Server 2013 That Affect Edge Server Planning

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2012-10-22*

Lync Server 2013 introduces new features that extend the features and communications methods for your users. Also, Lync Server 2013 introduces changes to existing services to better integrate and extend the services that are available to your organization. Following is a summary of changes that may affect your planning and deployment of Lync Server 2013 Edge Server services.

Support for IPv6 Addressing

Lync Server 2013 supports IPv6 addressing for all Edge Server services. If you have provided IPv6 addresses for the interfaces through configuration in Windows Server, you can use IPv6 addresses in your Edge Server configuration through the IP address configuration in Topology Builder. Additionally, the extensible messaging and presence protocol (XMPP) supports IPv6. No additional configuration is required. If IPv6 is configured in the topology, XMPP will use IPv6 (where required).

An added requirement to support IPv6 in Lync Server 2013 is to create domain name system records for records that must be discovered and resolved to an IPv6 address. IPv6 DNS uses host records that are defined as **AAAA** and called “quad-A”. Other record types are consistent with their IPv4 counterparts.

Support for Extensible Messaging and

Presence Protocol (XMPP) Deployment

Edge Server introduces a fully integrated XMPP proxy (deployed on the Edge Servers) and an XMPP gateway (deployed on your Front End Servers). You can deploy XMPP federation as an optional component. By adding and configuring the XMPP proxy and XMPP gateway, you can enable your Microsoft Lync 2013 users to add contacts from XMPP-based partners for instant messaging (IM) and presence.

Note:

Currently, the XMPP services in Edge Server only provide IM and presence between Lync Server clients and XMPP-based contacts. Additionally, XMPP is hosted in only one site.

Important:

The XMPP capability of Lync Server 2013 is tested and supported by Microsoft for instant messaging federation with Google Talk. For any other XMPP systems contact the third-party vendor to verify that they support federation with Lync Server 2013, and for any deployment or troubleshooting recommendations.

Support for Rolling Audio/Video Authentication and Server to Server Authentication Certificates

A certificate is used to generate tokens that are issued to clients and other consumers of the A/V Authentication service and for server to server authentication. The Audio/Video Authentication certificate is of type *AudioVideoAuthentication* and the Server to Server Authentication certificate is of type *OAuthTokenIssuer*.

For Audio/Video Authentication, tokens are used to authenticate port allocation requests, and the tokens are cached for up to 8 hours – the default lifetime of the token. Under normal operation, this is a very reliable method to create and distribute authentication material to the A/V consumers. However, certificates have a finite lifetime and expire on a predefined date and time (based on creation date and the policies enforced at the certification authority that created the certificate, typically 2 years for this type of certificate). When the certificate expires, any tokens created by the expired certificate and cached by consumers become not valid. Any attempts to use a token created with an expired certificate would result in failed Media Relay allocations and any current Audio/Video sessions will fail. The client would need to acquire a new token created by a valid certificate to resume normal Audio and Video functionality.

Server to Server Authentication is managed by a global certificate that is requested and applied to all servers in the deployment. The certificate is responsible for authenticating servers in Lync Server 2013 as well as authenticating to Exchange 2013 and Microsoft SharePoint Server 2013. For more information on how Server to Server Authentication works, see Managing Server-to-Server Authentication (Oauth) and Partner Applications. One very important difference between the Audio/Video Authentication process and the Server to Server Authentication process is the lifetime of the authentication, or tokens. For Audio/Video Authentication, the authentication expires after eight hours. Server-to-Server Authentication has a lifetime of 24 hours. You must plan accordingly for each of the certificate types.

New for Lync Server 2013 is the ability to stage a replacement Audio/Video Authentication certificate and Server to Server Authentication certificate in advance of the expiration of the current certificate. The new certificate is then used for generating new tokens or new authentication requests. but retains the old certificate for verifying the current sessions and authentications.. What this accomplishes is to effectively prevent nearly all failures due to token and certificate expirations. For details of this feature and how to configure it, see Staging AV and OAuth Certificates Using -Roll in Set-CsCertificate

Reduced Reliance on Cookie-based Affinity

In previous versions of Lync Server and Office Communications Server, cookie-based affinity was used by the Web services to ensure that the client and Web services session state was maintained. Lync Server 2013 Web services use a built in affinity mechanism that eliminates most of the requirements for cookie-based affinity.

⚠**Warning:**

The Microsoft Lync 2010 Mobile client must still use cookie-based affinity and will require configuration of cookie-based affinity until you have migrated all clients to the upcoming Microsoft Lync Mobile client (Date of release not yet determined).

For details about cookie-based affinity in Lync Server 2013, see Components Required for External User Access.

AutoDiscover Enhancements

The autodiscover feature in Lync Server 2013 enables clients to locate additional features that are made available for communication. Autodiscover was first introduced in the cumulative update for Lync Server 2010: November 2011 for Mobility and Microsoft Lync 2010 Mobile. The autodiscover feature (also known by the DNS record names LyncDiscover and LyncDiscoverInternal) allows clients to locate and use mobility services (for Microsoft Lync 2010 Mobile clients), the Microsoft Lync Web App, and the Lync Web scheduler, as well as communications with Microsoft Exchange Server and SharePoint Server. Autodiscover is installed as normal part of the setup and deployment of your infrastructure and Lync Server 2013 servers. The Topology Builder and Lync Server Deployment Wizard eliminate most of the configuration tasks that were required in cumulative update for Lync Server 2010: November 2011.

Services for Mobile Clients

Introduced in the cumulative update for Lync Server 2010: November 2011, mobility services in Lync Server 2013 enable mobile phones running Lync Mobile and tablet devices using supported Apple iOS, Android, Windows Phone, or Nokia mobile devices to perform activities such as sending and receiving instant messages, viewing contacts, and viewing presence. In addition, mobile devices support some Enterprise Voice features, such as click to join a conference, Call via Work, single number reach, voice mail, and missed call notification.

Note:

The mobility services use the reverse proxy and published services that are deployed on your Front End Servers. No changes are required to Edge Servers. Minimally you need outbound SIP/TCP/5061from the server running the Lync Server Access Edge service.

Director Role is Optional

The role of the Director server in the Lync Server 2013 topology has not changed. It still hosts web services, preauthenticates incoming user requests, and directs external users to their home pool. By changing the Director from a recommended role to an optional role, Microsoft does not intend to diminish the value of the Director. The intention is to reduce server count and other hardware requirements (for example, hardware load balancers for the Director) without compromising features and functionality. Because the Front End Servers can do the same job as the Director with no impact to services provided, you can deploy Directors if you choose to. You can safely exclude the Director with confidence that the Front End Servers will provide the same services in place of a Director.

1.3.9.2 System Requirements for External User Access Components

System Requirements for External User Access Components

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2013-01-17*

System requirements for edge components include hardware, software, and collocation requirements for Edge Servers, reverse proxy servers and optional Directors that you plan to deploy.

- Components Required for External User Access
- Configuration Requirements for Reverse Proxy
- Hardware Load Balancer Requirements
- Hardware and Software Requirements for Edge Components
- Supported Server Collocation for Edge Components

1.3.9.2.1 Components Required for External User Access

Components Required for External User Access

See Also

Planning > Planning for External User Access > System Requirements for External User Access Components >

Topic Last Modified: *2013-01-17*

Most Edge components are deployed in a perimeter network. The following components make up the edge topology of the perimeter network. Except where noted, the components are part of the Scenarios for External User Access and are in the perimeter network. Edge components include the following:

- Edge Servers
- Reverse proxies
- Firewalls
- Directors (optional, and logically located on the internal network)
- Load balancing for Scaled Edge Topologies (either DNS load balancing or a hardware load balancer)

Important:
Using DNS load balancing on one interface and hardware load balancing on the other is not supported. You must use hardware load balancing for both interfaces or DNS load balancing for both.

Edge Servers

The Edge Servers send and receive network traffic for the services offered by internal deployment by external users. The Edge Server runs the following services:

- **Access Edge service** The Access Edge service provides a single, trusted connection point for both outbound and inbound Session Initiation Protocol

(SIP) traffic.

- **Web Conferencing Edge service** The Web Conferencing Edge service enables external users to join meetings that are hosted on your internal Lync Server 2013 deployment.
- **A/V Edge service** The A/V Edge service makes audio, video, application sharing, and file transfer available to external users. Your users can add audio and video to meetings that include external participants, and they can communicate using audio and/or video directly with an external user in point-to-point sessions. The A/V Edge service also provides support for desktop sharing and file transfer.
- **XMPP Proxy service** The XMPP Proxy service accepts and sends extensible messaging and presence protocol (XMPP) messages to and from configured XMPP Federated partners.

Authorized external users can access the Edge Servers in order to connect to your internal Lync Server 2013 deployment, but the Edge Servers do not provide a means for any other access to the internal network.

Reverse Proxy

The reverse proxy is required for the following:

- To allow users to connect to meetings or dial-in conferences using simple URLs
- To enable external users to download meeting content
- To enable external users to expand distribution groups
- To allow the user to obtain a user-based certificate for client certificate based authentication
- To enable remote users to download files from the Address Book Server or to submit queries to the Address Book Web Query service
- To enable remote users to obtain updates to client and device software
- To enable mobile devices to automatically discover Front End Servers offering mobility services
- To enable push notifications to mobile devices from the Office 365 or Apple push notification services

For additional information related to reverse proxies and the requirements that reverse proxies must meet, see the details in Configuration Requirements for Reverse Proxy.

Note:

External users do not need a virtual private network (VPN) connection to your organization in order to participate in communications using Lync Server 2013. If you have implemented VPN technology in your organization and your users use the VPN for Lync, media traffic (such as video conferencing) can be adversely affected. You should consider providing a means for media traffic to connect to the AV Edge service directly and bypass the VPN. For details, see the NextHop Blog article, “Enabling Lync Media to Bypass a VPN Tunnel,” at http://go.microsoft.com/fwlink/p/?LinkId=256532.

Firewall

You can deploy your edge topology with only an external firewall or both external and internal firewalls. The scenario architectures include two firewalls. Using two firewalls is the recommended approach because it ensures strict routing from one network edge to the other, and it protects your internal deployment behind two levels of firewall.

Director

A Director is a separate, optional server role in Lync Server 2013 that does not home user accounts, or provide presence or conferencing services. It serves as an internal next hop server to which an Edge Server routes inbound SIP traffic destined for internal servers. The Director preauthenticates inbound requests and redirects them to the user's home pool or server. By preauthenticating at the Director, you can drop requests from user accounts that are unknown to the deployment.

A Director helps insulate Standard Edition servers and Front End Servers in Enterprise Edition Front End pools from malicious traffic such as denial-of-service (DoS) attacks. If the network is flooded with invalid external traffic in such an attack, the traffic ends at the Director. For details about the use of Directors, see Scenarios for the Director.

⊟See Also

Concepts

Hardware Load Balancer Requirements

1.3.9.2.2 Configuration Requirements for Reverse Proxy

Configuration Requirements for Reverse Proxy

Planning > Planning for External User Access > System Requirements for External User Access Components >

Topic Last Modified: *2013-03-05*

Lync Server 2013 imposes a few requirements on communications from the external client that are then passed on to the external Web services hosted on the Director, Director pool, Front End Server or Front End pool. The reverse proxy is also responsible for publishing the Office Web Apps Server, if you are offering conferencing to your users.

> **Note:**
>
> Lync Server 2013 does not specify a particular reverse proxy that you must use. Lync Server 2013 only defines operational requirements that the reverse proxy must be able to do. Typically, the reverse proxy that you already have deployed in your infrastructure may be able to meet the requirements.

Reverse Proxy Requirements

The functional operations that Lync Server 2013 expect a reverse proxy to perform are:

- Use secure socket layer (SSL) and transport layer security (TLS) implemented by using certificates acquired from a public certification authority to connect to the published external Web services of the Director, Director pool, Front End Server or Front End pool. The Director and the Front End Server can be in a load-balanced pool by using hardware load balancers.
- Able to publish internal Web sites using certificates for encryption, or publish them over an unencrypted means, if needed.
- Able to publish an internally hosted web site externally by using a fully qualified domain name (FQDN).
- Able to publish all contents of the hosted web site. By default, you can use the **/*** directive, which is recognized by most web servers to mean "Publish all content on the web server." You can also modify the directive—for example, **/Uwca/***, which means "Publish all content under the virtual directory Ucwa."
- Must be configurable to require Secure Sockets Layer (SSL) and/or Transport Layer Security (TLS) connections with clients that request content from a published website.
- Must accept certificates with subject alternative name (SAN) entries.
- Must be able to allow binding of a certificate to a listener or interface through which the external web services FQDN will resolve. Listener configurations are preferable to interfaces. Many listeners can be configured on a single

interface.

- Must allow for the configuration of host header handling. Often, the original host header sent by the requesting client must be passed transparently, instead of being modified by the reverse proxy.
- Bridging of SSL and TLS traffic from one externally defined port (for example, TCP 443) to another defined port (for example, TCP 4443). The reverse proxy may decrypt the packet on receipt and then reencrypt the packet on sending.
- Bridging of unencrypted TCP traffic from one port (for example, TCP 80) to another (for example, TCP 8080).
- Allow configuration of, or accept, NTLM authentication, No authentication and Pass-through authentication.

1.3.9.2.3 Hardware Load Balancer Requirements

Hardware Load Balancer Requirements

Planning > Network Planning for Lync Server > Load Balancing Requirements >

Topic Last Modified: *2012-10-22*

The Lync Server 2013 scaled consolidated Edge topology is optimized for DNS load balancing for new deployments federating primarily with other organizations using Lync Server. If high availability is required for any of the following scenarios, a hardware load balancer must be used on Edge Server pools for the following:

- Federation with organizations using Office Communications Server 2007 R2 or Office Communications Server 2007
- Exchange UM for remote users using Exchange UM prior to Exchange 2010 with SP1
- Connectivity to public IM users

Important:

Using DNS load balancing on one interface and hardware load balancing on the other is not supported. You must use hardware load balancing for both interfaces or DNS load balancing for both.

Note:

If you are using a hardware load balancer, the load balancer deployed for connections with the internal network must be configured to load balance only the traffic to servers running the Access Edge service and the A/V Edge service. It cannot load balance the traffic to the internal Web Conferencing Edge service or the internal XMPP Proxy service.

Note:

The direct server return (DSR) NAT is not supported with Lync Server 2013.

To determine whether your hardware load balancer supports the necessary features required by Lync Server 2013, see "Lync Server 2010 Load Balancer Partners" at http://go.microsoft.com/fwlink/p/?linkId=202452.

Hardware Load Balancer Requirements for Edge Servers Running the A/V Edge Service

Following are the hardware load balancer requirements for Edge Servers running the A/V Edge service:

- Turn off TCP nagling for both internal and external ports 443. Nagling is the process of combining several small packets into a single, larger packet for more efficient transmission.

- Turn off TCP nagling for external port range 50,000 – 59,999.
- Do not use NAT on the internal or external firewall.
- The edge internal interface must be on a different network than the Edge Server external interface and routing between them must be disabled.
- The external interface of the Edge Server running the A/V Edge Service must use publically routable IP addresses and no NAT or port translation on any of the edge external IP addresses.

Hardware Load Balancer Requirements

Cookie-based affinity requirements are greatly reduced in Lync Server 2013 for Web services. If you are deploying Lync Server 2013 and will not retain any Lync Server 2010 Front End Servers or Front End pools, you do not need cookie-based persistence. However, if you will temporarily or permanently retain any Lync Server 2010 Front End Servers or Front End pools, you still use cookie-based persistence as it is deployed and configured for Lync Server 2010.

Note:

If you decide to use cookie-based affinity even though your deployment does not require it, there is no negative impact to doing so.

For deployments that **will not use** cookie-based affinity:

- On the reverse proxy publishing rule for port 4443, set **Forward host header** to True. This will ensure that the original URL is forwarded.

For deployments that **will use** cookie-based affinity:

- On the reverse proxy publishing rule for port 4443, set **Forward host header** to True. This will ensure that the original URL is forwarded.
- Hardware load balancer cookie MUST NOT be marked httpOnly
- Hardware load balancer cookie MUST NOT have an expiration time
- Hardware load balancer cookie MUST be named **MS-WSMAN** (This is the value that the Web services expect, and cannot be changed)
- Hardware load balancer cookie MUST be set in every HTTP response for which the incoming HTTP request did not have a cookie, regardless of whether a previous HTTP response on that same TCP connection had already obtained a cookie. If the load balancer optimizes cookie insert to only occur once per TCP connection, that optimization MUST NOT be used

Note:

Typical hardware load balancer configurations use source-address affinity and a 20 min. TCP session lifetime, which is fine for Lync Server and Lync 2013 clients because session state is maintained through client usage and/or and application interaction.

If you are deploying mobile devices, your hardware load balancer must be able to load balance individual request within a TCP session (in effect, you must be able to load balance an individual request based on the target IP address).

⚠**Warning:**

F5 hardware load balancers have a feature called OneConnect that ensures each request within a TCP connection is individually load balanced. If you are deploying mobile devices, ensure your hardware load balancer vendor supports the same functionality. The latest Apple iOS mobile apps require Transport Layer Security (TLS) version 1.2. F5 provides specific settings for this.
For details on third party hardware load balancers, see http://go.microsoft.com/fwlink/p/?linkId=230700

Following are the hardware load balancer requirements for Director and Front End pool Web Services:

- For internal Web Services VIPs, set Source_addr persistence (internal port 80, 443) on the hardware load balancer. For Lync Server 2013, Source_addr persistence means that multiple connections coming from a single IP address are always sent to one server to maintain session state.
- Use TCP idle timeout of 1800 seconds.
- On the firewall between the reverse proxy and the next hop pool's hardware load balancer, create a rule to allow https: traffic on port 4443, from the reverse proxy to the hardware load balancer. The hardware load balancer must be configured to listen on ports 80, 443, and 4443.

Summary of Hardware Load Balancer Affinity Requirements

Client/user location	External web services FQDN affinity requirements	Internal web services FQDN affinity requirements
Lync Web App (internal and external users) Mobile device (internal and external users)	No affinity	Source address affinity
Lync Web App (external users only) Mobile device (internal and external users)	No affinity	Source address affinity
Lync Web App (internal users only) Mobile device (not deployed)	No affinity	Source address affinity

Port Monitoring for Hardware Load Balancers

You define port monitoring on the hardware load balancers to determine when specific services are no longer available due to hardware or communications failure. For example, if the Front End Server service (RTCSRV) stops because the Front End Server or Front End pool fails, the HLB monitoring should also stop receiving traffic on the Web Services. You implement port monitoring on the HLB to monitor the following:

Front End Server User Pool – HLB Internal Interface

Virtual IP/Port	Node Port	Node Machine/ Monitor	Persistence Profile	Notes
<pool>web-int_mco_443_vs 443	443	Front End 5061	Source	HTTPS
<pool>web-int_mco_80_vs 80	80	Front End 5061	Source	HTTP

Front End Server User Pool – HLB External Interface

Virtual IP/Port	Node Port	Node Machine/ Monitor	Persistence Profile	Notes
<pool>web_mco _443_vs 443	4443	Front End 5061	None	HTTPS
<pool>web_mco _80_vs 80	8080	Front End 5061	None	HTTP

1.3.9.2.4 Hardware and Software Requirements for Edge Components

Hardware and Software Requirements for Edge Components

Planning > Planning for External User Access > System Requirements for External User Access Components >

Topic Last Modified: *2013-02-21*

The hardware and software requirements for edge components include those for the Microsoft Lync Server 2013 communications software components, including Edge Servers and the optional Directors, as well as those for other components, including reverse proxy servers, firewalls, and load balancers to be deployed the perimeter network to support external user access. For details about the components required to support external user access and supported topologies, see Components Required for External User Access.

Hardware and Software Requirements for Edge Servers

The operating system requirements for Edge Servers are the same as for the other Lync Server 2013 roles: the 64-bit edition of the Windows Server 2008 R2 SP1 or Windows Server 2012.

The following table shows the hardware requirements for Edge Servers.

Hardware System Requirements for Edge Servers

Hardware component	Minimum requirement
CPU	One of the following: • 64-bit dual processor, quad-core, 2.0 GHz or higher • 64-bit 4-way processor, dual-core, 2.0 GHz or higher
Memory	12 GB recommended
Disk	• One of the following: • 10K RPM hard disk drive (HDD) • High-performance solid state drive (SSD) with performance equal to or better than 10K RPM HDD • 2x RAID 10 (striped and mirrored) 15K

	RPM disk set
Network	Two interfaces required, either one 2-port 1 Gbps NIC or two 1-port 1 Gbps NICs.

Lync Server 2013 is available only in 64-bit, therefore each Edge Server requires one of the following operating systems.

- Windows Server 2008 R2 Enterprise Edition with SP1 operating system, or Windows Server 2008 R2 Standard Edition with SP1 operating system.
- Windows Server 2012 Enterprise or Datacenter operating system.

Directors are internal components and installed as part of the internal network prior to deployment of Edge Servers. For hardware and software requirements for Directors, see Hardware and Software Requirements for the Director.

Lync Server 2013 Edge Servers require the installation of additional programs and updates. The requirements for additional software on Edge Servers are listed here.

- Each server running Lync Server 2013 must have the correct release of Windows PowerShell 3.0 installed. For details, see Installing Windows PowerShell 3.0.
- Lync Server requires Microsoft .NET Framework 4.5. For Lync Server 2013 installed on Windows Server 2008 R2, you must manually install the 64-bit edition of Microsoft .NET Framework 4.5 on the server prior to installing Lync Server 2013. To manually install it, download the Microsoft .NET 4.5 Framework from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?LinkId=268529
- **Windows Identity Foundation** in Lync Server 2013 requires the installation of Windows Identity Foundation in order to support server to server authentication scenarios. Windows Server 2008 R2 and Windows Server 2012 require different procedures to install the Windows Identify Foundation. Select your server operating system from the following list:
  - Windows Server 2008 R2   For Windows Server 2008 R2, you check to see if it has already been installed on your computer. To do this, go to **Add/ Remove Programs**, **View Installed Updates**, and look under **Windows** for the entry **Windows Identity Foundation (KB974405)**. For details about installing Windows Identity Foundation, see http://go.microsoft.com/fwlink/?LinkId=285258.
  - Windows Server 2012   For Windows Server 2012, you use **Server Manager** to install the Windows Identity Foundation. In the Server Manager **Add Roles and Features Wizard**, select **Features**. Select **Windows Identity Foundation 3.5** from the list. Click **Next**, then click **Install**.

1.3.9.2.5 Supported Server Collocation for Edge Components

Supported Server Collocation for Edge Components

Planning > Planning for External User Access > System Requirements for External User Access Components >

Topic Last Modified: *2012-09-08*

The Access Edge service, Web Conferencing Edge service, A/V Edge service and XMPP Proxy service are collocated on the Edge Servers. The following servers provide functions needed for external user access and must be deployed as dedicated servers:

- Edge Server
- Director (Optional)
- Reverse proxy

Important:
The reverse proxy does not need to be dedicated to serving only Lync Server 2013. For example, you can provide services to publish the Lync Server Web services, and concurrently provide a published Web site for another Web site that has no bearing on Lync Server at all. If you already have a reverse proxy server in the perimeter network to support other services, you can use it for Lync Server 2013.

1.3.9.3 Overview of External User Access

Overview of External User Access

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2012-10-13*

In this documentation, we use the term *external user* to define a large category of users who communicate with your Lync Server 2013 and Lync 2013 users from outside the firewall. External users that you can authorize to communicate Lync Server 2013 with internal users (that is, users who sign in to Lync Server from inside the firewall) can include the following:

- **Remote users** Users of your organization who sign in to Lync Server from outside the firewall (for example, business travelers and telecommuters) by using a virtual private network (VPN), Microsoft Direct Access (a feature of Windows Server 2008 R2 and Windows Server 2012), clients using transport layer security connection (TLS)), or the Lync Web App by using a browser.
- **Federated users** Users who have an account with a trusted customer or partner organization, such as Lync Server 2010, Lync Server 2013 or Office Communications Server 2007 R2. Federated users can also be members of defined partner organizations using extensible messaging and presence protocol (XMPP) by way of the XMPP proxy on the Edge Server and XMPP gateway on the Front End Server or pool. A defined trust relationship, called a federation, is not related to or dependent upon an Active Directory Domain Services (AD DS) trust relationship.
- **Public Instant Messaging Connectivity users** Contacts that your users establish through public instant messaging connectivity services (Windows Live, Yahoo! and AOL).
- **Mobile users** Users that are members of your organization that use a smart phone or tablet running a Lync Mobile client sign in to your internal deployment and are able to communicate with the other classes of users. The mobile user uses mobility services that are published through the reverse proxy to access the internal deployment. For details on features and capabilities available to Lync Mobile , see the Mobile Client Comparison Tables at http://go.microsoft.com/fwlink/p/?LinkID=234777.
- **Anonymous users** Users who do not have a user account in your organization's Active Directory Domain Services (AD DS) or in a supported federated domain, but who have received invitations to participate remotely in an on-premises conference.

Your edge deployment provides external access for the following types of communication:

- **IM and presence** Authorized external users can participate in IM conversations and conferences, and they can get information about one another’s presence status. Users of public IM service providers can participate in IM conversations with individual Lync Server users in your organization and access presence information, but they cannot participate in IM multiparty conferences using Lync Server. It is strictly peer-to-peer communication. File transfer is not supported for users of public IM service providers, and audio/video in peer-to-peer communications is supported for Windows Messenger 2011 users, but not other users of public IM service providers.

Both SIP and XMPP protocols are supported. To provide services for XMPP, see Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation.

- **Web conferencing** Authorized external users can participate in conferences that are hosted on your Lync Server deployment. Remote users, federated users, and anonymous users can be enabled for participation in web conferencing, but public IM users cannot participate in conferences. Depending on the options that you select, web conferencing-enabled users can participate in desktop and application sharing and can act as meeting organizers or presenters.
- **A/V conferencing** Authorized external users can participate in audio and video conferences that your Lync Server deployment hosts. Audio/video in peer-to-peer communications is supported for Windows Messenger 2011 users, but not for other users of public IM service providers.

In order to control communications, you can configure one or more policies that define how users inside and outside your organization communicate with each other. You can also configure settings and apply policies for individual internal users or for specific types of external users to control communications with external users.

Lync Server 2013 roles that are used to provide external access:

Edge Server The Edge Server is a server or a pool of servers that run the services that allow external access to IM and presence, conferencing, audio/video, and other media (for example, file transfer) services. Optionally, you can configure the Edge Server to federate with other Lync Server or Office Communications Server 2007 R2 deployments, and other XMPP deployments. The optional public IM connectivity feature is enabled and configured through the Edge Server.

Director The Director is an optional server or server pool running the Lync Server 2013 Director role that pre-authenticates user requests and routes requests to the users' home Front End Server or Front End pool, but does not home any user accounts.

Reverse Proxy A reverse proxy is a general term for specialized servers that publish resources available on the internal network and retrieve information for clients from the published resource. Lync Server 2013 uses the reverse proxy to publish a number of features, such as conferencing meetings, conference join locations, the address book, distribution list expansion, downloading meeting content, device updates, Mobility services, and more. Any reverse proxy that can meet the requirements for publishing the necessary resource locations can be used. Microsoft Forefront Threat Management Gateway (TMG) 2010 is used as an example for the purposes of illustrating the publishing rules necessary, but Forefront TMG 2010 is not required.

Important:

Lync Server 2013 supports both IPv4 and IPv6. Windows Server 2008 R2 and Windows Server 2012 uses a dual stack that can use both IPv4 and IPv6 concurrently. This is important because of the transitional nature of a deployment moving from IPv4 to IPv6. IPv4 can be supported in some areas, where in other areas of the deployment, IPv6 can be used. This is especially important where the Internet and internal deployments are concerned. External clients must communicate through the reverse proxy to use services such as mobility, meetings, address book download, and others. Currently, Forefront Threat Management Gateway 2010 and Internet Security and Acceleration Server 2006 do not support IPv6 addressing, regardless of the operating system version that they are deployed on. You must plan accordingly in relation to your use of IPv6 and IPv4 as they relate to external clients.

1.3.9.4 Understanding Autodiscover

Understanding Autodiscover

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2013-03-05*

The Lync Server 2013 Autodiscover Service is a feature that was originally introduced in Microsoft Lync Server 2010 as part of the Cumulative Update for Lync Server 2010: November 2011. In addition to fixes, this cumulative update delivered support for Lync Mobile and Lync 2013 clients.

In Lync Server 2013, the Autodiscover Service is an integral part of the operation of external and internal mobile clients, and Autodiscover is also extended to new clients, such as the recently introduced Lync Windows Store app for Windows 8. Autodiscover is also used by the Lync 2013 desktop clients. Autodiscover is recognized in Lync Server by the required domain name system (DNS) records **lyncdiscover.<domain>** and **lyncdiscoverinternal.<domain>**. Additionally, newer versions of the Lync 2010 and Lync 2013 desktop client prefer Autodiscover over the domain name system (DNS) SRV records, using DNS SRV records only if lyncdiscover.<domain> or lyncdiscoverinternal.<domain> does not respond or does not resolve. The Lync Windows Store app for Windows 8 and Lync Mobile uses Autodiscover exclusively and will not refer to the traditional DNS SRV records.

In Lync Server 2013, Autodiscover is expanded to communicate to the client which elements, features, and communication methods are available to the client. The information is communicated through a request that is sent from the client, and the Lync Server web services responds with a clearly defined response that names what is available to the client, and how to contact those features in the format of the Autodiscover Response document.

The best way to understand the Autodiscover response document, including how the web services communicate features to clients through this document, is to dissect and define each line in a typical response from the Lync web service Autodiscover response document.

> **Note:**
>
> In the details that follow, the user has already authenticated to the home server by responding to an authentication request.

> **Note:**
>
> The Lync Autodiscover Web Service is defined in the **Microsoft Office Protocols** in the **Open Specifications** section of the **Microsoft Developer Network** (MSDN) library. For details, see the full specification document, "Lync Autodiscover Web Service Protocol," at: http://go.microsoft.com/fwlink/?LinkId=273839. For details about authentication, see "OC Authentication Web Service Protocol" at http://go.microsoft.com/fwlink/?LinkId=279015.

The Lync Server Web Service Autodiscover Response

The response returned when the Autodiscover request is sent is the same for an internal or an external client. Some parameters that are location–aware may change. If a client request is received, but the actual pool is other than the one that has been contacted, the user’s home pool will be set for that user. A colleague whose user account is on a different pool, but logging in from the same office, would get a slightly different response. The response indicates the correct Front End Server or Front End pool for that user.

An example of an Autodiscover Response document:

```
<AutodiscoverResponse xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="htt
   <User>
      <SipServerInternalAccess fqdn="pool01.contoso.com" port="5061"/>
      <SipClientInternalAccess fqdn=" pool01.contoso.com" port="443"/>
      <SipServerExternalAccess fqdn="sip.contoso.com" port="5061"/>
      <SipClientExternalAccess fqdn="sip.contoso.com " port="443"/>
      <Link token ="External/Autodiscover" href="https://webexternal.contoso.com/
      <Link token="Internal/Autodiscover" href="https://webinternal.contoso.net/A
      <Link token="External/AuthBroker" href="https://webexternal.contoso.com/Rea
      <Link token="Internal/AuthBroker" href="https://webinternal.contoso.net/Rea
      <Link token="External/WebScheduler" href="https://webexternal.contoso.com/S
      <Link token="Internal/WebScheduler" href="https://webinternal.contoso.net/S
      <Link token="External/Mcx" href="https://webexternal.contoso.com/Mcx/McxSer
      <Link token="Internal/Mcx" href="https://webexternal.contoso.net/Mcx/McxSer
      <Link token="External/Ucwa" href="https://webexternal.contoso.com/ucwa/v1/a
      <Link token="Internal/Ucwa" href="https://webinternal.contoso.net/ucwa/v1/a
      <Link token="Ucwa" href="https://webexternal.contoso.com/ucwa/v1/applicatio
      <Link token="External/XFrame" href="https://webexternal.contoso.com/Autodis
      <Link token="Internal/XFrame" href="https://webinternal.contoso.net/Autodis
      <Link token="XFrame" href="https://webexternal.contoso.com/Autodiscover/XFr
      <Link token="Self" href="https://webexternal.contoso.net/Autodiscover/Autod
   </User>
</AutodiscoverResponse>
```

Autodiscover Response Document Details

The Autodiscover Response document can be in one of two formats. The default format is a JavaScript Object Notation (JSON). The other format is extensible markup language (XML) document. The XML is used for this example. The request and response are predictable because the document has a defined schema that determines the format. The line in the document that describes the schema used is the first line in the request or response:

```
<AutodiscoverResponse xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="htt
```

The definition of **AccessLocation=”External”** indicates that the request was made from an external user.

```
<SipServerInternalAccess fqdn="pool01.contoso.com" port="5061"/>
```

```
<SipServerExternalAccess fqdn="sip.contoso.com" port="5061"/>
```

SipServerInternalAccess and SipServerExternalAccess are currently not used. These entries are reserved for future use.

```
<SipClientInternalAccess fqdn=" pool01.contoso.com" port="443"/>
```

```
<SipClientExternalAccess fqdn="sip.contoso.com " port="443"/>
```

SipClientInternalAccess and SipClientExternalAccess describe the fully qualified domain name and port that an internal or external client will use to access the defined SIP Server. The Lync desktop client and the Lync Windows Store app use these entries, based on their location (internal or external) to find the Director or Front End Server.

```
<Link token="Internal/Autodiscover" href="https://webinternal.contoso.net/Autodis
```

```
<Link token ="External/Autodiscover" href="https://webexternal.contoso.com/Autodi
```

The `Autodiscover` references contain the service entry points for the Autodiscover service. The token attribute contains the name of the service, and the href is a URL that defines for the client where the service can be found. Clients on an external network use the `External/Autodiscover`. The Autodiscover service is installed as part of the deployment process. `Internal/Autodiscover` is not currently used, and is reserved for future use.

```
<Link token="Internal/AuthBroker" href="https://webinternal.contoso.net/Reach/sip
```

```
<Link token="External/AuthBroker" href="https://webexternal.contoso.com/Reach/sip
```

The `AuthBroker` references contain the service entry points for the internal and the external authentication broker service, in this case, sip.svc. The token attribute contains the name of the service, and the href is a URL that defines for the client where the service can be found. Clients on the internal network with use `Internal/AuthBroker`. Clients on an external network use the `External/AuthBroker`. The AuthBroker service is installed as part of the deployment process of your internal Lync Server 2013 deployment web services.

```
<Link token="Internal/WebScheduler" href="https://webinternal.contoso.net/Schedul
```

```
<Link token="External/WebScheduler" href="https://webexternal.contoso.com/Schedul
```

The `WebScheduler` token references the URLs for client access to the web-based scheduling for Lync Server conferences. Currently, on the `External/WebScheduler` is used. The WebScheduler is installed as part of the deployment process of your internal Lync Server 2013 deployment web services.

```
<Link token="Internal/Mcx" href="https://webexternal.contoso.net/Mcx/McxService.s
```

```
<Link token="External/Mcx" href="https://webexternal.contoso.com/Mcx/McxService.s
```

`Internal/Mcx` and `External/Mcx` are the locations of the Mobility services, introduced in Cumulative Update for Lync Server 2010: November 2011. These references will continue to be used by Lync 2010 Mobile on all supported devices. The Mcx service is installed as part of the deployment process of your internal Lync Server 2013 deployment web services.

```
<Link token="Internal/Ucwa" href="https://webinternal.contoso.net/ucwa/v1/applica
```

```
<Link token="External/Ucwa" href="https://webexternal.contoso.com/ucwa/v1/applica
```

```
<Link token="Ucwa" href="https://webexternal.contoso.com/ucwa/v1/applications"/>
```

Internal/Ucwa, **External/Ucwa** and **Ucwa** provide a means for clients to access the Unified Communications Web Application Programming Interface (UCWA API, or simply UCWA). `Internal/Ucwa` and `External/Ucwa` virtual directories are access points reserved for future feature enhancement, and are not used. The `Ucwa` virtual directory is used for Microsoft Lync Mobile (introduced with Lync Server 2013) on all supported devices. The UCWA service is installed as part of the deployment process of your internal Lync Server 2013 deployment web services.

```
<Link token="Internal/XFrame" href="https://webinternal.contoso.net/Autodiscover/
```

```
<Link token="External/XFrame" href="https://webexternal.contoso.com/Autodiscover/
```

```
<Link token="XFrame" href="https://webexternal.contoso.com/Autodiscover/XFrame/XF
```

`Internal/XFrame`, **External/XFrame** and **XFrame** provide access for UCWA-based server applications. XFrame is installed as part of the deployment process of your internal Lync Server 2013 deployment web services.

```
<Link token="Self" href="https://webexternal.contoso.net/Autodiscover/Autodiscove
```

The `Self` token refers to information specific to the client (user response type) that is making the request. The client that made this request was external, and this Autodiscover reference is to the user portion of the Autodiscover service.

See Also

Other Resources

System Requirements for External User Access Components
Planning for Autodiscover

1.3.9.5 Choosing a Topology

Choosing a Topology

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2013-02-21*

When you choose a topology, you can use one the following supported topology options:

> **Note:**
> Unless otherwise noted, if you have experience with Microsoft Lync Server 2010, you will find the guidance here is largely unchanged.

- Single Consolidated Edge with Private IP Addresses and NAT
- Single Consolidated Edge with Public IP Addresses
- Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT
- Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses
- Scaled Consolidated Edge with Hardware Load Balancers

> **Important:**
> The internal Edge interface and external Edge interface must use the same type of load balancing. You cannot use DNS load balancing on one Edge interface and hardware load balancing on the other Edge interface.

The following table summarizes the functionality available with the supported Microsoft Lync Server 2013 topologies. The column headings indicate the functionality available for a given Edge configuration option. Using the Scaled Edge (DNS load balanced) option as an example, you can see that it supports high availability, can use non-routable private IP addresses (with NAT) or routable public IP addresses assigned to the Edge external interfaces, and reduces cost because a hardware load balancer is not required.

Edge failover scenarios supported with DNS Load Balancing are Lync-to-Lync point-to-point sessions, Lync conferencing sessions, Lync-to-PSTN sessions and Office 365. Edge failover scenarios that do not benefit from DNS Load Balancing are failover for remote user Exchange Unified Messaging (UM) (prior to Exchange 2010 SP1), public instant messaging (IM) connectivity, and federation with servers running Office Communications Server.

Summary of Edge Server Topology Options

Topology	High availability	Additional DNS A records required for external Edge Server in the Edge pool	Edge Failover for Lync-to-Lync sessions	Edge Failover for Lync-to-Lync EUM/PIC/OCS Federation sessions
Single Edge using NAT	No	No	No	No
Single Edge using Public IP	No	No	No	No
Scaled Edge (DNS Load Balanced) using NAT	Yes	Yes	Yes	*

Scaled Edge (DNS Load Balanced) using Public IP	Yes	Yes	Yes	*
Scaled Edge Hardware load balanced)	Yes	No (one DNS A record per VIP)	Yes	Yes

***** Failover for public instant messaging (IM) connectivity, and federation with servers running Office Communications Server is not available with DNS load balancing. Exchange UM (remote user) failover using DNS load balancing requires Exchange Server 2010 SP1 or newer.

> **Note:**
>
> Single Edge and Scaled Edge (DNS load balanced) topologies can use:
>
> - Routable public IP addresses
> - Non-routable private IP address if symmetric network address translation (NAT) is used
>
> > **Note:**
> >
> > If you use public IP address or private IP address with NAT, you will still use the same number of IP addresses based on your configuration choice in Topology Builder. You can configure the Edge Server to use a single IP address with distinct ports per service, or use distinct IP addresses per service, but use the same port (by default, TCP 443).
>
> If you decide to use non-routable private IP addresses with NAT:
>
> - You must use routable private IP addresses on all three external interfaces
> - You must configure symmetric NAT for incoming and outgoing traffic
>
> Scaled Edge (hardware load balanced) topology must use public IP addresses.

Lync Server 2013 supports placing Access, Web Conferencing, and A/V Edge external interfaces behind a router or firewall that performs network address translation (NAT) for both single and scaled consolidated Edge Server topologies.

Using NAT for all Edge external interfaces requires the use of DNS load balancing. When compared to using hardware load balancers, using DNS load balancing without NAT allows you to reduce the number of public IP address per Edge Server in an Edge pool as described in the following list:

- Lync Server 2013 Scaled Consolidated Edge (DNS load balanced) Requires three public IP addresses for each Edge Server in an Edge pool.
- Lync Server 2013 Scaled Consolidated Edge (hardware load balanced) Requires three public IP address for load balancer virtual IP addresses (one time requirement that does not increment as more Edge Servers are added to the pool) plus three public IP addresses per Edge Server in a pool.

IP Address Requirements for Scaled Consolidated Edge (IP Address per role)

Number of Edge Servers per pool	Number of required IP addresses Lync Server 2013 (DNS load balanced)	Number of required IP addresses Lync Server 2013 (hardware load balanced)
2	6	3 (1 per VIP) + 6
3	9	3 (1 per VIP) + 9
4	12	3 (1 per VIP) + 12

5	15	3 (1 per VIP) + 15

IP Address Requirements for Scaled Consolidated Edge (Single IP address for all roles)

Number of Edge Servers per pool	Number of required IP addresses Lync Server 2013 (DNS load balanced)	Number of required IP addresses Lync Server 2013 (hardware load balanced)
2	2	1 (1 per VIP) + 2
3	3	1 (1 per VIP) + 3
4	4	1 (1 per VIP) + 4
5	5	1 (1 per VIP) + 5

The primary decision points for topology selection are high availability and load balancing. The requirement for high availability can influence the load balancing decision.

- **High availability** If you need high availability, deploy at least two Edge Servers in a pool. A single Edge pool will support up to twelve Edge Servers. If more capacity is required, you can deploy multiple Edge pools. As a general rule, 10% of a given user base will need external access.

  Important:
  Topology Builder will allow you to configure up to twenty Edge Servers in a single Edge pool. The tested and supported maximum number of Edge Servers in a pool is twelve and Topology Builder allowing for a number larger than twelve should not be construed as implied support for more than twelve Edge Servers in a single Edge pool.

- **Hardware load balancing** Hardware load balancing is supported for load balancing Lync Server 2013 Edge Servers when using publicly routable IP addresses for the Edge external interfaces. For example, you would use this approach in situations where failover is required for any of the following applications:
  - Public IM connectivity
  - Federation with companies running Microsoft Office Communications Server 2007 or Microsoft Office Communications Server 2007 R2
  - External access to Exchange 2007 Unified Messaging (UM) or Exchange 2010 UM

    Important:
    DNS load balancing for Exchange 2010 SP1 and newer is supported for Exchange UM.

  These three applications will continue to operate, but they are not DNS load balancing aware and will only connect to the first Edge Server in the pool. If that server is unavailable, the connection will fail. For example, if multiple Edge Servers are deployed in a pool to handle the federated traffic load, only one access proxy actually receives traffic while the others are idle.

Important:
Using DNS load balancing is recommended if you are federating with companies using Lync Server 2010 and Microsoft Office 365. Be aware that there are significant performance impacts if most of your federated partners are using Office Communications Server 2007 or Office Communications Server 2007 R2.

1.3.9.6 Data Collection

Data Collection

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2012-09-08*

In Microsoft Lync Server 2013 communications software, you can run the Microsoft Lync Server 2013, Planning Tool without documenting your existing and proposed IP addresses and Edge Server fully qualified domain names (FQDNs), but it is significantly harder to do so without causing configuration errors. For example, if coexistence is required for a period of time, a common mistake is to reuse FQDNs from an existing Edge deployment for your Lync Server 2013 Edge deployment. By having the existing and proposed IP addresses and FQDNs written down in a spreadsheet, table, or other visual form, you help prevent setup problems during installation.

> ⚠**Warning:**
>
> If you have used previous versions of the Planning Tool, you may have used the tool to create your topology and the exported the topology document for use in Topology Builder to publish your topology. The ability to export the topology was removed from Planning Tool. Using a previous version of the Planning Tool to create a topology document for Lync Server 2013 is strongly discouraged, and will produce unexpected results.

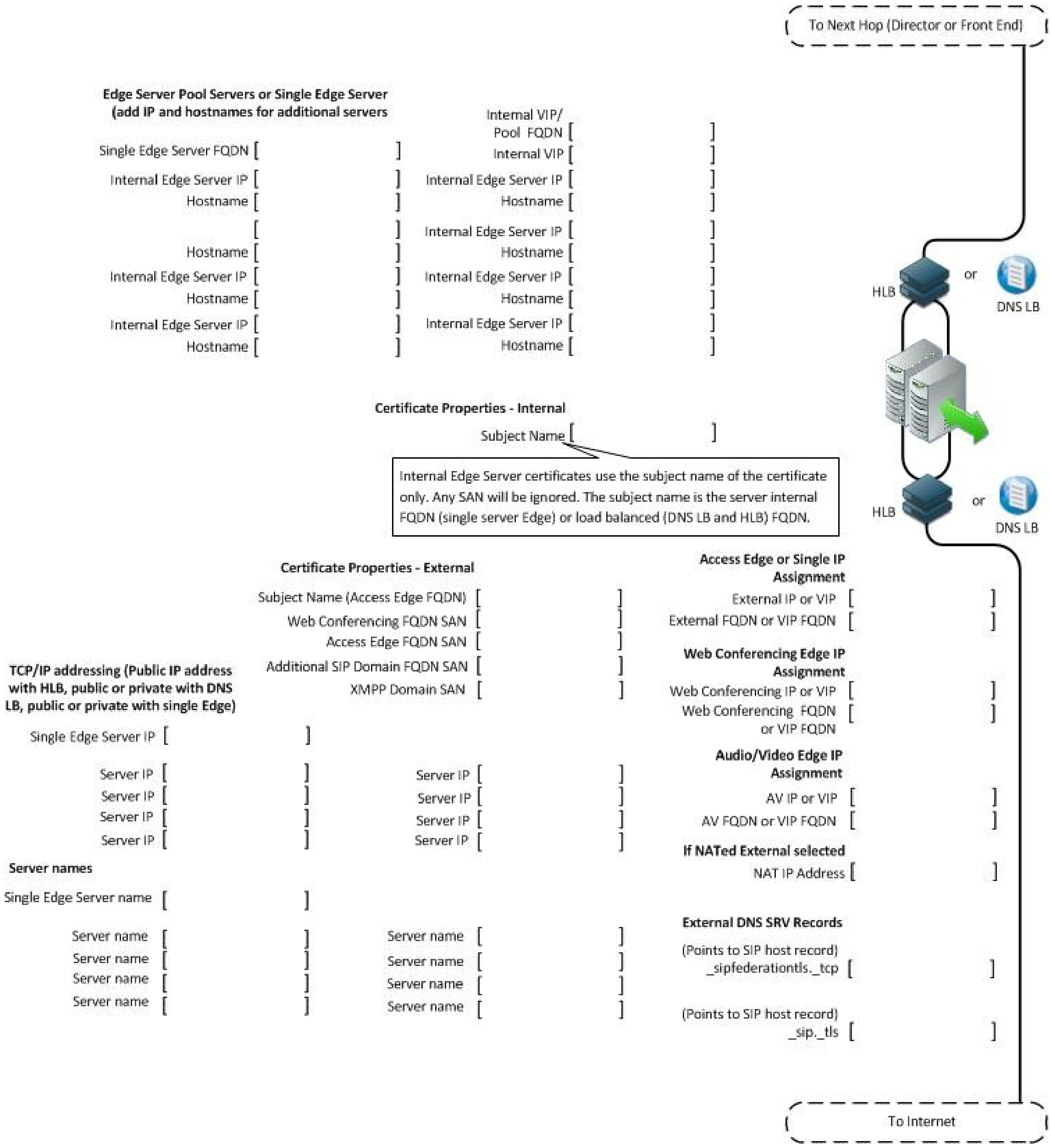
Therefore, the recommended approach is to use the following data collection template, which corresponds to your Edge topology, to gather the various FQDN and IP addresses that you will need to enter into the Planning Tool. By documenting the current and proposed configuration, you can put the values in the proper context for your production environment. And, you are forced to think about how you will configure coexistence and features such as simple URLs, file shares, and load balancing.

To successfully deploy Microsoft Lync Server 2013, you need to understand the interaction of and reliance on the individual components. By collecting data from your existing network and server infrastructure, and applying the planning guidance in these sections, you can integrate Lync Server 2013 Edge Server components into your infrastructure.

Introduced in Choosing a Topology, there are three main architectures with two variations, for a total of five possible deployment scenarios. One of these scenarios will be the starting point for your data collection. The IP addresses, server names, and domain names are examples that coincide with the matching certificate, firewall, and DNS diagrams that detail the information required for a complete planning solution. The diagrams and filling in your required certificate, DNS and firewall values is especially important in cross-team communications where the management of the certification authority, firewall configuration and DNS is managed by teams other than the team that plans the deployment. The diagrams provide information on required components that can be used to communicate these requirements for cross-team collaboration.

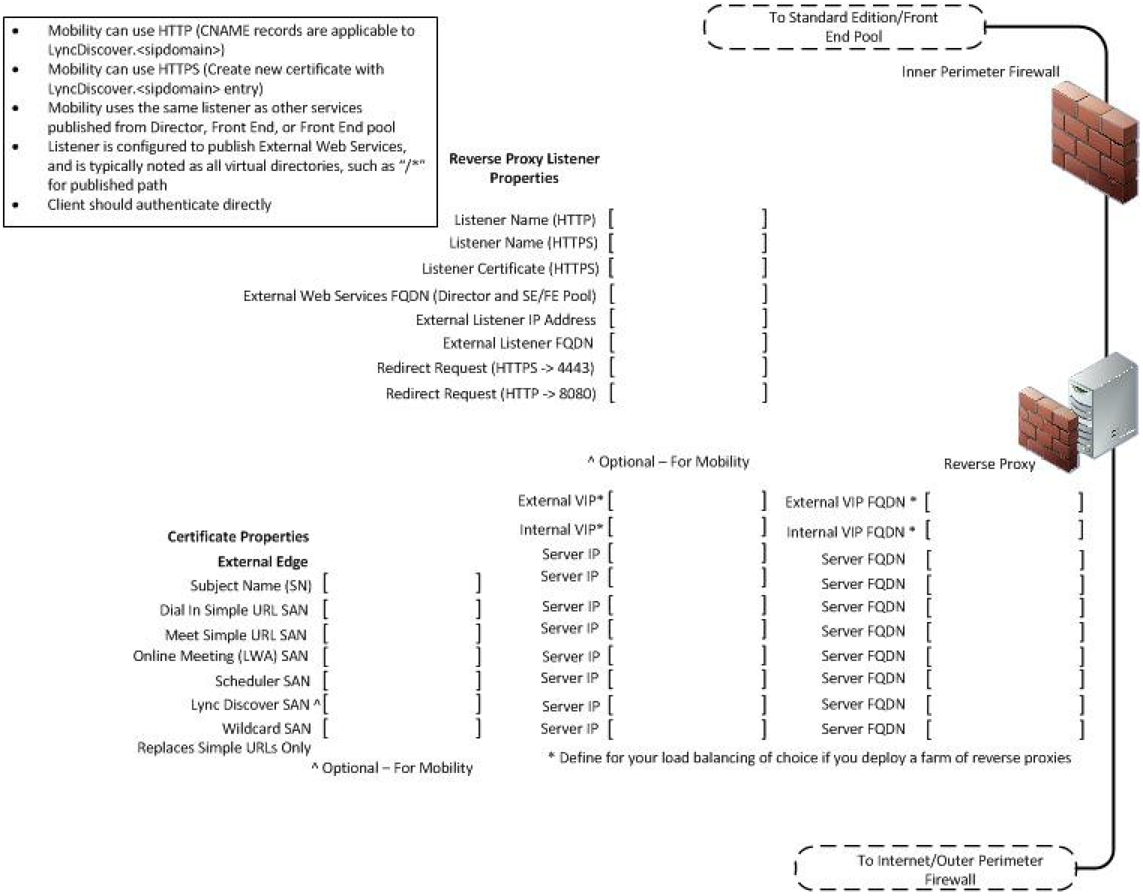
The provided diagrams are intentionally generic, but allow for the collection of all pertinent data that would be necessary for communication of requirements in a cross team scenario where networking, firewall, certificate creation and management, server deployment, and server management are handled by different groups. Having the required details for configuration of networking, firewalls, ports and protocols, certificates, and servers is invaluable when the deployment of Lync Server is underway.

Edge Server and Edge pool


To Next Hop (Director or Front End)
Edge Server Pool Servers or Single Edge Server (add IP and hostnames for additional servers
Single Edge Server FQDN [ ]
Internal Edge Server IP [ ]
Hostname [ ]
[ ]
Hostname [ ]
Internal Edge Server IP [ ]
Hostname [ ]
Internal Edge Server IP [ ]
Hostname [ ]
Internal VIP/ Pool FQDN [ ]
Internal VIP [ ]
Internal Edge Server IP [ ]
Hostname [ ]
Internal Edge Server IP [ ]
Hostname [ ]
Internal Edge Server IP [ ]
Hostname [ ]
Internal Edge Server IP [ ]
Hostname [ ]
HLB
or
DNS LB
Certificate Properties - Internal
Subject Name [ ]
HLB
or
DNS LB
Certificate Properties - External
Subject Name (Access Edge FQDN) [ ]
Web Conferencing FQDN SAN [ ]
Access Edge FQDN SAN [ ]
Additional SIP Domain FQDN SAN [ ]
XMPP Domain SAN [ ]
Access Edge or Single IP Assignment
External IP or VIP [ ]
External FQDN or VIP FQDN [ ]
Web Conferencing Edge IP Assignment
Web Conferencing IP or VIP [ ]
Web Conferencing FQDN or VIP FQDN [ ]
Audio/Video Edge IP Assignment
AV IP or VIP [ ]
AV FQDN or VIP FQDN [ ]
If NATed External selected
NAT IP Address [ ]
External DNS SRV Records
(Points to SIP host record) _sipfederationtls._tcp [ ]
(Points to SIP host record) _sip._tls [ ]
TCP/IP addressing (Public IP address with HLB, public or private with DNS LB, public or private with single Edge)
Single Edge Server IP [ ]
Server IP [ ]
Server IP [ ]
Server IP [ ]
Server IP [ ]
Server IP [ ]
Server IP [ ]
Server IP [ ]
Server IP [ ]
Server names
Single Edge Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
To Internet

Internal Edge Server certificates use the subject name of the certificate only. Any SAN will be ignored. The subject name is the server internal FQDN (single server Edge) or load balanced (DNS LB and HLB) FQDN.

Reverse Proxy



To Standard Edition/Front End Pool
Inner Perimeter Firewall
Reverse Proxy
To Internet/Outer Perimeter Firewall

- Mobility can use HTTP (CNAME records are applicable to LyncDiscover.<sipdomain>)
- Mobility can use HTTPS (Create new certificate with LyncDiscover.<sipdomain> entry)
- Mobility uses the same listener as other services published from Director, Front End, or Front End pool
- Listener is configured to publish External Web Services, and is typically noted as all virtual directories, such as "/*" for published path
- Client should authenticate directly

Reverse Proxy Listener Properties

Listener Name (HTTP) [ ]
Listener Name (HTTPS) [ ]
Listener Certificate (HTTPS) [ ]
External Web Services FQDN (Director and SE/FE Pool) [ ]
External Listener IP Address [ ]
External Listener FQDN [ ]
Redirect Request (HTTPS -> 4443) [ ]
Redirect Request (HTTP -> 8080) [ ]

^ Optional – For Mobility

External VIP* [ ] External VIP FQDN * [ ]
Internal VIP* [ ] Internal VIP FQDN * [ ]
Server IP [ ] Server FQDN [ ]
Server IP [ ] Server FQDN [ ]
Server IP [ ] Server FQDN [ ]
Server IP [ ] Server FQDN [ ]
Server IP [ ] Server FQDN [ ]
Server IP [ ] Server FQDN [ ]
Server IP [ ] Server FQDN [ ]
Server IP [ ] Server FQDN [ ]

* Define for your load balancing of choice if you deploy a farm of reverse proxies

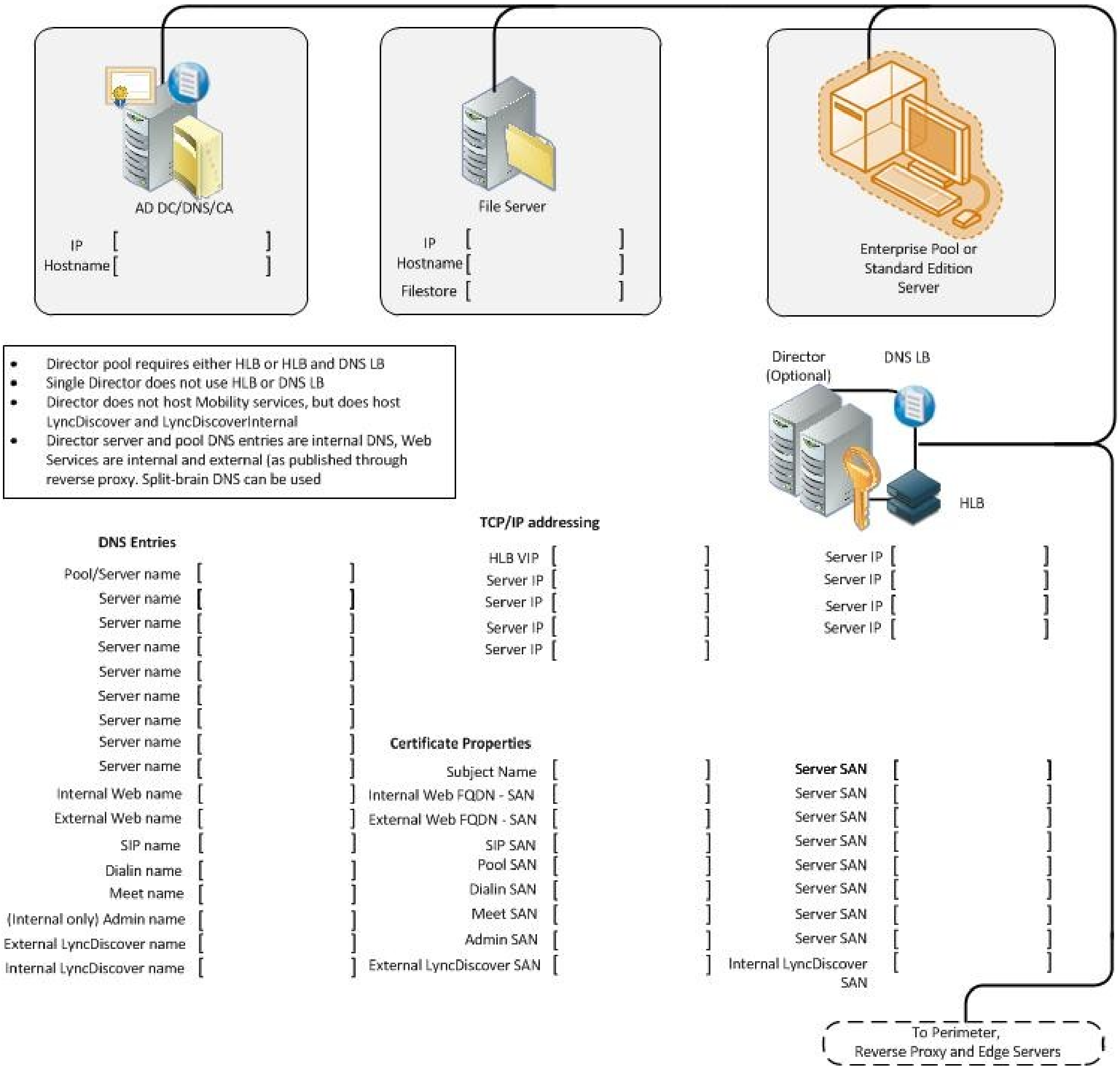
Certificate Properties

External Edge

Subject Name (SN) [ ]
Dial In Simple URL SAN [ ]
Meet Simple URL SAN [ ]
Online Meeting (LWA) SAN [ ]
Scheduler SAN [ ]
Lync Discover SAN ^[ ]
Wildcard SAN [ ]
Replaces Simple URLs Only

^ Optional – For Mobility

Director or Director pool



- Director pool requires either HLB or HLB and DNS LB
- Single Director does not use HLB or DNS LB
- Director does not host Mobility services, but does host LyncDiscover and LyncDiscoverInternal
- Director server and pool DNS entries are internal DNS, Web Services are internal and external (as published through reverse proxy. Split-brain DNS can be used

DNS Entries

Pool/Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Server name [ ]
Internal Web name [ ]
External Web name [ ]
SIP name [ ]
Dialin name [ ]
Meet name [ ]
(Internal only) Admin name [ ]
External LyncDiscover name [ ]
Internal LyncDiscover name [ ]

TCP/IP addressing

HLB VIP [ ]
Server IP [ ]
Server IP [ ]
Server IP [ ]
Server IP [ ]

Server IP [ ]
Server IP [ ]
Server IP [ ]
Server IP [ ]

Certificate Properties

Subject Name [ ]
Internal Web FQDN - SAN [ ]
External Web FQDN - SAN [ ]
SIP SAN [ ]
Pool SAN [ ]
Dialin SAN [ ]
Meet SAN [ ]
Admin SAN [ ]
External LyncDiscover SAN [ ]

Server SAN [ ]
Server SAN [ ]
Server SAN [ ]
Server SAN [ ]
Server SAN [ ]
Server SAN [ ]
Server SAN [ ]
Server SAN [ ]
Internal LyncDiscover SAN [ ]

1.3.9.7 Determine DNS Requirements

Determine DNS Requirements

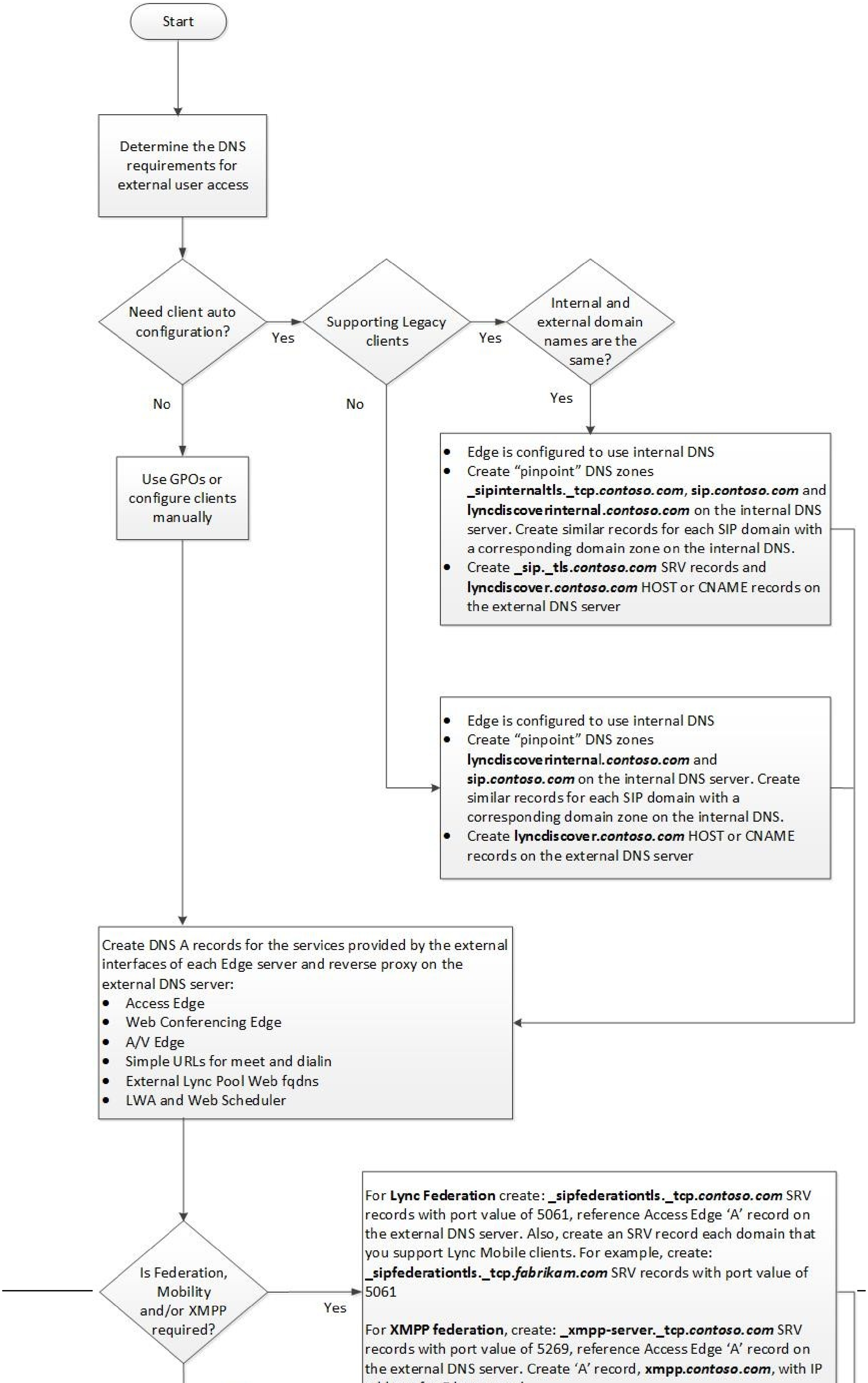
Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2013-02-22*

Use the following flow chart to determine Domain Name System (DNS) requirements. Changes for the Cumulative Updates for Lync Server 2013: February 2013 are noted where they apply.

Important:

Microsoft Lync Server 2013 supports the use of IPv6 addressing. To use IPv6 addresses, you must also provide support for IPv6 DNS and configure DNS host AAAA (known as “quad-A”) records. In deployments where both IPv4 and IPv6 are being used, it is best to configure and maintain both host A records for IPv4 and host AAAA for IPv6. Even if your deployment has transitioned fully to IPv6, IPv4 DNS host records may still be required when external users are still using IPv4.


Start
Determine the DNS requirements for external user access
Need client auto configuration?
Yes
No
Supporting Legacy clients
Yes
No
Internal and external domain names are the same?
Yes
Use GPOs or configure clients manually
Is Federation, Mobility and/or XMPP required?
Yes

- Edge is configured to use internal DNS
- Create "pinpoint" DNS zones **_sipinternaltls._tcp.contoso.com**, **sip.contoso.com** and **lyncdiscoverinternal.contoso.com** on the internal DNS server. Create similar records for each SIP domain with a corresponding domain zone on the internal DNS.
- Create **_sip._tls.contoso.com** SRV records and **lyncdiscover.contoso.com** HOST or CNAME records on the external DNS server

- Edge is configured to use internal DNS
- Create "pinpoint" DNS zones **lyncdiscoverinternal.contoso.com** and **sip.contoso.com** on the internal DNS server. Create similar records for each SIP domain with a corresponding domain zone on the internal DNS.
- Create **lyncdiscover.contoso.com** HOST or CNAME records on the external DNS server

Create DNS A records for the services provided by the external interfaces of each Edge server and reverse proxy on the external DNS server:

- Access Edge
- Web Conferencing Edge
- A/V Edge
- Simple URLs for meet and dialin
- External Lync Pool Web fqdns
- LWA and Web Scheduler

For **Lync Federation** create: **_sipfederationtls._tcp.contoso.com** SRV records with port value of 5061, reference Access Edge 'A' record on the external DNS server. Also, create an SRV record each domain that you support Lync Mobile clients. For example, create: **_sipfederationtls._tcp.fabrikam.com** SRV records with port value of 5061

For **XMPP federation**, create: **_xmpp-server._tcp.contoso.com** SRV records with port value of 5269, reference Access Edge 'A' record on the external DNS server. Create 'A' record, **xmpp.contoso.com**, with IP

Important:

By default the computer name of a computer that is not joined to a domain is a host name, not a fully qualified domain name (FQDN). Topology Builder uses FQDNs, not host names. So, you must configure a DNS suffix on the name of the computer to be deployed as an Edge Server that is not joined to a domain. **Use only standard characters** (including A–Z, a–z, 0–9, and hyphens) when assigning FQDNs of your Lync Servers, Edge Servers, and pools. Do not use Unicode characters or underscores. Nonstandard characters in an FQDN are often not supported by external DNS and public CAs (that is, when the FQDN must be assigned to the SN in the certificate). For additional details, see Configure DNS Host Records

How Lync Clients Locate Services

Microsoft Lync 2010, Lync 2013, and Lync Mobile are similar in how the client finds and accesses services in Lync Server 2013. The notable exception is the Lync Windows Store app that uses a different service location process. This section details two scenarios of how the clients locate services, first the traditional method using a series of SRV and A host records, second using only the Autodiscover service records. Cumulative updates to the desktop clients change the DNS location process from Lync Server 2010 For all clients, the DNS query process continues until a successful query is returned, or the list of possible DNS records is exhausted, and the final error is returned to the client.

For all clients **except** for the Lync Windows Store app During DNS lookup, SRV records are queried and returned to the client in the following order:

1. lyncdiscoverinternal.<*domain*>   A (host) record for the Autodiscover service on the internal Web services
2. lyncdiscover.<*domain*>   A (host) record for the Autodiscover service on the external Web services
3. _sipinternaltls._tcp.<*domain*>   SRV (service locator) record for internal TLS connections
4. _sipinternal._tcp.<*domain*>   SRV (service locator) record for internal TCP connections (performed only if TCP is allowed)
5. _sip._tls.<*domain*>   SRV (service locator) record for external TLS connections
6. sipinternal.<*domain*>   A (host) record for the Front End pool or Director, resolvable only on the internal network
7. sip.<*domain*>   A (host) record for the Front End pool or Director on the internal network, or the Access Edge service when the client is external
8. sipexternal.<*domain*>   A (host) record for the Access Edge service when the client is external

The Lync Windows Store app changes the process completely because it uses two records:

1. lyncdiscoverinternal.<*domain*>   A (host) record for the Autodiscover service on the internal Web services
2. lyncdiscover.<*domain*>   A (host) record for the Autodiscover service on the external Web services

There is no fallback to the other record types.

The difference between the methods used for newer clients as compared to older clients is that the Autodiscover service is becoming the preferred method to locate all services.

When a connection is successful, the Autodiscover Service returns all the Web Services URLs for the user's home pool, including the Mobility Service (known as Mcx by the virtual directory created for the service in IIS), Microsoft Lync Web App and Web scheduler URLs. However, both the internal Mobility Service URL and the external Mobility Service URL is associated with the external Web Services FQDN. Therefore, regardless of whether a mobile device is internal or external to the network, the device always connects to the Mobility Service externally through the reverse proxy.

If the Cumulative Updates for Lync Server 2013: February 2013 has been installed, the Autodiscover Service also returns references to Internal/UCWA, External/UCWA and UCWA. These entries refer to the Unified Communications Web API (UCWA) web component. Currently, only the entry UCWA is used and provides a reference to a URL for the web component. UCWA is used by Lync 2013 Mobile clients instead of the Mcx Mobility Service used by the Lync 2010 Mobile clients.

Note:

When creating SRV records, it is important to remember that they must point to a DNS A and AAAA (if you are using IPv6 addressing) record in the same domain in which the DNS SRV record is created. For example, if the SRV record is in contoso.com, the A and AAAA (if you are using IPv6 addressing) record it points to cannot be in fabrikam.com.

Tip:

The default configuration is to direct all mobile client traffic through the external site. You can modify settings to return only the internal URL, if this is more preferable for your requirements. With this configuration, users can use Lync mobile applications on their mobile devices only when they are inside the corporate network. To define this configuration, you use the **Set-CsMcxConfiguration** cmdlet.

Note:

Although mobile applications can also connect to other Lync Server 2013 services, such as Address Book Service, internal mobile application web requests go to the external web FQDN only for the Mobility Service. Other service requests, such as Address Book requests, do not require this configuration.

Mobile devices support manual discovery of services. In this case, each user must configure the mobile device settings with the full internal and external Autodiscover Service URIs, including the protocol and path, as follows:

- https://<*ExtPoolFQDN*>/Autodiscover/autodiscoverservice.svc/Root for external access
- https://<*IntPoolFQDN*>/AutoDiscover/AutoDiscover.svc/Root for internal access

We recommend that you use automatic discovery, rather than manual discovery. However, manual settings can be useful for troubleshooting mobile device connectivity issues.

Configuring Split-Brain DNS with Lync Server

Split-brain DNS is known by a number of names, for example, split DNS or split-horizon DNS. Simply, it describes a DNS configuration where there are two DNS zones with the same namespace – but one DNS zone services internal-only requests, and the other DNS zone services external-only requests. However, many of the DNS SRV and A records contained in the internal DNS will not be contained in the external DNS, and the reverse is also true. In cases where the same DNS record exists in both the internal and external DNS (for example, www.contoso.com), the IP address returned will be different based on where (internal or external) the query was initiated.

Important:

Currently, Split-Brain DNS is not supported for the mobility, or more specifically, the LyncDiscover and LyncDiscoverInternal DNS records. LyncDiscover must be defined on an external DNS server and LyncDiscoverInternal must be defined on an internal DNS server.

For the purposes of these topics, the term split-brain DNS will be used.

If you are configuring split-brain DNS, the following internal and external zone contain a summary of the types of DNS records required in each zone. For details, see Scenarios for External User Access.

Internal DNS:

- Contains a DNS zone called contoso.com for which it is authoritative
- The internal contoso.com zone contains:
  - DNS A and AAAA (if you are using IPv6 addressing) and SRV records for internal Lync Server 2013 client autoconfiguration (optional)
  - DNS A and AAAA (if you are using IPv6 addressing) or CNAME records for automatic discovery of Lync Server 2013 Web Services (optional)
  - DNS A and AAAA (if you are using IPv6 addressing) records for Front End pool name, Director or Director pool name, and all internal servers running Lync Server 2013 in the corporate network
  - DNS A and AAAA (if you are using IPv6 addressing) records for the Edge internal interface of each Lync Server 2013, Edge Server in the perimeter network
  - DNS A and AAAA (if you are using IPv6 addressing) records for the internal interface of each reverse proxy server in the perimeter network (optional for management of reverse proxy)
  - All Lync Server 2013 Edge Server internal edge interfaces in the perimeter network use the internal DNS zone for resolving queries to contoso.com
  - All servers running Lync Server 2013 and clients running Lync 2013 in the corporate network point to the internal DNS servers for resolving queries to contoso.com, or use of HOSTS file on each Edge server and list A and AAAA (if you are using IPv6 addressing) records for next hop server, specifically the Director or Director VIP, Front End pool VIP, or Standard Edition server

External DNS:

- Contains a DNS zone called contoso.com for which it is authoritative
- The external contoso.com zone contains:
  - DNS A and AAAA (if you are using IPv6 addressing) and SRV records for Lync Server 2013 client autoconfiguration (optional)
  - DNS A and AAAA (if you are using IPv6 addressing) or CNAME records for automatic discovery of Lync Server 2013 Web Services for use with mobility
  - DNS A and AAAA (if you are using IPv6 addressing) and SRV records for the Edge external interface of each Lync Server 2013, Edge Server or hardware load balancer virtual IP (VIP) in the perimeter network
  - DNS A and AAAA (if you are using IPv6 addressing) records for the external interface of the reverse proxy server or VIP for a pool of reverse proxy servers in the perimeter network

Automatic Configuration without Split-Brain DNS

Using split-brain DNS, a Lync Server 2013 user that signs in internally can take advantage of automatic configuration if the internal DNS zone contains a _sipinternaltls._tcp SRV record for each SIP domain in use. However, if you do not use split-brain DNS, internal automatic configuration of clients running Lync will not work unless one of the workarounds described in later in this section is implemented. This is because Lync Server 2013 requires the user's SIP URI to match the domain of the Front End pool designated for automatic configuration. This was also the case with earlier versions of Communicator.

For example, if you have two SIP domains in use, the following DNS service (SRV) records would be required:

- If a user signs in as bob@contoso.com the following SRV record will work for automatic configuration because the user's SIP domain (contoso.com) matches the domain of automatic configuration Front End pool):

_sipinternaltls._tcp.contoso.com. 86400 IN SRV 0 0 5061 pool01.contoso.com

- If a user signs in as alice@fabrikam.com the following DNS SRV record will work for automatic configuration of the second SIP domain.
  _sipinternaltls._tcp.fabrikam.com. 86400 IN SRV 0 0 5061 pool01.fabrikam.com

For comparison, if a user signs in as tim@litwareinc.com the following DNS SRV record will not work for automatic configuration, because the client's SIP domain (litwareinc.com) does not match the domain that the pool is in (fabrikam.com):

_sipinternaltls._tcp.litwareinc.com. 86400 IN SRV 0 0 5061 pool01.fabrikam.com

If automatic configuration is required for clients running Lync, select one of the following options:

- **Group Policy Objects** Use Group Policy objects (GPOs) to populate the correct server values.

  Note:
  This option does not enable automatic configuration, but it does automate the process of manual configuration, so if this approach is used, the SRV records associated with automatic configuration are not required.

- **Matching internal zone** Create a zone in the internal DNS that matches the external DNS zone (for example, contoso.com) and create DNS A and AAAA (if you are using IPv6 addressing) records corresponding to the Lync Server 2013 pool used for automatic configuration. For example, if a user is homed on pool01.contoso.net but signs into Lync as bob@contoso.com, create an internal DNS zone called contoso.com and inside it, create a DNS A and AAAA (if IPv6 addressing is used) record for pool01.contoso.com.
- **Pin-point internal zone** If you are creating an entire zone in the internal DNS is not an option, you can create pin-point (that is, dedicated) zones that correspond to the SRV records that are required for automatic configuration, and populate those zones using dnscmd.exe. Dnscmd.exe is required because the DNS user interface does not support creation of pin-point zones. For example, if the SIP domain is contoso.com and you have a Front End pool called pool01 that contains two Front End Servers, you need the following pin-point zones and A records in your internal DNS:

```
dnscmd . /zoneadd _sipinternaltls._tcp.contoso.com. /dsprimary
dnscmd . /recordadd _sipinternaltls._tcp.contoso.com. @ SRV 0 0 5061 po
dnscmd . /zoneadd pool01.contoso.com. /dsprimary
dnscmd . /recordadd pool01.contoso.com. @ A 192.168.10.90
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
dnscmd . /recordadd pool01.contoso.com. @ A 192.168.10.91
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
```

  If your environment contains a second SIP domain (for example, fabrikam.com), you need the following pin-point zones and A records in your internal DNS:

```
dnscmd . /zoneadd _sipinternaltls._tcp.fabrikam.com. /dsprimary
dnscmd . /recordadd _sipinternaltls._tcp.fabrikam.com. @ SRV 0 0 5061 p
dnscmd . /zoneadd pool01.fabrikam.com. /dsprimary
dnscmd . /recordadd pool01.fabrikam.com. @ A 192.168.10.90
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
dnscmd . /recordadd pool01.fabrikam.com. @ A 192.168.10.91
dnscmd . /recordadd pool01.contoso.com. @ AAAA <IPv6 address>
```

Note:
The Front End pool FQDN appears twice, but with two different IP addresses. This is because DNS load balancing is used, but if hardware load balancing is used, there would be only a single Front End pool entry. Also, the Front End pool FQDN values change between the contoso.com example and the fabrikam.com example, but the IP addresses remain the same. This is because users signing in from either SIP domain, use the same Front End pool for automatic configuration.

For details, see the DMTF blog article, "Communicator Automatic Configuration and Split-Brain DNS," at http://go.microsoft.com/fwlink/p/?linkId=200707.

Note:
The content of each blog and its URL are subject to change without notice.

Configuring the domain name system (DNS) for Disaster Recovery

To configure DNS to redirect Lync Server 2013 Web traffic to your disaster recovery and failover sites, you must be using a DNS provider that supports GeoDNS. You can set up your DNS records for Web to support disaster recovery, so that features that use Web services continue even if one entire Front End pool goes down. This disaster recovery feature supports the Autodiscover (Lyncdiscover URL), Meet and Dial-In simple URLs.

You define and configure additional DNS host (A and AAAA if using IPv6) records for internal and external resolution of Web services at your GeoDNS provider. The following details assume paired pools, geographically dispersed, and GeoDNS supported by your provider with either round-robin DNS, or configured to use Pool1 as primary, and fail over to Pool2 in the event of communications loss or hardware failure.

GeoDNS record (example)	Pool records (example)	CNAME records (example)	DNS settings (select one option)
Meet-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Meet.contoso.com alias to Pool1InternalWebFQDN.contoso.com Meet.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Meet-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Meet.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Meet.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Dialin-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Dialin.contoso.com alias to Pool1InternalWebFQDN.contoso.com Dialin.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Dialin-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Dialin.contoso.com alias to Pool1ExternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure

		Dialin.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	
Lyncdiscoverint-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Lyncdiscoverinternal.contoso.com alias to Pool1InternalWebFQDN.contoso.com Lyncdiscoverinternal.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Lyncdiscover-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Lyncdiscover.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Lyncdiscover.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Scheduler-int.geolb.contoso.com	Pool1InternalWebFQDN.contoso.com Pool2InternalWebFQDN.contoso.com	Scheduler.contoso.com alias to Pool1InternalWebFQDN.contoso.com Scheduler.contoso.com alias to Pool2InternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure
Scheduler-ext.geolb.contoso.com	Pool1ExternalWebFQDN.contoso.com Pool2ExternalWebFQDN.contoso.com	Scheduler.contoso.com alias to Pool1ExternalWebFQDN.contoso.com Scheduler.contoso.com alias to Pool2ExternalWebFQDN.contoso.com	Round Robin between pools Use primary, connect to secondary if failure

DNS Load Balancing

DNS load balancing is typically implemented at the application level. The application (for example, a client running Lync), tries to connect to a server in a pool by connecting to one of the IP addresses returned from the DNS A and AAAA (if IPv6 addressing is used) record query for the pool fully qualified domain name (FQDN).

For example, if there are three front end servers in a pool named pool01.contoso.com, the following will happen:

- Clients running Lync query DNS for pool01.contoso.com. The query returns three IP addresses and caches them as follows (not necessarily in this order):
  pool01.contoso.com   192.168.10.90
  pool01.contoso.com   192.168.10.91

pool01.contoso.com 192.168.10.92

- The client attempts to establish a Transmission Control Protocol (TCP) connection to one of the IP addresses. If that fails, the client tries the next IP address in the cache.
- If the TCP connection succeeds, the client negotiates TLS to connect to the primary registrar on pool01.contoso.com.
- If the client tries all cached entries without a successful connection, the user is notified that no servers running Lync Server 2013 are available at the moment.

Note:

DNS-based load balancing is different from DNS round robin (DNS RR) which typically refers to load balancing by relying on DNS to provide a different order of IP addresses corresponding to the servers in a pool. Typically DNS RR only enables load distribution, but does not enable failover. For example, if the connection to the one IP address returned by the DNS A and AAAA (if you are using IPv6 addressing) query fails, the connection fails. Therefore, DNS round robin by itself is less reliable than DNS-based load balancing. You can use DNS round robin in conjunction with DNS load balancing.

DNS load balancing is used for the following:

- Load balancing server-to-server SIP to the Edge Servers
- Load balancing Unified Communications Application Services (UCAS) applications such as Conferencing Auto Attendant, Response Group, and Call Park
- Preventing new connections to UCAS applications (also known as "draining")
- Load balancing all client-to-server traffic between clients and Edge Servers

DNS load balancing cannot be used for the following:

- Client-to-server web traffic to Director or Front End Servers

DNS load balancing and federated traffic:

If multiple DNS records are returned by a DNS SRV query, the Access Edge service always picks the DNS SRV record with the lowest numeric priority and highest numeric weight. The Internet Engineering Task Force document "A DNS RR for specifying the location of services (DNS SRV)" http://www.ietf.org/rfc/rfc2782.txt specifies that if there are multiple DNS SRV records defined, priority is first used, then weight. For example DNS SRV record A has a weight of 20 and a priority of 40 and DNS SRV record B has a weight of 10 and priority of 50. DNS SRV record A with priority 40 will be selected. The following rules apply to DNS SRV record selection:

- Priority is considered first. A client MUST attempt to contact the target host defined by the DNS SRV record with the lowest numbered priority it can reach. Targets with the same priority SHOULD be tried in an order defined by the weight field.
- The weight field specifies a relative weight for entries with the same priority. Larger weights SHOULD be given a proportionately higher probability of being selected. DNS administrators SHOULD use Weight 0 when there isn't any server selection to do. In the presence of records containing weights greater than 0, records with weight 0 should have a very small chance of being selected.

If multiple DNS SRV records with equal priority and weight are returned, the Access Edge service will select the SRV record that was received first from the DNS server.

1.3.9.8 Determine External A/V Firewall and Port Requirements

Determine External A/V Firewall and Port Requirements

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2012-10-29*

Audio/Video (A/V) communication can be a complex. Because of the nature of protocols used in A/V and how clients and servers use the protocols, a special section is warranted to explain the differences between client and server versions.

Use the following A/V Firewall and Port table to determine firewall requirements and which ports to open. Then, review the network address translation (NAT) terminology because NAT can be implemented in many different ways. For a detailed example of firewall port settings, see the reference architectures in Scenarios for External User Access.

General Protocol Usage for UDP and TCP in Audio/Video and Media Traffic

Audio/Video Transport	Usage
UDP	Preferred transport layer protocol for audio and video
TCP	Fallback transport layer protocol for audio and video Required transport layer protocol for application sharing to Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013 Required transport layer protocol for file transfer to Lync Server 2010 and Lync Server 2013

External A/V Firewall Port Requirements for External User Access

The firewall port requirements for external (and internal) SIP and conferencing interfaces are consistent, regardless of the version of your client or the version of the federation partner.

The same is not true for the Audio/Video Edge external interface. For federation with Office Communications Server 2007, the A/V Edge service requires that external firewall rules allow RTP/TCP and RTP/UDP traffic in the 50,000 through 59,999 port range to flow in both directions. The previous table assumes that Lync Server 2013 is the primary federation partner and it is being configured to communicate with one of the other federation partner types listed.

Configuring the Audio/Video port range of 50,000-59,999 must take into account that the port range will contain the source ports for communications to federation partners. In detail, consider that a communication is initiated from a federation partner. The communication from the A/V Edge service ports in the 50,000-59,999 range will connect to the expected port TCP 443 of the partner’s A/V Edge service. Conversely, inbound traffic to your A/V Edge service port TCP 443 will have a source port in the range of 50,000-59,999.

Different firewalls and policies for firewall administration may require only destination rules to be configured, or they may require both source and destination to be configured. If your requirements are for destination ports only, the Audio/Video requirements are:

Source IP	Destination IP	Destination Port
A/V Edge service interface	Any	TCP 443
A/V Edge service interface	Any	UDP 3478
Any	A/V Edge service interface	TCP 443
Any	A/V Edge service interface	UDP 3478

If your policies require both inbound and outbound firewall rule definitions, the Audio/ Video requirements are:

Source IP	Destination IP	Source Port	Destination Port
A/V Edge service interface	Any	TCP 50,000-59,999	TCP 443
A/V Edge service interface	Any	UDP 3478	UDP 3478
Any	A/V Edge service interface	Any	TCP 443
Any	A/V Edge service interface	Any	UDP 3478

Important:

Microsoft Office Communications Server 2007 requires a slightly different configuration. The TCP and UDP port range of 50,000-59,999 must be open inbound and outbound. This requirement is only for Office Communicator 2007. Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013 only require TCP range 50,000-59,999 open outbound.

NAT Requirements for External User Access

NAT has typically been a routing function, but newer devices such as firewalls and even hardware load balancers can be configured for NAT. Rather than focusing on which device is performing NAT, this topic describes the required NAT behavior instead.

Lync Server 2013 communications software does not support NAT for traffic to or from the Edge internal interface, but for the Edge external interface, the following NAT behavior is required.

Important:

You must configure symmetric NAT for incoming and outgoing traffic. Symmetric NAT is the NAT technology described in this topic.

This documentation uses the acronyms ChangeDST and ChangeSRC in tables and drawings to define the following required behavior:

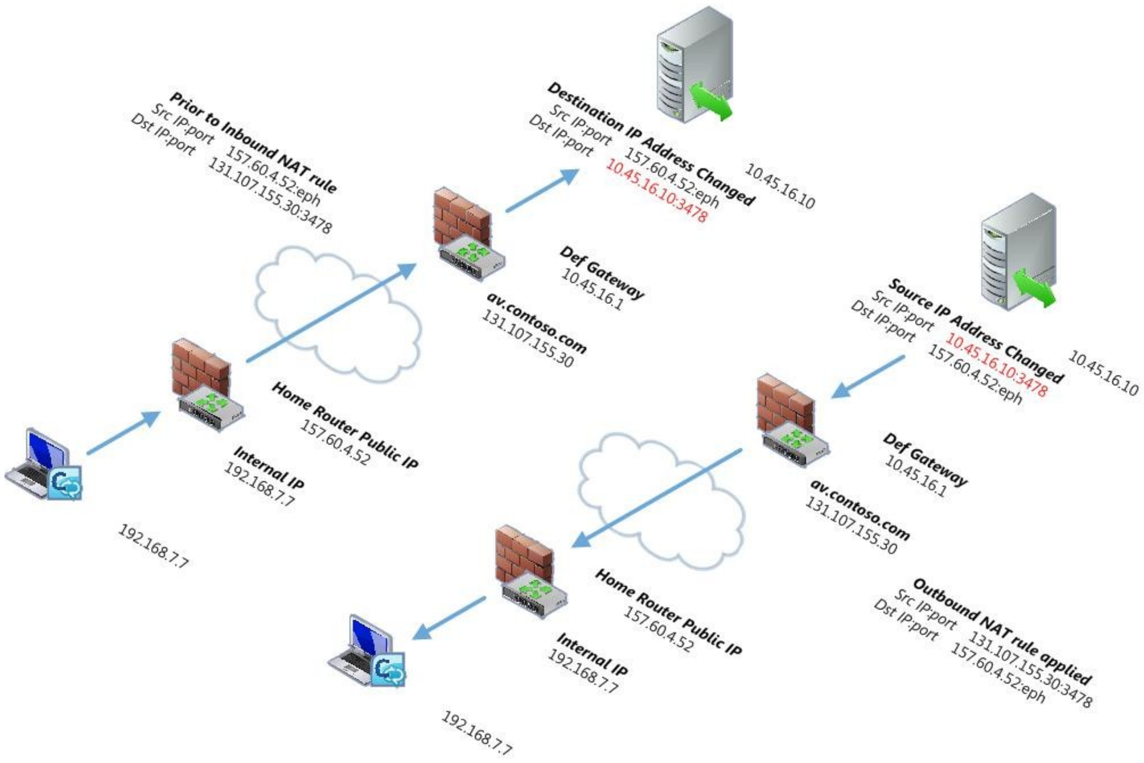
- **ChangeDST** The process of changing the destination IP address on packets destined for the network that is using NAT. This is also known as transparency, port forwarding, destination NAT mode, or half-NAT mode.
- **ChangeSRC** the process of changing the source IP address on packets leaving the network that is using NAT. This is also known as proxy, secure

NAT, stateful NAT, source NAT or full-NAT mode.

Regardless of the naming convention used, the NAT behavior required for the external interface of the Edge Server is as follows:

- For traffic from the Internet to the Edge external interface:
  - Change the destination IP address of the incoming packet from the Edge external interface public IP address to the translated IP address of the Edge external interface.
  - Leave the source IP address intact so that there is a return route for the traffic.
- For traffic from the Edge external interface to the Internet:
  - Change the source IP address of the packet leaving the Edge external interface, from the translated IP address to the public IP address of the Edge external interface so that the internal Edge IP address is not exposed and because it is a non-routable IP address.
  - Leave the destination IP address intact on the outgoing packets.

The following figure shows the distinction between changing the destination IP address (ChangeDST) for inbound traffic and changing the source IP Address (ChangeSRC) for outbound traffic using the A/V edge as an example.


Prior to Inbound NAT rule
Src IP:port 157.60.4.52:eph
Dst IP:port 131.107.155.30:3478
Destination IP Address Changed
Src IP:port 157.60.4.52:eph
Dst IP:port 10.45.16.10:3478
10.45.16.10
Def Gateway
10.45.16.1
av.contoso.com
131.107.155.30
Home Router Public IP
157.60.4.52
Internal IP
192.168.7.7
192.168.7.7
Source IP Address Changed
Src IP:port 10.45.16.10:3478
Dst IP:port 157.60.4.52:eph
10.45.16.10
Def Gateway
10.45.16.1
av.contoso.com
131.107.155.30
Home Router Public IP
157.60.4.52
Internal IP
192.168.7.7
Outbound NAT rule applied
Src IP:port 131.107.155.30:3478
Dst IP:port 157.60.4.52:eph
192.168.7.7

The key points are:

- Traffic that is inbound to the server running the A/V Edge service, the source IP address does not change but the destination IP address changes from 131.107.155.30 to the translated IP address of 10.45.16.10.
- Traffic that is outbound from the server running the A/V Edge service back to the workstation, the source IP address changes from the server's public IP address to the public IP address of the server running the A/V Edge service. The destination IP remains the workstation's public IP address. After the packet leaves the first NAT device outbound, the rule on the NAT device changes the source IP address of the server running the A/V Edge service

external interface IP address (10.45.16.10) to its public IP address (131.107.155.30).

1.3.9.9 Plan for Edge Server Certificates

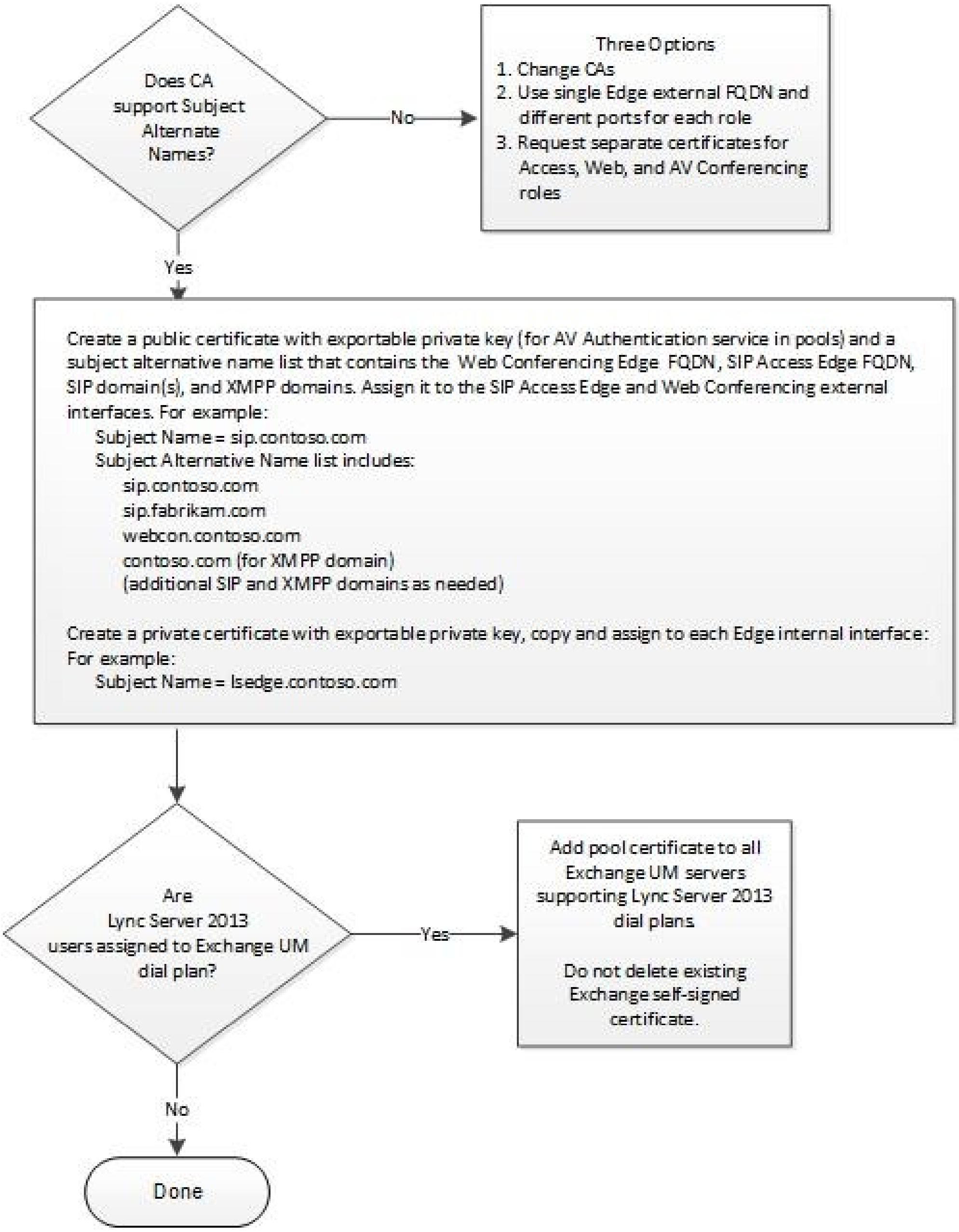
Plan for Edge Server Certificates

See Also

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2012-11-05*

Certificate creation for Edge is simplified in Lync Server 2013.


Does CA support Subject Alternate Names?
No
Three Options
1. Change CAs
2. Use single Edge external FQDN and different ports for each role
3. Request separate certificates for Access, Web, and AV Conferencing roles
Yes
Create a public certificate with exportable private key (for AV Authentication service in pools) and a subject alternative name list that contains the Web Conferencing Edge FQDN, SIP Access Edge FQDN, SIP domain(s), and XMPP domains. Assign it to the SIP Access Edge and Web Conferencing external interfaces. For example:
Subject Name = sip.contoso.com
Subject Alternative Name list includes:
sip.contoso.com
sip.fabrikam.com
webcon.contoso.com
contoso.com (for XMPP domain)
(additional SIP and XMPP domains as needed)
Create a private certificate with exportable private key, copy and assign to each Edge internal interface:
For example:
Subject Name = lsedge.contoso.com
Are Lync Server 2013 users assigned to Exchange UM dial plan?
Yes
Add pool certificate to all Exchange UM servers supporting Lync Server 2013 dial plans
Do not delete existing Exchange self-signed certificate.
No
Done

Create a single public certificate, ensure that you have an exportable private key defined for the certificate, and assign it to the following Edge Server external interfaces using the certificate wizard:

Important:

Wildcard certificates are not supported in Lync Server, except where used to summarize the Simple URLs through the reverse proxy. You must define distinct subject alternate names (SANs) for each SIP domain name, Web Conferencing Edge service, A/V Edge service and XMPP domain offered by your deployment.

Note:

Introduced in Lync Server 2013, staging Audio/Video Authentication certificates in advance of the expiration time of the current certificate requires some additional planning. Instead of one certificate with multiple purposes for the external Edge interface, you will require two certificates, one assigned to the Access Edge service and Web Conferencing Edge service, and one certificate for the A/V Edge service. For additional details, see Staging AV and OAuth Certificates Using -Roll in Set-CsCertificate

Important:

In the event of a pool of Edge Servers, you export the certificate with the private key to each Edge Server and assign the certificate to each Edge Server service. Do the same for the internal Edge Server certificate, exporting the certificate with the private key and assigning to each internal Edge interface.

- Ensure that you have an exportable private key assigned for the certificate
- Access Edge service (referred to as **SIP Access Edge External** in the certificate wizard)
- Web Conferencing Edge service (referred to as **Web Conferencing Edge External** in the certificate wizard)
- A/V Authentication service (referred to as **A/V Edge External** in the certificate wizard)

Create a single internal certificate with exportable private key, copy and assign it to each of the Edge Server internal interfaces:

- Edge Server (referred to as **Edge Internal** in the certificate wizard)

Important:

It is possible to use separate and distinct certificates for each Edge Server service. A good reason to choose separate certificates is if you want to use the new rolling certificate feature for the A/V Edge service certificate. In the case of this feature, decoupling the A/V Edge service certificate from the Access Edge service and Web Conferencing Edge service is recommended. If you choose to request, acquire and assign separate certificates for each service, you must request that the private key be exportable for the A/V Edge service (again, this is in actuality the A/V Authentication service) and assign the same certificate to the A/V Edge External interface on each Edge Server.

Tasks

Staging AV and OAuth Certificates Using -Roll in Set-CsCertificate

Concepts

Changes in Lync Server 2013 That Affect Edge Server Planning

1.3.9.10 Scenarios for External User Access

Scenarios for External User Access

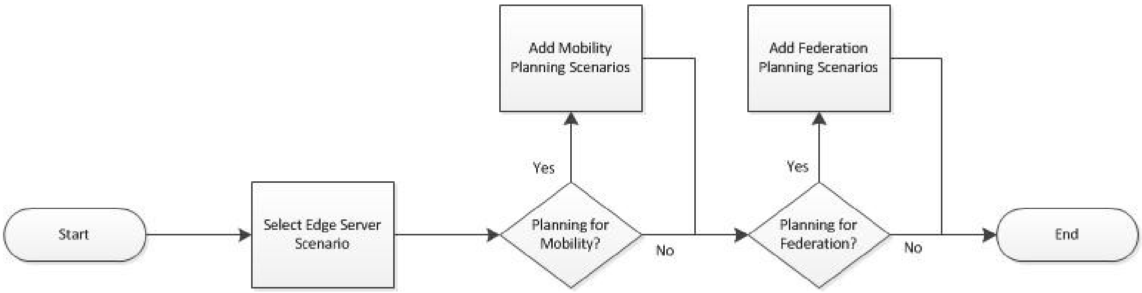
Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2012-09-08*

Providing external user access for Lync Server 2013 requires that you deploy at least one Edge Server and one reverse proxy in your perimeter network. Optionally, you may deploy a Director or Director pool in your internal network.

If you need greater capacity than a single Edge Server can provide, or if you need high availability for your Edge Server deployment, you can configure load balancing and deploy multiple Edge Servers in a load balanced pool. If your organization has multiple data centers, you can have Edge Server or Edge pool deployments at more than one location. However, only one of the Edge Server deployments can be designated as the federation route.

This section defines the scenarios for Edge Server deployments and maps the planning sections to the possible scenarios. For example, if your deployment requires high availability, federation with extensible messaging and presence (XMPP) contacts, and Lync mobility, you would select the matching entries in the following table that would satisfy these requirements and use the referenced planning sections to define your deployment, as illustrated in the following flowchart.


Start
Select Edge Server Scenario
Planning for Mobility?
Yes
Add Mobility Planning Scenarios
No
Planning for Federation?
Yes
Add Federation Planning Scenarios
No
End

By using this process, you can plan for and document the configuration of all potential features that you intend to deploy for your users. However, you can add federation and mobility services after you have deployed the Edge Server and have confirmed the correct operation before adding other features. The process of adding features to an existing Edge Server deployment is covered in the Deployment section. For details on deployment, see Deploying External User Access By including planning for these features during the initial planning process, you can prepare for the DNS, firewall, and certificate requirements for the added features, which enables you to acquire the certificates and configure DNS and port/protocol requirements in advance.

Tip:

If you are planning to install the Edge Servers and reverse proxy and then add features later (for example, federation and mobility), determine what certificates you will require for all services after deployment. Planning for and acquiring the certificates for all features in advance, initially deployed or not, saves you from having to order new certificates to satisfy the requirements of federation (that is, on the Edge Servers) or the reverse proxy (that is, for mobility services).

Note:

All edge services run on each Edge Server. Services cannot be split between two different Edge Servers. If you deploy an Edge pool for scalability, all edge services are deployed on each Edge Server in the pool. XMPP federation, Office Communications Server, and Lync Server federation, public IM connectivity and client mobility are additional services that can be deployed after you have deployed your first Edge Server or Edge pool. Mobility services is a feature that uses the reverse proxy. Installation of mobility services will not add features to your Edge Servers, but will require reconfiguration of your reverse proxy. The **Installation goal** column that lists these features provides planning guidance in the associated column under **Edge Server planning section or sections** for concurrently planning these features to be deployed when the Edge Servers are installed and configured.

Identifying and Mapping Your Deployment Goals

Installation goal	Edge Server planning documentation
You have decided that a single server is sufficient for Edge services in your infrastructure. You also intend to use private IP addresses for the Edge server external interfaces with NAT to the Internet.	Single Consolidated Edge with Private IP Addresses and NAT

Use this planning section if you are deploying a single Edge Server in your perimeter. You will deploy an Edge Server with private IP addresses assigned to the Edge Server and will use NAT to provide the public IP addresses for the external users on the Internet.	
You have decided that a single server is sufficient for Edge services in your infrastructure. You also intend to use public IP addresses for the Edge server external interfaces to the Internet. Use this planning section if you are deploying a single Edge Server in your perimeter. You will deploy an Edge Server with public IP addresses assigned to the Edge Server. Instead of NAT, you will use routing in this scenario. The actual public IP address of the Edge Server are made available for external user connections.	Single Consolidated Edge with Public IP Addresses
You have decided that high availability of the Edge services is important to your users and you will deploy two or more Edge Servers in this pool. You also intend to use private IP addresses for the Edge Server external interfaces with NAT to the Internet. Use this planning section if you are deploying a pool of Edge Servers in your perimeter. You will deploy the Edge Servers with private IP addresses assigned to the Edge Server, using DNS load balancing to distribute communication across the pool. You will use NAT to provide the public IP addresses for the external users on the Internet.	Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT
You have decided that high availability of the Edge services is important to your users and you will deploy two or more Edge Servers in this pool. You also intend to use public IP addresses for the Edge Server external interfaces to the Internet. Use this planning section if you are deploying a pool of Edge Servers in your perimeter. You will deploy the Edge Servers with public IP addresses assigned to the Edge Server, using DNS load balancing to distribute communication across the pool. Instead of NAT, you will use routing to provide the public IP addresses for the external users on the Internet.	Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses
You have decided that high availability of the Edge services is important to your users and you will deploy two or more Edge	Scaled Consolidated Edge with Hardware Load Balancers

Servers in this pool using a hardware load balancer. Use this planning section if you are deploying a pool of Edge Servers in your perimeter. You will deploy the Edge Servers with public IP addresses assigned to the Edge Server, using hardware load balancers to distribute communication across the pool. Instead of NAT, you will use routing to provide the public IP addresses for the external users on the Internet.	
The federation scenarios allow you to plan for the feature that will extend the types of partners that your users can communicate with. • Lync Server federation • Office Communications Server federation • Public IM connectivity • XMPP federation	Planning for Federation Scenarios • Planning for Lync Server and Office Communications Server Federation • Planning for Public Instant Messaging Connectivity • Planning for Extensible Messaging and Presence Protocol (XMPP) Federation
Mobility services are offered through the reverse proxy. Services that enable mobility for external users are deployed on the Front End Server or Front End pool. You create or modify existing publishing rules on the reverse proxy to enable mobility services for your external users.	Planning for Mobility

Tip:

In the following Scenarios sections are reference architectures, example DNS, port/protocol definitions, and certificate requirements. Also included are diagrams for your DNS, port/protocol definitions and certificate needs. The diagrams will provide a template for you to fill in and distribute to other teams (for example, your organization's Network Team, Public Key Infrastructure Team, and Server Deployment Team). The goal of the diagrams is to enhance communication and to ensure success when communicating the required Edge Server configuration elements to the people who will do the actual configuration work. We recommend that you use the diagrams and associated reference architectures to plan your deployment.

1.3.9.10.1 Single Consolidated Edge with Private IP Addresses and NAT

Single Consolidated Edge with Private IP Addresses and NAT

See Also

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2012-09-08*

If your organization requires support for fewer than 15,000 Access Edge service client connections, 1,000 active Lync Server Web Conferencing service client connections, and 500 concurrent A/V Edge sessions, and high availability of the Edge Server is not important, this topology offers the advantages of lower hardware cost and simpler deployment. If you need greater capacity or you require high availability, you need to deploy a scaled consolidated Edge Server topology. For details, see one of the following:

- Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses

Using NAT
- Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses
- Scaled Consolidated Edge with Hardware Load Balancers

The figure does not show Directors, an optional server role deployed in the internal network between the Edge Servers and your Front End pools or server. For details about the topology for Directors, see Components Required for the Director. The figure represents a single reverse proxy.

Note:

The figure shown is for orientation and example IP addressing, but does not intend to represent actual communication flows with the correct incoming and outgoing traffic. The figure represents a high level view of possible traffic. Details for traffic flow as they pertain to incoming (to listening ports) and outgoing (to destination servers or clients) is represented in the Port Summary diagram in each scenario. For example, TCP 443 is actually inbound (to the Edge or reverse proxy) only, and is only a two-way flow from a protocol (TCP) perspective. Additionally, the figure shows the nature of traffic as it changes when NAT (network address translation) occurs (destination address is changed on inbound, source address is changed on outbound). Example external and internal firewall, and server interfaces are shown for reference purposes only. Finally, example default gateway and route relationships are shown, where applicable. Note also that the diagram uses the *.com* DNS zone to represent the external DNS zone for both reverse proxy and Edge Servers, and the *.net* DNS zone refers to the internal DNS zone.

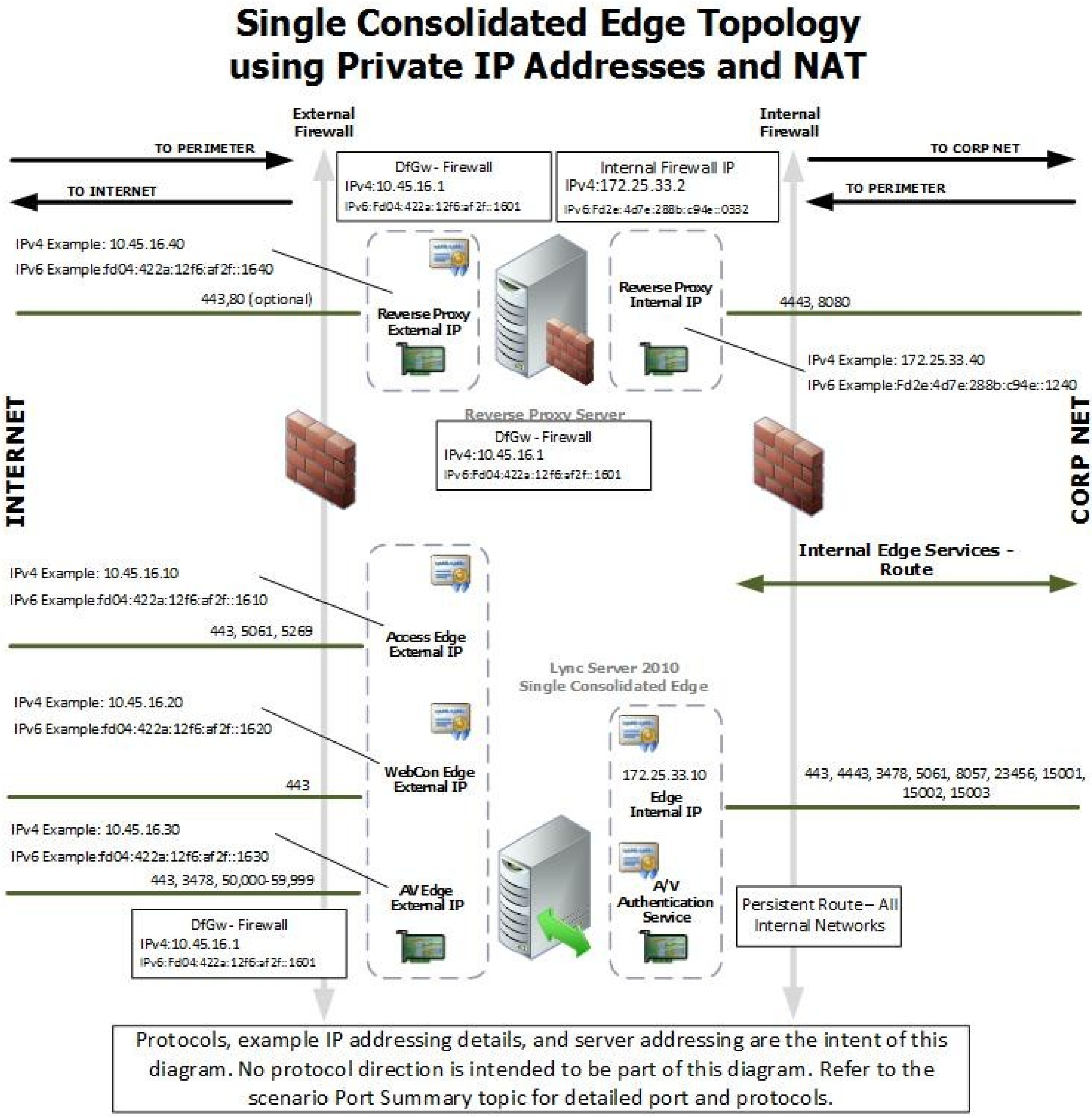
New to Microsoft Lync Server 2013 is support for IPv6 addressing. Much like IPv4 addressing, IPv6 addresses must be assigned in such a way that the addresses are part of your assigned IPv6 address space. The addresses in this topic are for example only. You must acquire IPv6 addresses that will function in your deployment, provide the correct scope and will interoperate with internal and external addressing. Windows Server provides a feature that is important to transitional IPv6 operation and IPv4 to IPv6 communication called the *dual stack*. The dual stack is a separate and distinct network stack for IPv4 and for IPv6. The dual stack is what allows you to assign addressing for IPv4 and IPv6 concurrently, and allows the server to communicate with other hosts and clients based on what their requirements are.

Typical address types that you will use for IPv6 addressing will be the IPv6 global addresses (similar to public IPv4 addresses), IPv6 unique local addresses (similar to the private IPv4 address ranges) and IPv6 link-local addresses (similar to automatic private IP addresses in Windows Server for IPv4)

Network address translation technologies (NAT) for IPv6 exist that will allow for NAT IPv6 to IPv4 (commonly referred to as NAT64) and for NAT IPv6 to IPv6 (commonly referred to as NAT66). The existence of NAT technologies means that the five scenarios presented for Lync Server Edge Servers are still valid.

Warning:

IPv6 is a complex topic and requires careful planning with your networking team and your Internet provider to ensure that the addresses you assign at the Windows server level and at the Lync Server 2013 level will work as expected. See the links at the end of this topic for additional resources on IPv6 addressing and planning.



Single Consolidated Edge Topology using Private IP Addresses and NAT

External Firewall
Internal Firewall
TO PERIMETER
TO INTERNET
TO CORP NET
TO PERIMETER
DfGw - Firewall
IPv4:10.45.16.1
IPv6:Fd04:422a:12f6:af2f::1601
Internal Firewall IP
IPv4:172.25.33.2
IPv6:Fd2e:4d7e:288b:c94e::0332
IPv4 Example: 10.45.16.40
IPv6 Example:fd04:422a:12f6:af2f::1640
443,80 (optional)
Reverse Proxy External IP
Reverse Proxy Internal IP
4443, 8080
IPv4 Example: 172.25.33.40
IPv6 Example:Fd2e:4d7e:288b:c94e::1240
Reverse Proxy Server
DfGw - Firewall
IPv4:10.45.16.1
IPv6:Fd04:422a:12f6:af2f::1601
INTERNET
CORP NET
Internal Edge Services - Route
IPv4 Example: 10.45.16.10
IPv6 Example:fd04:422a:12f6:af2f::1610
443, 5061, 5269
Access Edge External IP
Lync Server 2010 Single Consolidated Edge
IPv4 Example: 10.45.16.20
IPv6 Example:fd04:422a:12f6:af2f::1620
443
WebCon Edge External IP
172.25.33.10
Edge Internal IP
443, 4443, 3478, 5061, 8057, 23456, 15001, 15002, 15003
IPv4 Example: 10.45.16.30
IPv6 Example:fd04:422a:12f6:af2f::1630
443, 3478, 50,000-59,999
A/V Edge External IP
A/V Authentication Service
Persistent Route – All Internal Networks
DfGw - Firewall
IPv4:10.45.16.1
IPv6:Fd04:422a:12f6:af2f::1601

Protocols, example IP addressing details, and server addressing are the intent of this diagram. No protocol direction is intended to be part of this diagram. Refer to the scenario Port Summary topic for detailed port and protocols.

Important:

If you are using Call Admission Control (CAC), you still must assign IPv4 addresses to the Edge Server internal interface. CAC uses IPv4 addresses and must have them available to operate.

- Certificate Summary - Single Consolidated Edge with Private IP Addresses Using NAT
- Port Summary - Single Consolidated Edge with Private IP Addresses Using NAT
- DNS Summary - Single Consolidated Edge with Private IP Addresses Using NAT

See Also

Other Resources

IP Version 6 Addressing Architecture
IPv6 Global Unicast Address Format
Unique Local IPv6 Unicast Addresses

Certificate Summary - Single Consolidated Edge with Private IP Addresses Using NAT

Planning for External User Access > Scenarios for External User Access > Single Consolidated Edge with Private IP Addresses and NAT >

Topic Last Modified: *2012-10-22*

Microsoft Lync Server 2013 uses certificates to mutually authenticate other servers and to encrypt data from server to server and server to client. Certificates require name matching of the domain name system (DNS) records associated with the servers and the subject name (SN) and subject alternative name (SAN) on the certificate. To successfully map servers, DNS records and certificate entries, you must carefully plan your intended server fully qualified domain names as registered in DNS and the SN and SAN entries on the certificate.

The certificate assigned to the external interfaces of the Edge Server is requested from a public certification authority (CA). Public CAs that have demonstrated success in supplying certificates for the purposes of Unified Communications are listed in the following article: http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=929395. When requesting the certificate, you can use the certificate request generated by the Lync Server Deployment Wizard or create the request manually using Lync Server Management Shell cmdlets or by a process provided by a public CA. For details on Lync Server Management Shell cmdlets for certificate management, see Certificate and Authentication Cmdlets When assigning the certificate, the certificate is assigned to the Access Edge service interface, the Web Conferencing Edge service interface, and the Audio/Video Authentication service. The Audio/Video Authentication service should not be confused with the A/V Edge service which does not use a certificate to encrypt the audio and video streams. The internal Edge Server interface can use a certificate from an internal (to your organization) CA or a certificate from a public CA. The internal interface certificate uses only the SN and does not need or use SAN entries.

Note:

The following table shows a second SIP entry (sip.fabrikam.com) in the subject alternative name list for reference. For each SIP domain in your organization, you need to add a corresponding FQDN listed in the certificate subject alternative name list.

Certificates Required for Single Consolidated Edge with Private IP Addresses using NAT

Component	Subject name (SN)	Subject alternative names (SAN)/Order	Comments
Single consolidated Edge (External Edge)	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com	Certificate must be from a Public CA, and must have the server EKU and client EKU if public IM connectivity with AOL is to be deployed. The certificate is assigned to the external Edge interfaces for: • Access Edge • Conferencing Edge

			- A/V Edge Note that SANs are automatically added to the certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.
Single consolidated Edge (Internal Edge)	lsedge.contoso.net	No SAN required	Certificate can be issued by a public or private CA, and must contain the server EKU. The certificate is assigned to the internal Edge interface.

Certificate Summary – Public Instant Messaging Connectivity

Component	**Subject name**	**Subject alternative names (SAN)/Order**	**Comments**
External/Access Edge	sip.contoso.com	sip.contoso.com webcon.contoso.com sip.fabrikam.com	Certificate must be from a Public CA, and must have the server EKU and client EKU if public IM connectivity with AOL is to be deployed. The certificate is assigned to the external Edge interfaces for: - Access Edge - Conferencing Edge - A/V Edge Note that SANs are automatically added to the certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.

Certificate Summary for Extensible Messaging and Presence Protocol

Component	**Subject name**	**Subject alternative**	**Comments**

		names (SAN)/Order	
Assign to Access Edge service of Edge Server or Edge pool	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com xmpp.contoso.com ***.contoso.com**	The first three SAN entries are the normal SAN entries for a full Edge Server. The contoso.com is the entry required for federation with the XMPP partner at the root domain level. This entry will allow XMPP for all domains with the suffix *.contoso.com.

1.3.9.10.1.2 Port Summary - Single Consolidated Edge with Private IP Addresses Using NAT

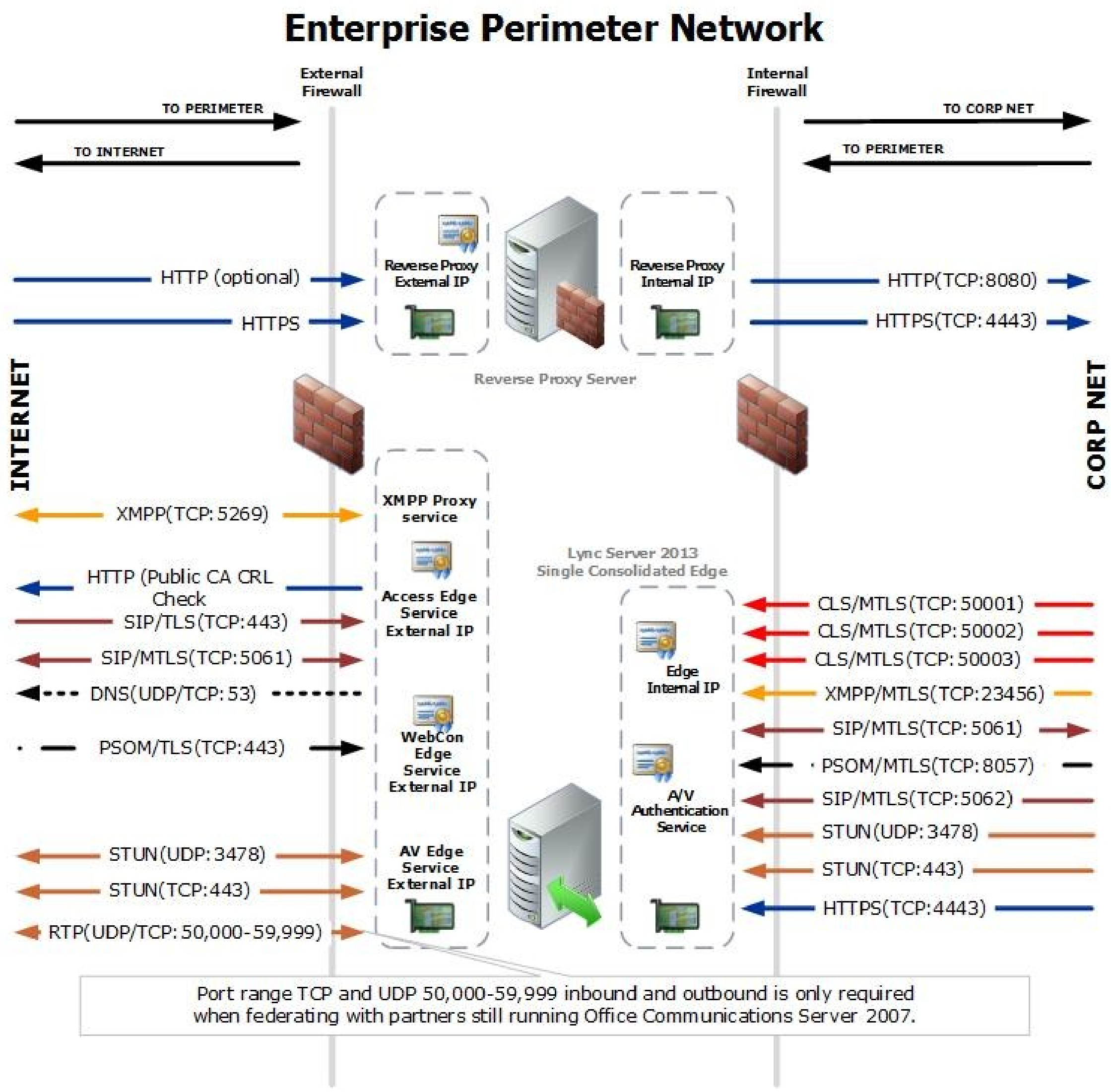
Port Summary - Single Consolidated Edge with Private IP Addresses Using NAT

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2013-02-22*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.



Port and Protocol Details

We recommend that you open only the ports required to support the functionality for which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bi-directionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V), and federation.

Firewall Summary for Single Consolidated Edge with Private IP Addresses using NAT: External Interface

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP

			federations
Access/HTTP/TCP/80	Edge Server Access Edge service	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service	Any	DNS query over UDP
Access/SIP(TLS)/ TCP/443	Any	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Any	For federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)/TCP/443	Any	Edge Server Web Conferencing Edge service	Web Conferencing media
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-59,999	Edge Server A/V Edge service	Any	Required only for federation with partners running Office Communications Server 2007.
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service	Required only for federation with partners running Office Communications Server 2007
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service	Required only for federation with partners running Office Communications Server 2007
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service	Any	3478 outbound is used to determine

			the version of Edge Server that Lync Server is communicating with and also for media traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/ UDP/3478	Any	Edge Server A/V Edge service	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/ TCP/443	Any	Edge Server A/V Edge service	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/ TCP/443	Edge Server A/V Edge service	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Single Consolidated Edge with Private IP Addresses Using NAT: Internal Interface

Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Comments
XMPP/MTLS/ TCP/23456	Any (can be defined as Standard Edition server IP, Standard Edition server IP address, or pool IP address running the XMPP Gateway service)	Edge Server internal interface	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
SIP/MTLS/TCP/5061	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Edge Server internal interface	Outbound SIP traffic (from Director, Director pool IP address, Front End Server or Front End pool IP address) to Edge Server internal interface
SIP/MTLS/TCP/5061	Edge Server internal interface	Any (can be defined as Director, Director pool IP address, Front End Server or Front	Inbound SIP traffic (to Director, Director pool IP address, Front End Server or Front End

		End pool IP address)	pool IP address) from Edge Server internal interface
PSOM/MTLS/TCP/8057	Any (can be defined as Front End Server IP address, or each Front End Server IP address in a Front End pool)	Edge Server internal interface	Web conferencing traffic from Front End Server or each Front End Server if in a pool, to Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server internal interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/UDP/3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server
STUN/MSTURN/TCP/443	Any	Edge Server internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server if UDP communication cannot be established, TCP is used for file transfer and desktop sharing
HTTPS/TCP/4443	Any (can be defined as the Front End Server IP address, or pool that holds the Central Management store)	Edge Server internal interface	Replication of changes from the Central Management store to the Edge Server
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line

			(ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	**Source IP address**	**Destination IP address**	**Notes**
Access/SIP(MTLS)/ TCP/5061	Access Edge service public IP address	Any	For federated and public IM connectivity using SIP

Firewall Summary – Public Instant Messaging Connectivity

Role/Protocol/TCP or UDP/Port	**Source IP address**	**Destination IP address**	**Notes**
Access/SIP(MTLS)/ TCP/5061	Public IM connectivity partners	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Public IM connectivity partners	For federated and public IM connectivity using SIP
Access/SIP(TLS)/ TCP/443	Clients	Edge Server Access Edge service	Client-to-server SIP traffic for external

			user access
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/UDP/3478	Edge Server A/V Edge service	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger
A/V/STUN,MSTURN/UDP/3478	Live Messenger clients	Edge Server A/V Edge service	Required for public IM connectivity with Windows Live Messenger

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Edge Server Access Edge serviceinterface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Edge Server Access Edge service interface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from the Edge Server XMPP proxy to federated XMPP partners
XMPP/MTLS/TCP/23456	Any	Each internal Edge Server Interface IP	Internal XMPP traffic from the XMPP Gateway on the Front End Server or Front End pool to the Edge Server internal IP address or each Edge pool member's internal IP address

1.3.9.10.1.3 DNS Summary - Single Consolidated Edge with Private IP Addresses Using NAT

DNS Summary - Single Consolidated Edge with Private IP Addresses Using NAT

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS

Requirements for Edge Servers and Features >

Topic Last Modified: *2012-09-08*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about automatic configuration of clients running Lync 2013 if split-brain DNS is not configured, see "Automatic Configuration without Split-Brain DNS" in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the single consolidated edge topology shown in the Single Consolidated Edge Topology figure. Note that certain DNS records are required only for automatic configuration of Lync 2013 and Lync 2010 clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated automatic configuration records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Single Consolidated Edge Topology figure in Single Consolidated Edge with Private IP Addresses and NAT, the default gateway would point to the external firewall (10.45.16.1).

You can configure two network adapters in your Edge Server as follows:

- **Network adapter 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 10.45.16.10 for Access Edge, 10.45.16.20 for Web Conferencing Edge, 10.45.16.30 for AV Edge

  Note:

  It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge, 444/TCP for the Web Conferencing Edge and 443/TCP for the AV Edge might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

  Access Edge IP address is primary with default gateway set to integrated router (10.45.16.1).
  Web conferencing and A/V Edge IP addresses secondary.

Tip:

Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Single Consolidated Edge with Private IP Addresses Using NAT (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20	Web Conferencing Edge external interface
External DNS/A	av.contoso.com	131.107.155.30	A/V Edge external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of federated partners known as "Allowed SIP Domain" (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users
Internal DNS/A	lsedge.contoso.net	172.25.33.10	Consolidated Edge internal interface

◆Important:

The records listed in the previous table are shown with either a *.net* extension or a *.com* extension to highlight which zone they need to reside in if you are not using split-brain DNS. If you are using split-brain DNS, all records would be in the same *.com* zone, with the only distinction being whether they are in the internal or external DNS zone version. For details, see "Split-Brain DNS" in Determine DNS Requirements.

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp.contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of your federation to other potential federation partners, and is known as "Allowed SIP Domains" (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users **Important:** This SRV record is required for mobility and the push notification clearing house

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat as necessary for all internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy

			through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An allowed XMPP domain must also be configured in the XMPP Federated Partners policy. See topics in **See Also** for additional details
External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP proxy	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service. Typically, the SRV record that you create will point to this host (A or AAAA) record

1.3.9.10.2 Single Consolidated Edge with Public IP Addresses

Single Consolidated Edge with Public IP Addresses

See Also

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2012-09-08*

If your organization needs support for fewer than 15,000 Access Edge service client connections, 1,000 active Lync Server Web Conferencing service client connections, and 500 concurrent A/V Edge sessions, and high availability of the Edge Server is not important, this topology offers the advantages of lower hardware cost and simpler deployment. If you need greater capacity or you require high availability, you should deploy a scaled consolidated Edge Server topology.

- Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT
- Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses
- Scaled Consolidated Edge with Hardware Load Balancers

◆**Important:**
When using public IP address on the Edge Server, the default gateway on the Edge Server is no longer your firewall or router, but the router or firewall at your public perimeter edge – which will be a public address. The reverse proxy continues to use the router or firewall associated with the outermost perimeter network. The difference between the reverse proxy and the Edge Server with public IP addresses is that the reverse proxy is still using NAT and the Edge Server is using a route relationship.

The figure does not show Directors, an optional server role deployed in the internal network between the Edge Servers and your Front End pools or server. For details about the topology for Directors, see Components Required for the Director. The figure represents a single reverse proxy.

Note:

The figure shown is for orientation and example IP addressing, but does not intend to represent actual communication flows with the correct incoming and outgoing traffic. The figure represents a high level view of possible traffic. Details for traffic flow as they pertain to incoming (to listening ports) and outgoing (to destination servers or clients) is represented in the Port Summary diagram in each scenario. For example, TCP 443 is actually inbound (to the Edge or reverse proxy) only, and is only a two-way flow from a protocol (TCP) perspective. Additionally, the figure shows the nature of traffic as it changes when NAT (network address translation) occurs (destination address is changed on inbound, source address is changed on outbound). Example external and internal firewall, and server interfaces are shown for reference purposes only. Finally, example default gateway and route relationships are shown, where applicable. Note also that the diagram uses the *.com* DNS zone to represent the external DNS zone for both reverse proxy and Edge Servers, and the *.net* DNS zone refers to the internal DNS zone.

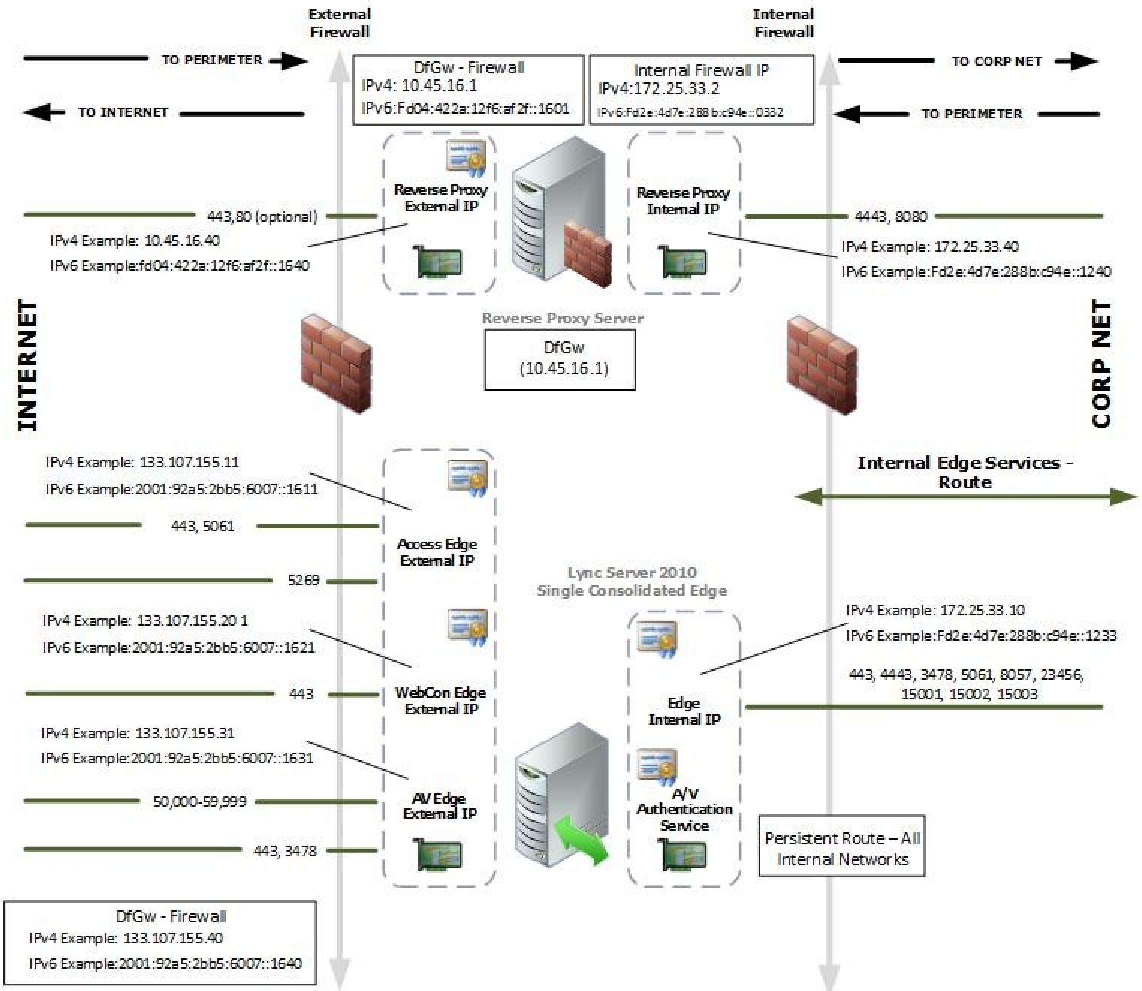
New to Microsoft Lync Server 2013 is support for IPv6 addressing. Much like IPv4 addressing, IPv6 addresses must be assigned in such a way that the addresses are part of your assigned IPv6 address space. The addresses in this topic are for example only. You must acquire IPv6 addresses that will function in your deployment, provide the correct scope and will interoperate with internal and external addressing. Windows Server provides a feature that is important to transitional IPv6 operation and IPv4 to IPv6 communication called the *dual stack*. The dual stack is a separate and distinct network stack for IPv4 and for IPv6. The dual stack is what allows you to assign addressing for IPv4 and IPv6 concurrently, and allows the server to communicate with other hosts and clients based on what their requirements are.

Typical address types that you will use for IPv6 addressing will be the IPv6 global addresses (similar to public IPv4 addresses), IPv6 unique local addresses (similar to the private IPv4 address ranges) and IPv6 link-local addresses (similar to automatic private IP addresses in Windows Server for IPv4)

Network address translation technologies (NAT) for IPv6 exist that will allow for NAT IPv6 to IPv4 (commonly referred to as NAT64) and for NAT IPv6 to IPv6 (commonly referred to as NAT66). The existence of NAT technologies means that the five scenarios presented for Lync Server Edge Servers are still valid.

Warning:

IPv6 is a complex topic and requires careful planning with your networking team and your Internet provider to ensure that the addresses you assign at the Windows server level and at the Lync Server 2013 level will work as expected. See the links at the end of this topic for additional resources on IPv6 addressing and planning.



Single Consolidated Edge Topology using Public IP Addresses

External Firewall
Internal Firewall
TO PERIMETER
TO INTERNET
DfGw - Firewall
IPv4: 10.45.16.1
IPv6:Fd04:422a:12f6:af2f::1601
Internal Firewall IP
IPv4:172.25.33.2
IPv6:Fd2e:4d7e:288b:c94e::0332
TO CORP NET
TO PERIMETER
Reverse Proxy External IP
Reverse Proxy Internal IP
443,80 (optional)
IPv4 Example: 10.45.16.40
IPv6 Example:fd04:422a:12f6:af2f::1640
4443, 8080
IPv4 Example: 172.25.33.40
IPv6 Example:Fd2e:4d7e:288b:c94e::1240
Reverse Proxy Server
DfGw
(10.45.16.1)
INTERNET
CORP NET
IPv4 Example: 133.107.155.11
IPv6 Example:2001:92a5:2bb5:6007::1611
443, 5061
Access Edge External IP
5269
Internal Edge Services - Route
Lync Server 2010
Single Consolidated Edge
IPv4 Example: 133.107.155.20 1
IPv6 Example:2001:92a5:2bb5:6007::1621
443
WebCon Edge External IP
IPv4 Example: 172.25.33.10
IPv6 Example:Fd2e:4d7e:288b:c94e::1233
443, 4443, 3478, 5061, 8057, 23456, 15001, 15002, 15003
Edge Internal IP
IPv4 Example: 133.107.155.31
IPv6 Example:2001:92a5:2bb5:6007::1631
50,000-59,999
AV Edge External IP
A/V Authentication Service
443, 3478
Persistent Route – All Internal Networks
DfGw - Firewall
IPv4 Example: 133.107.155.40
IPv6 Example:2001:92a5:2bb5:6007::1640

Protocols, example IP addressing details, and server addressing are the intent of this diagram. No protocol direction is intended to be part of this diagram. Refer to the scenario Port Summary topic for detailed port and protocols.

◆Important:

If you are using Call Admission Control (CAC), you still must assign IPv4 addresses to the Edge Server internal interface. CAC uses IPv4 addresses and must have them available to operate.

- Certificate Summary - Single Consolidated Edge with Public IP Addresses
- Port Summary - Single Consolidated Edge with Public IP Addresses
- DNS Summary - Single Consolidated Edge with Public IP Addresses

⊟See Also

Other Resources

IP Version 6 Addressing Architecture
IPv6 Global Unicast Address Format
Unique Local IPv6 Unicast Addresses

Certificate Summary - Single Consolidated Edge with Public IP Addresses

Planning for External User Access > Scenarios for External User Access > Single Consolidated Edge with Public IP Addresses >

Topic Last Modified: *2012-09-08*

Microsoft Lync Server 2013 uses certificates to mutually authenticate other servers and to encrypt data from server to server and server to client. Certificates require name matching of the domain name system (DNS) records associated with the servers and the subject name (SN) and subject alternative name (SAN) on the certificate. To successfully map servers, DNS records and certificate entries, you must carefully plan your intended server fully qualified domain names as registered in DNS and the SN and SAN entries on the certificate.

The certificate assigned to the external interfaces of the Edge Server is requested from a public certification authority (CA). Public CAs that have demonstrated success in supplying certificates for the purposes of Unified Communications are listed in the following article: http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=929395 When requesting the certificate, you can use the certificate request generated by the Lync Server Deployment Wizard or create the request manually or by a process provided by the public CA. When assigning the certificate, the certificate is assigned to the Access Edge service interface, the Web Conferencing Edge service interface, and the Audio/Video Authentication service. The Audio/Video Authentication service should not be confused with the A/V Edge service which does not use a certificate to encrypt the audio and video streams. The internal Edge Server interface can use a certificate from an internal (to your organization) CA or a certificate from a public CA. The internal interface certificate uses only the SN and does not need or use SAN entries.

Note:

The following table shows a second SIP entry (sip.fabrikam.com) in the subject alternative name list for reference. For each SIP domain in your organization, you need to add a corresponding FQDN listed in the certificate subject alternative name list.

Certificates Required for Single Consolidated Edge with Public IP Addresses

Component	Subject name (SN)	Subject alternative names (SAN)/Order	Comments
Single consolidated Edge (External Edge)	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com	Certificate must be from a Public CA, and must have the server EKU and client EKU if public IM connectivity with AOL is to be deployed. The certificate is assigned to the external Edge interfaces for: • Access Edge • Conferencing Edge • A/V Edge

			Note that SANs are automatically added to the certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.
Single consolidated Edge (Internal Edge)	lsedge.contoso.net	No SAN required	Certificate can be issued by a public or private CA, and must contain the server EKU. The certificate is assigned to the internal Edge interface.

Certificate Summary – Public Instant Messaging Connectivity

Component	**Subject name**	**Subject alternative names (SAN)/Order**	**Comments**
External/Access Edge	sip.contoso.com	sip.contoso.com webcon.contoso.com sip.fabrikam.com	Certificate must be from a Public CA, and must have the server EKU and client EKU if public IM connectivity with AOL is to be deployed. The certificate is assigned to the external Edge interfaces for: • Access Edge • Conferencing Edge • A/V Edge Note that SANs are automatically added to the certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.

Certificate Summary for Extensible Messaging and Presence Protocol

Component	**Subject name**	**Subject alternative names (SAN)/Order**	**Comments**

Assign to Access Edge service of Edge Server or Edge pool	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com xmpp.contoso.com ***.contoso.com**	The first three SAN entries are the normal SAN entries for a full Edge Server. The contoso.com is the entry required for federation with the XMPP partner at the root domain level. This entry will allow XMPP for all domains with the suffix *.contoso.com.

1.3.9.10.2.2 Port Summary - Single Consolidated Edge with Public IP Addresses

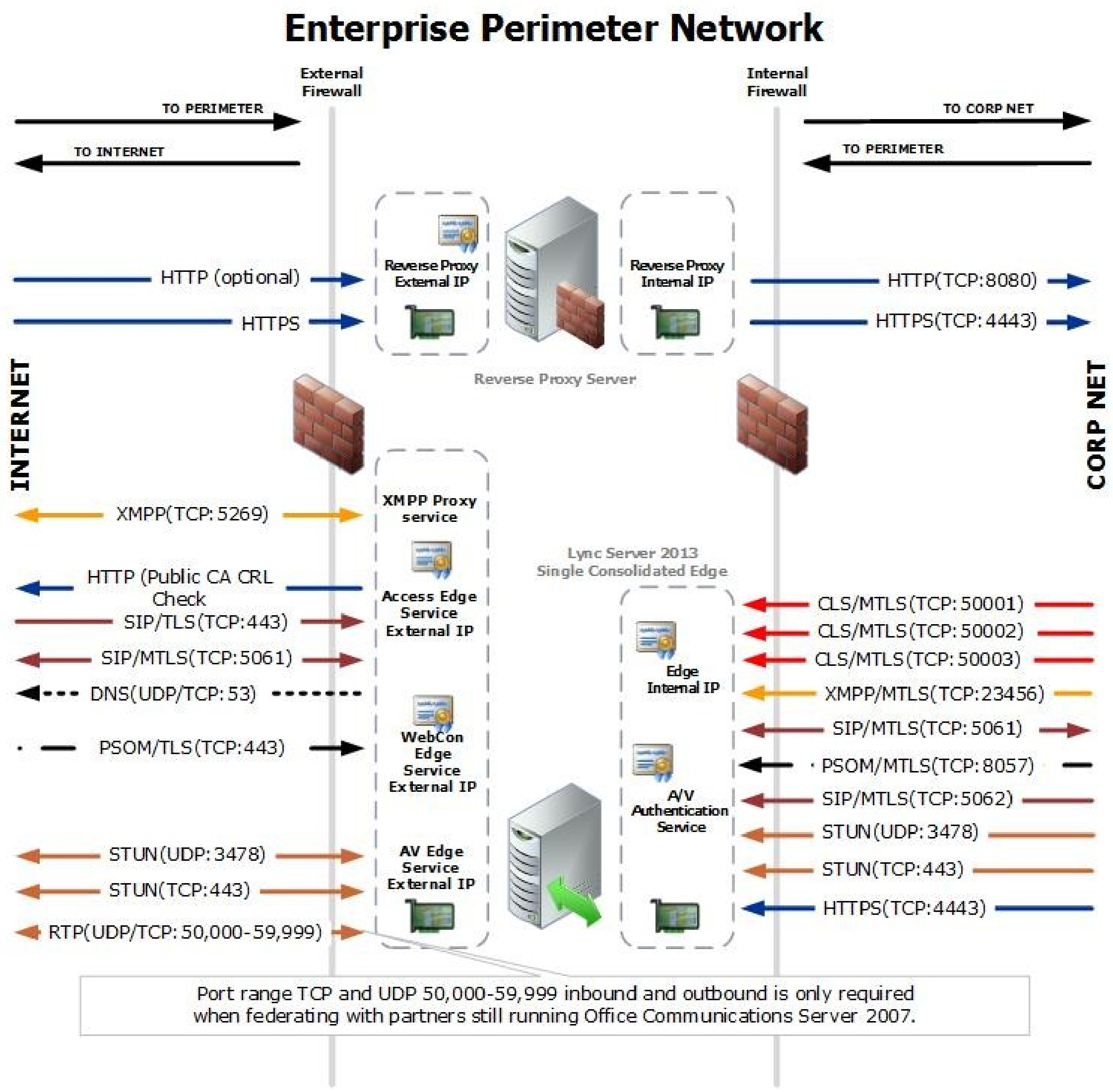
Port Summary - Single Consolidated Edge with Public IP Addresses

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2013-02-21*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool. Planning information for the reverse proxy and federation are found in Scenarios for Reverse Proxy and Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation sections, respectively.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.



Port and Protocol Details

We recommend that you open only the ports required to support the functionality for which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bidirectionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V) and federation.

Firewall Summary for Single Consolidated Edge with Public IP Addresses: External Interface

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP

			federations
Access/HTTP/TCP/80	Edge Server Access Edge service public IP address	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service public IP address	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service public IP address	Any	DNS query over UDP
Access/SIP(TLS)/ TCP/443	Any	Edge Server Access Edge service public IP address	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Edge Server Access Edge service public IP address	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service public IP address	Any	For federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)/TCP/443	Any	Edge Server Web Conferencing Edge service public IP address	Web Conferencing media
A/V/RTP/TCP/50,000-59,999	Edge Server Access Edge service public IP address	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-59,999	Edge Server A/V Edge service public IP address	Any	Required only for federation with partners running Office Communications Server 2007
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007.
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications

			Server 2007.
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service public IP address	Any	3478 outbound is used to determine the version of Edge Server that Lync Server is communicating with and also for media traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/ UDP/3478	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/ TCP/443	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/ TCP/443	Edge Server A/V Edge service public IP address	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Single Consolidated Edge with Public IP Addresses: Internal Interface

Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Comments
XMPP/MTLS/ TCP/23456	Any (can be defined as Standard Edition server IP, Standard Edition server IP address, or pool IP address running the XMPP Gateway service)	Edge Server internal interface	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
SIP/MTLS/TCP/5061	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Edge Server IP, or pool that holds the internal interface	Outbound SIP traffic (from Director, Director pool IP address, Front End Server or Front End pool IP address) to Edge Server internal interface

SIP/MTLS/TCP/5061	Edge Server internal interface	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool address)	Inbound SIP traffic (to Director, Director pool IP address, Front End Server or Front End pool IP address) from Edge Server internal interface
PSOM/MTLS/TCP/8057	Any (can be defined as Front End Server IP address, or each Front End Server IP address in a Front End pool)	Edge Server internal interface	Web conferencing traffic from Front End Server or each Front End Server if in a pool, to Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server internal interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/UDP/3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server
STUN/MSTURN/TCP/443	Any	Edge Server internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server if UDP communication cannot be established, TCP is used for file transfer and desktop sharing
HTTPS/TCP/4443	Any (can be defined as the Front End Server IP address, or pool that holds the Central Management store)	Edge Server internal interface	Replication of changes from the Central Management store to the Edge Server
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized

			Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Access Edge service public IP address	Any	For federated and public IM connectivity using SIP

Firewall Summary – Public Instant Messaging Connectivity

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Public IM connectivity partners	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Public IM connectivity partners	For federated and public IM connectivity using SIP

Access/SIP(TLS)/ TCP/443	Clients	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger
A/V/STUN,MSTURN/ UDP/3478	Live Messenger clients	Edge Server A/V Edge service	Required for public IM connectivity with Windows Live Messenger

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Edge Server Access Edge service interface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Edge Server Access Edge service interface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from the Edge Server XMPP proxy to federated XMPP partners
XMPP/MTLS/ TCP/23456	Any	Each internal Edge Server Interface IP	Internal XMPP traffic from the XMPP Gateway on the Front End Server or Front End pool to the Edge Server internal IP address or each Edge pool member's internal IP address

1.3.9.10.2.3 DNS Summary - Single Consolidated Edge w ith Public IP Addresses

DNS Summary - Single Consolidated Edge with Public

IP Addresses

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-09-08*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about automatic configuration of clients running Lync 2013 if split-brain DNS is not configured, see "Automatic Configuration without Split-Brain DNS" in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the single consolidated edge topology shown in the Single Consolidated Edge Topology figure. Note that certain DNS records are required only for automatic configuration of Lync 2013 and Lync 2010 clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated automatic configuration records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Single Consolidated Edge Topology with Public IP Addresses figure in Single Consolidated Edge with Public IP Addresses, the default gateway would point to the external router at your Internet perimeter or firewall that can provide a public IP addresses. The network relationship for Edge Server interfaces is a route relationship instead of a NAT relationship.

You can configure two network adapters in your Edge Server as follows:

- **Network adapter 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 (External Interface)**
  Three public IP addresses are assigned to this network adapter, for example 131.107.155.10 for Access Edge, 131.107.155.20 for Web Conferencing Edge, 131.107.155.30 for AV Edge.

  > **Note:**
  > It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge, 444/TCP for the Web Conferencing Edge and 443/TCP for the AV Edge might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

  The Access Edge public IP address is primary with default gateway set to the public router (131.107.155.1).
  Web conferencing and A/V Edge public IP addresses are additional IP

addresses in the **Advanced** section of the properties of **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.

Tip:

Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Single Consolidated Edge with Public IP Addresses (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20	Web Conferencing Edge external interface
External DNS/A	av.contoso.com	131.107.155.30	A/V Edge external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of federated partners known as "Allowed SIP Domain" (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users
Internal DNS/A	lsedge.contoso.net	172.25.33.10	Consolidated Edge internal interface

Important:

The records listed in the previous table are shown with either a *.net* extension or a *.com* extension to highlight which zone they need to reside in if you are not using split-brain

DNS. If you are using split-brain DNS, all records would be in the same zone, with the only distinction being whether they are in the internal or external version. For details, see “Split-Brain DNS” in Determine DNS Requirements.

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp.contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of your federation to other potential federation partners, and is known as “Allowed SIP Domains” (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users ◆**Important:** This SRV record is required for mobility and the push notification clearing house

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat

			as necessary for all internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An allowed XMPP domain must also be configured in the XMPP Federated Partners policy. See topics in **See Also** for additional details
External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP proxy	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service. Typically, the SRV record that you create will point to this host (A or AAAA) record

1.3.9.10.3 Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

See Also

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2012-09-08*

In the Edge Server pool topology, two or more Edge Servers are deployed as a load-balanced pool in the perimeter network of the data center. Domain Name System (DNS) load balancing is used for traffic to both the external and internal Edge interfaces.

If your organization requires support for more than 15,000 Access Edge service client connections, 1,000 active Lync Server Web Conferencing service client connections, or 500 concurrent A/V Edge sessions, and/or high availability of the Edge Server is important, this topology offers the advantages of scalability and failover support.

The figure does not show Directors, an optional server role deployed in the internal network between the Edge Servers and your Front End pools or server. For details about the topology for Directors, see Components Required for the Director. The figure represents a single reverse proxy.

Note:

The figure shown is for orientation and example IP addressing, but does not intend to represent actual communication flows with the correct incoming and outgoing traffic. The figure represents a high level view of possible traffic. Details for traffic flow as they pertain to incoming (to listening ports) and outgoing (to destination servers or clients) is represented in the Port Summary diagram in each scenario. For example, TCP 443 is actually inbound (to the Edge or reverse proxy) only, and is only a two-way flow from a protocol (TCP) perspective. Additionally, the figure shows the nature of traffic as it changes when NAT (network address translation) occurs (destination address is changed on inbound, source address is changed on outbound). Example external and internal firewall, and server interfaces are shown for reference purposes only. Finally, example default gateway and route relationships are shown, where applicable. Note also that the diagram uses the *.com* DNS zone to represent the external DNS zone for both reverse proxy and Edge Servers, and the *.net* DNS zone refers to the internal DNS zone.

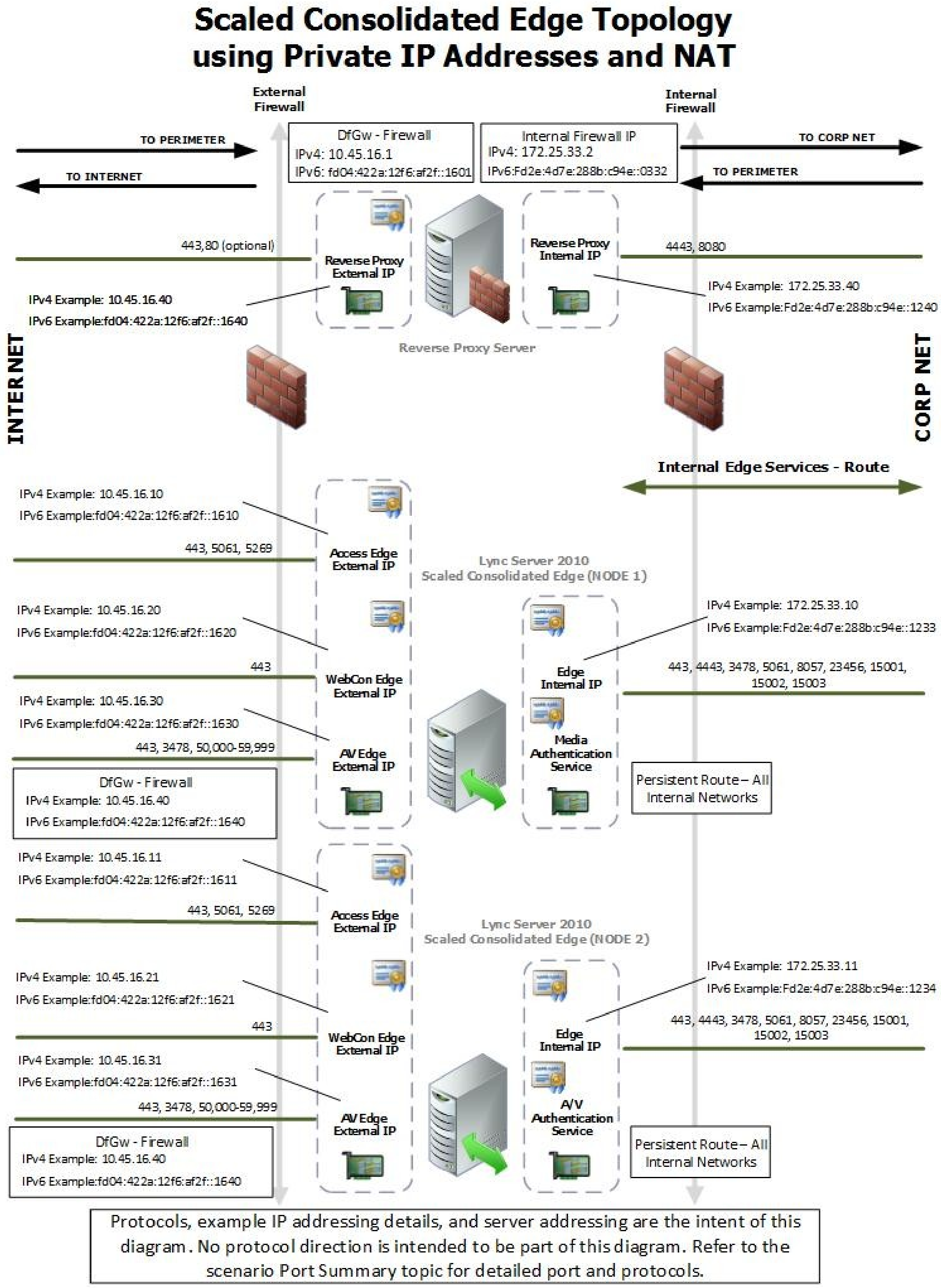
New to Microsoft Lync Server 2013 is support for IPv6 addressing. Much like IPv4 addressing, IPv6 addresses must be assigned in such a way that the addresses are part of your assigned IPv6 address space. The addresses in this topic are for example only. You must acquire IPv6 addresses that will function in your deployment, provide the correct scope and will interoperate with internal and external addressing. Windows Server provides a feature that is important to transitional IPv6 operation and IPv4 to IPv6 communication called the *dual stack*. The dual stack is a separate and distinct network stack for IPv4 and for IPv6. The dual stack is what allows you to assign addressing for IPv4 and IPv6 concurrently, and allows the server to communicate with other hosts and clients based on what their requirements are.

Typical address types that you will use for IPv6 addressing will be the IPv6 global addresses (similar to public IPv4 addresses), IPv6 unique local addresses (similar to the private IPv4 address ranges) and IPv6 link-local addresses (similar to automatic private IP addresses in Windows Server for IPv4)

Network address translation technologies (NAT) for IPv6 exist that will allow for NAT IPv6 to IPv4 (commonly referred to as NAT64) and for NAT IPv6 to IPv6 (commonly referred to as NAT66). The existence of NAT technologies means that the five scenarios presented for Lync Server Edge Servers are still valid.

⚠**Warning:**

IPv6 is a complex topic and requires careful planning with your networking team and your Internet provider to ensure that the addresses you assign at the Windows server level and at the Lync Server 2013 level will work as expected. See the links at the end of this topic for additional resources on IPv6 addressing and planning.


Scaled Consolidated Edge Topology
using Private IP Addresses and NAT
External Firewall
Internal Firewall
TO PERIMETER
TO INTERNET
DfGw - Firewall
IPv4: 10.45.16.1
IPv6: fd04:422a:12f6:af2f::1601
Internal Firewall IP
IPv4: 172.25.33.2
IPv6:Fd2e:4d7e:288b:c94e::0332
TO CORP NET
TO PERIMETER
443,80 (optional)
Reverse Proxy External IP
IPv4 Example: 10.45.16.40
IPv6 Example:fd04:422a:12f6:af2f::1640
Reverse Proxy Internal IP
4443, 8080
IPv4 Example: 172.25.33.40
IPv6 Example:Fd2e:4d7e:288b:c94e::1240
Reverse Proxy Server
INTERNET
CORP NET
Internal Edge Services - Route
IPv4 Example: 10.45.16.10
IPv6 Example:fd04:422a:12f6:af2f::1610
443, 5061, 5269
Access Edge External IP
Lync Server 2010
Scaled Consolidated Edge (NODE 1)
IPv4 Example: 10.45.16.20
IPv6 Example:fd04:422a:12f6:af2f::1620
443
WebCon Edge External IP
IPv4 Example: 172.25.33.10
IPv6 Example:Fd2e:4d7e:288b:c94e::1233
Edge Internal IP
443, 4443, 3478, 5061, 8057, 23456, 15001, 15002, 15003
IPv4 Example: 10.45.16.30
IPv6 Example:fd04:422a:12f6:af2f::1630
443, 3478, 50,000-59,999
AV Edge External IP
Media Authentication Service
DfGw - Firewall
IPv4 Example: 10.45.16.40
IPv6 Example:fd04:422a:12f6:af2f::1640
Persistent Route – All Internal Networks
IPv4 Example: 10.45.16.11
IPv6 Example:fd04:422a:12f6:af2f::1611
443, 5061, 5269
Access Edge External IP
Lync Server 2010
Scaled Consolidated Edge (NODE 2)
IPv4 Example: 10.45.16.21
IPv6 Example:fd04:422a:12f6:af2f::1621
443
WebCon Edge External IP
IPv4 Example: 172.25.33.11
IPv6 Example:Fd2e:4d7e:288b:c94e::1234
Edge Internal IP
443, 4443, 3478, 5061, 8057, 23456, 15001, 15002, 15003
IPv4 Example: 10.45.16.31
IPv6 Example:fd04:422a:12f6:af2f::1631
443, 3478, 50,000-59,999
AV Edge External IP
A/V Authentication Service
DfGw - Firewall
IPv4 Example: 10.45.16.40
IPv6 Example:fd04:422a:12f6:af2f::1640
Persistent Route – All Internal Networks

Protocols, example IP addressing details, and server addressing are the intent of this diagram. No protocol direction is intended to be part of this diagram. Refer to the scenario Port Summary topic for detailed port and protocols.

Important:

If you are using Call Admission Control (CAC), you still must assign IPv4 addresses to the Edge Server internal interface. CAC uses IPv4 addresses and must have them available to operate.

- Certificate Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT
- Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT
- DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

⊟See Also

Other Resources

IP Version 6 Addressing Architecture
IPv6 Global Unicast Address Format
Unique Local IPv6 Unicast Addresses

1.3.9.10.3.1 Certificate Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

Certificate Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

Planning for External User Access > Scenarios for External User Access > Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT >

Topic Last Modified: *2012-09-08*

Microsoft Lync Server 2013 uses certificates to mutually authenticate other servers and to encrypt data from server to server and server to client. Certificates require name matching of the domain name system (DNS) records associated with the servers and the subject name (SN) and subject alternative name (SAN) on the certificate. To successfully map servers, DNS records and certificate entries, you must carefully plan your intended server fully qualified domain names as registered in DNS and the SN and SAN entries on the certificate.

The certificate assigned to the external interfaces of the Edge Server is requested from a public certification authority (CA). Public CAs that have demonstrated success in supplying certificates for the purposes of Unified Communications are listed in the following article: http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=929395 When requesting the certificate, you can use the certificate request generated by the Lync Server Deployment Wizard or create the request manually or by a process provided by the public CA. When assigning the certificate, the certificate is assigned to the Access Edge service interface, the Web Conferencing Edge service interface, and the Audio/Video Authentication service. The Audio/Video Authentication service should not be confused with the A/V Edge service which does not use a certificate to encrypt the audio and video streams. The internal Edge Server interface can use a certificate from an internal (to your organization) CA or a certificate from a public CA. The internal interface certificate uses only the SN and does not need or use SAN entries.

Note:

The following table shows a second SIP entry (sip.fabrikam.com) in the subject alternative name list for reference. For each SIP domain in your organization, you need to add a corresponding FQDN listed in the certificate subject alternative name list.

Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

Component	Subject name (SN)	Subject alternative names (SAN)/Order	Comments
Scaled consolidated Edge (External Edge)	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com	Certificate must be from a Public CA, and must have the server EKU and client EKU if public IM connectivity with AOL is to be deployed. Additionally, for scaled Edge Servers, the certificate private key must be exportable and the certificate and private key copied to each Edge Server. The certificate is assigned to the external Edge interfaces for: • Access Edge • Conferencing Edge • A/V Edge Note that SANs are automatically added to the certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.
Scaled consolidated Edge (Internal Edge)	lsedge.contoso.net	No SAN required	Certificate can be issued by a public or private CA, and must contain the server EKU. The certificate is assigned to the internal Edge interface.

Certificate Summary – Public Instant Messaging Connectivity

Component	Subject name	Subject alternative names (SAN)/Order	Comments
External/Access Edge	sip.contoso.com	sip.contoso.com webcon.contoso.com sip.fabrikam.com	Certificate must be from a Public CA, and must have the server EKU and client EKU if public IM connectivity with AOL is to be deployed. The certificate is assigned to the external Edge interfaces for: • Access Edge • Conferencing Edge • A/V Edge Note that SANs are

			automatically added to the certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.

Certificate Summary for Extensible Messaging and Presence Protocol

Component	**Subject name**	**Subject alternative names (SAN)/Order**	**Comments**
Assign to Access Edge service of Edge Server or Edge pool	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com xmpp.contoso.com ***.contoso.com**	The first three SAN entries are the normal SAN entries for a full Edge Server. The contoso.com is the entry required for federation with the XMPP partner at the root domain level. This entry will allow XMPP for all domains with the suffix *.contoso.com.

1.3.9.10.3.2 Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

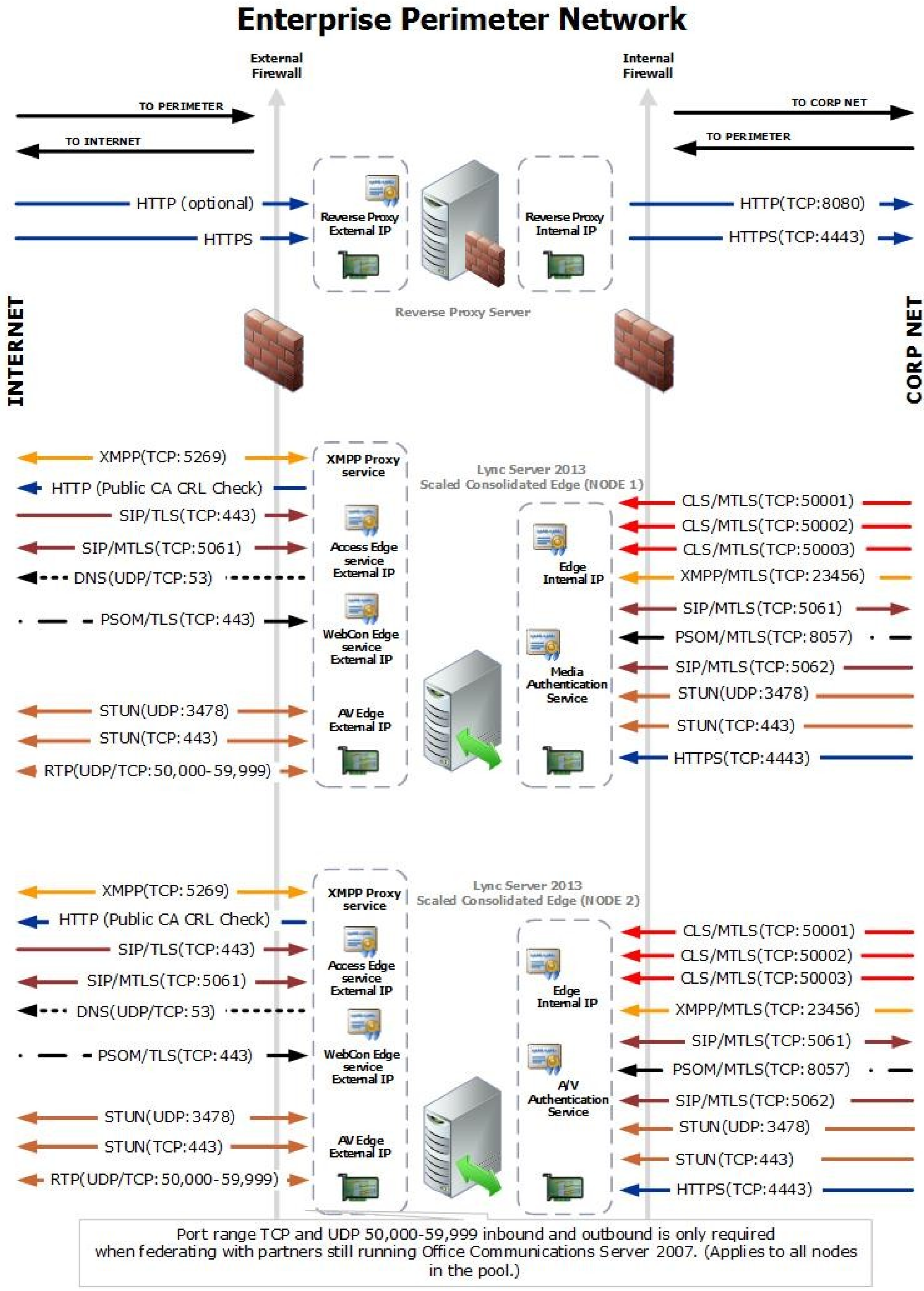
Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-12-04*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.



Port range TCP and UDP 50,000-59,999 inbound and outbound is only required when federating with partners still running Office Communications Server 2007. (Applies to all nodes in the pool.)

Port and Protocol Details

It is recommended that you open only the ports required to support the functionality for

which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bi-directionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V) and federation.

Firewall Summary for Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT: External Interface – Node 1 and Node 2 (Example)

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations
XMPP/TCP/5269	XMPP Proxy service (shares IP address with Access Edge service)	Any	XMPP Proxy service sends traffic to XMPP contacts in defined XMPP federations
Access/HTTP/TCP/80	Edge Server Access Edge service	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service	Any	DNS query over UDP
Access/SIP(TLS)/ TCP/443	Any	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Any	For federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)/TCP/443	Any	Edge Server Web Conferencing Edge service	Web Conferencing media
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-	Edge Server A/V Edge	Any	Required only for

59,999	service		federation with partners running Office Communications Server 2007.
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service	Required only for federation with partners running Office Communications Server 2007
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service	Required only for federation with partners running Office Communications Server 2007
A/V/STUN,MSTURN/UDP/3478	Edge Server A/V Edge service	Any	3478 outbound is used to determine the version of Edge Server that Lync Server is communicating with and also for media traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/UDP/3478	Any	Edge Server A/V Edge service	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/TCP/443	Any	Edge Server A/V Edge service	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/TCP/443	Edge Server A/V Edge service	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT: Internal Interface – Node 1 and Node 2 (Example)

Protocol/TCP or	Source IP address	Destination IP	Comments

UDP/Port		address	
XMPP/MTLS/TCP/23456	Any (can be defined as Front End Server address, or Front End pool IP address running the XMPP Gateway service)	Edge Server internal interface IP address	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
SIP/MTLS/TCP/5061	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Edge Server internal interface	Outbound SIP traffic (from Director, Director pool IP address, Front End Server or Front End pool IP address) to Edge Server internal interface
SIP/MTLS/TCP/5061	Edge Server internal interface	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Inbound SIP traffic (to Director, Director pool IP address, Front End Server or Front End pool IP address) from Edge Server internal interface
PSOM/MTLS/TCP/8057	Any (can be defined as Front End Server IP address, or each Front End Server IP address in a Front End pool)	Edge Server internal interface	Web conferencing traffic from Front End Server or each Front End Server if in a pool, to Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server internal interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/UDP/3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server
STUN/MSTURN/TCP/443	Any	Edge Server internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch

			Server if UDP communication cannot be established, TCP is used for file transfer and desktop sharing
HTTPS/TCP/4443	Any (can be defined as the Front End Server IP address, or pool that holds the Central Management store)	Edge Server internal interface	Replication of changes from the Central Management store to the Edge Server
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/	Access Edge service	Any	For federated and

TCP/5061	public IP address		public IM connectivity using SIP

Firewall Summary – Public Instant Messaging Connectivity

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Public IM connectivity partners	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Public IM connectivity partners	For federated and public IM connectivity using SIP
Access/SIP(TLS)/ TCP/443	Clients	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger
A/V/STUN,MSTURN/ UDP/3478	Live Messenger clients	Edge Server A/V Edge service	Required for public IM connectivity with Windows Live Messenger

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Edge Server Access Edge service interface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Edge Server Access Edge service interface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from

			the Edge Server XMPP proxy to federated XMPP partners
XMPP/MTLS/ TCP/23456	Any	Each internal Edge Server interface IP	Internal XMPP traffic from the XMPP Gateway on the Front End Server or Front End pool to the Edge Server internal IP address or each Edge pool member's internal IP address

1.3.9.10.3.3 DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-09-08*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about configuring automatic configuration of Lync 2013 clients if split-brain DNS is not configured, see the "Automatic Configuration without Split Brain DNS" section in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the single consolidated edge topology shown in the Single Consolidated Edge Topology figure. Note that certain DNS records are required only for automatic configuration of Lync 2013 clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Scaled Consolidated Edge Scenario figure in Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT, the default gateway would point to the external firewall.

You can configure two network adapters in each of your Edge Server as follows:

- **Network adapter 1 - Node 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal

interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).

- **Network adapter 1 - Node 2 (Internal Interface)**
  Internal interface with 172.25.33.11 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 Node 1 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 10.45.16.10 for Access Edge, 10.45.16.20 for Web Conferencing Edge, 10.45.16.30 for AV Edge.

  Note:

  It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge, 444/TCP for the Web Conferencing Edge and 443/TCP for the AV Edge might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

  The Access Edge public IP address is primary with default gateway set to the integrated router (10.45.16.1).
  Web conferencing and A/V Edge private IP addresses are additional IP addresses in the **Advanced** section of the properties of **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.
- **Network adapter 2 Node 2 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 10.45.16.11 for Access Edge, 10.45.16.21 for Web Conferencing Edge, 10.45.16.31 for AV Edge.
  The Access Edge public IP address is primary with default gateway set to the integrated router (10.45.16.1).
  Web conferencing and A/V Edge private IP addresses are additional IP addresses in the **Advanced** section of the properties of **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.

Tip:

Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10 and 131.107.155.11	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20 and 131.107.155.21	Web Conferencing Edge external

			interface
External DNS/A	av.contoso.com	131.107.155.30 and 131.107.155.31	A/V Edge external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface. Required for automatic DNS discovery of federated partners known as “Allowed SIP Domain” (called enhanced federation in previous releases). Repeat as necessary for all SIP domains with Lync enabled users
Internal DNS/A	lsedge.contoso.net	172.25.33.10 and 172.25.33.11	Consolidated Edge internal interface

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge external interface Required for automatic DNS discovery of your federation to other potential federation partners, and is known as “Allowed SIP Domains” (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users ◆**Important:** This SRV record is required for mobility and the push

			notification clearing house

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat as necessary for all internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An allowed XMPP domain must also be configured in the XMPP Federated Partners policy. See topics in **See Also** for additional details
External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP proxy	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service. Typically, the SRV record that you create will point to

			this host (A or AAAA) record

1.3.9.10.4 Scaled Consolidated Edge, DNS Load Balancing w ith Public IP Addresses

Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2012-09-08*

In the Edge Server pool topology, two or more Edge Servers are deployed as a load-balanced pool in the perimeter network of the data center. Domain Name System (DNS) load balancing is used for traffic to both the external and internal Edge interfaces.

If your organization requires support for more than 15,000 Access Edge service client connections, 1,000 active Lync Server Web Conferencing service client connections, or 500 concurrent A/V Edge sessions, and/or high availability of the Edge Server is important, this topology offers the advantages of scalability and failover support.

The figure does not show Directors, an optional server role deployed in the internal network between the Edge Servers and your Front End pools or server. For details about the topology for Directors, see Components Required for the Director. The figure represents a single reverse proxy.

Note:

The figure shown is for orientation and example IP addressing, but does not intend to represent actual communication flows with the correct incoming and outgoing traffic. The figure represents a high level view of possible traffic. Details for traffic flow as they pertain to incoming (to listening ports) and outgoing (to destination servers or clients) is represented in the Port Summary diagram in each scenario. For example, TCP 443 is actually inbound (to the Edge or reverse proxy) only, and is only a two-way flow from a protocol (TCP) perspective. Additionally, the figure shows the nature of traffic as it changes when NAT (network address translation) occurs (destination address is changed on inbound, source address is changed on outbound). Example external and internal firewall, and server interfaces are shown for reference purposes only. Finally, example default gateway and route relationships are shown, where applicable. Note also that the diagram uses the *.com* DNS zone to represent the external DNS zone for both reverse proxy and Edge Servers, and the *.net* DNS zone refers to the internal DNS zone.

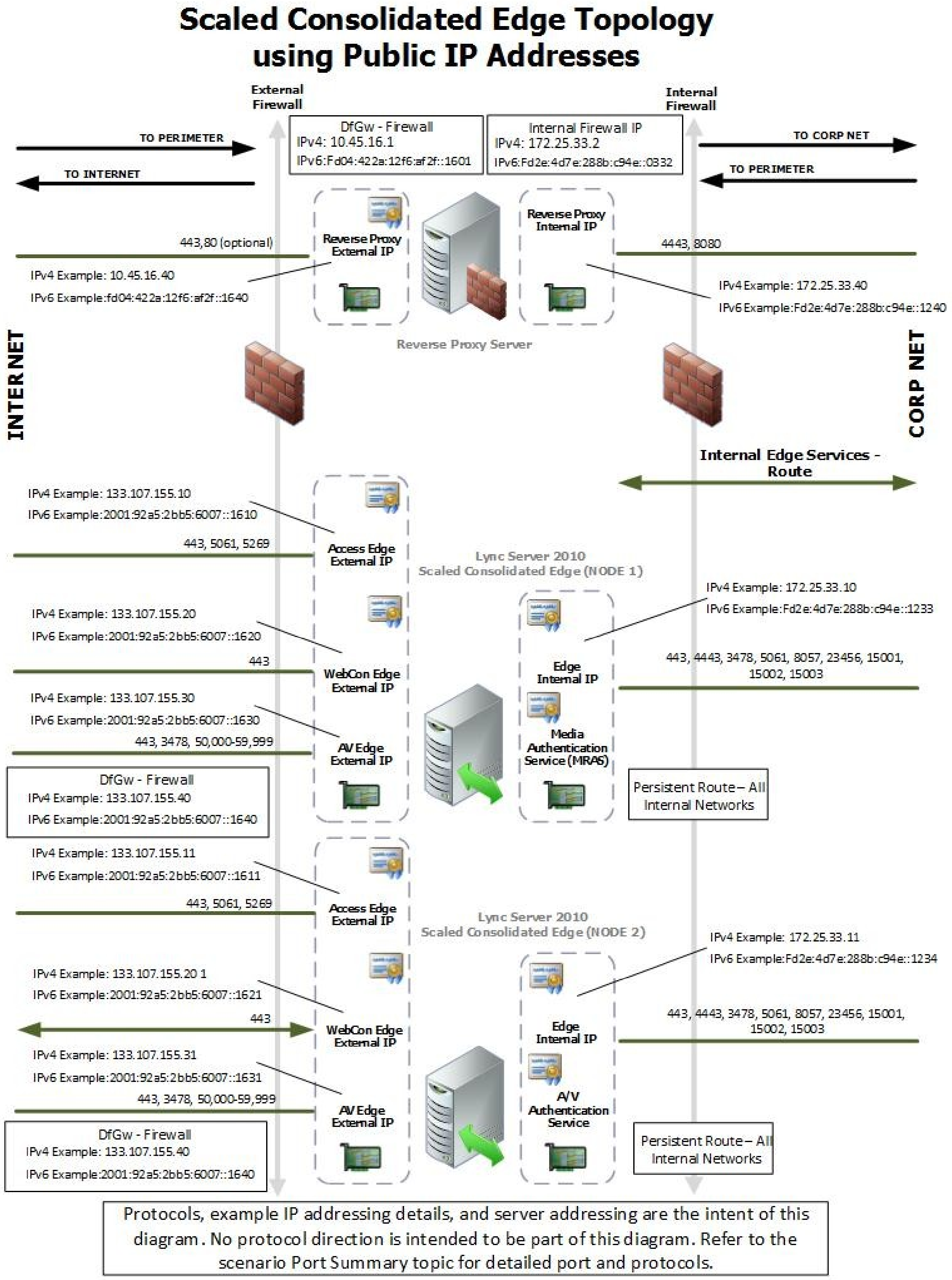
New to Microsoft Lync Server 2013 is support for IPv6 addressing. Much like IPv4 addressing, IPv6 addresses must be assigned in such a way that the addresses are part of your assigned IPv6 address space. The addresses in this topic are for example only. You must acquire IPv6 addresses that will function in your deployment, provide the correct scope and will interoperate with internal and external addressing. Windows Server provides a feature that is important to transitional IPv6 operation and IPv4 to IPv6 communication called the *dual stack*. The dual stack is a separate and distinct network stack for IPv4 and for IPv6. The dual stack is what allows you to assign addressing for IPv4 and IPv6 concurrently, and allows the server to communicate with other hosts and clients based on what their requirements are.

Typical address types that you will use for IPv6 addressing will be the IPv6 global addresses (similar to public IPv4 addresses), IPv6 unique local addresses (similar to the private IPv4 address ranges) and IPv6 link-local addresses (similar to automatic private IP addresses in Windows Server for IPv4)

Network address translation technologies (NAT) for IPv6 exist that will allow for NAT IPv6 to IPv4 (commonly referred to as NAT64) and for NAT IPv6 to IPv6 (commonly referred to as NAT66). The existence of NAT technologies means that the five scenarios presented for Lync Server Edge Servers are still valid.

⚠ **Warning:**

IPv6 is a complex topic and requires careful planning with your networking team and your Internet provider to ensure that the addresses you assign at the Windows server level and at the Lync Server 2013 level will work as expected. See the links at the end of this topic for additional resources on IPv6 addressing and planning.


Scaled Consolidated Edge Topology
using Public IP Addresses
External Firewall
Internal Firewall
DfGw - Firewall
IPv4: 10.45.16.1
IPv6:Fd04:422a:12f6:af2f::1601
Internal Firewall IP
IPv4: 172.25.33.2
IPv6:Fd2e:4d7e:288b:c94e::0332
TO PERIMETER
TO INTERNET
TO CORP NET
TO PERIMETER
443,80 (optional)
IPv4 Example: 10.45.16.40
IPv6 Example:fd04:422a:12f6:af2f::1640
Reverse Proxy External IP
Reverse Proxy Internal IP
4443, 8080
IPv4 Example: 172.25.33.40
IPv6 Example:Fd2e:4d7e:288b:c94e::1240
Reverse Proxy Server
INTERNET
CORP NET
Internal Edge Services - Route
IPv4 Example: 133.107.155.10
IPv6 Example:2001:92a5:2bb5:6007::1610
443, 5061, 5269
Access Edge External IP
Lync Server 2010
Scaled Consolidated Edge (NODE 1)
IPv4 Example: 172.25.33.10
IPv6 Example:Fd2e:4d7e:288b:c94e::1233
IPv4 Example: 133.107.155.20
IPv6 Example:2001:92a5:2bb5:6007::1620
443
WebCon Edge External IP
Edge Internal IP
443, 4443, 3478, 5061, 8057, 23456, 15001, 15002, 15003
IPv4 Example: 133.107.155.30
IPv6 Example:2001:92a5:2bb5:6007::1630
443, 3478, 50,000-59,999
AV Edge External IP
Media Authentication Service (MRAS)
DfGw - Firewall
IPv4 Example: 133.107.155.40
IPv6 Example:2001:92a5:2bb5:6007::1640
Persistent Route – All Internal Networks
IPv4 Example: 133.107.155.11
IPv6 Example:2001:92a5:2bb5:6007::1611
443, 5061, 5269
Access Edge External IP
Lync Server 2010
Scaled Consolidated Edge (NODE 2)
IPv4 Example: 172.25.33.11
IPv6 Example:Fd2e:4d7e:288b:c94e::1234
IPv4 Example: 133.107.155.20 1
IPv6 Example:2001:92a5:2bb5:6007::1621
443
WebCon Edge External IP
Edge Internal IP
443, 4443, 3478, 5061, 8057, 23456, 15001, 15002, 15003
IPv4 Example: 133.107.155.31
IPv6 Example:2001:92a5:2bb5:6007::1631
443, 3478, 50,000-59,999
AV Edge External IP
A/V Authentication Service
DfGw - Firewall
IPv4 Example: 133.107.155.40
IPv6 Example:2001:92a5:2bb5:6007::1640
Persistent Route – All Internal Networks
Protocols, example IP addressing details, and server addressing are the intent of this diagram. No protocol direction is intended to be part of this diagram. Refer to the scenario Port Summary topic for detailed port and protocols.

Important:

If you are using Call Admission Control (CAC), you still must assign IPv4 addresses to the Edge Server internal interface. CAC uses IPv4 addresses and must have them available to operate.

- Certificate Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses
- Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses
- DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

⊟See Also

Other Resources

IP Version 6 Addressing Architecture
IPv6 Global Unicast Address Format
Unique Local IPv6 Unicast Addresses

1.3.9.10.4.1 Certificate Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

Certificate Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

Planning for External User Access > Scenarios for External User Access > Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses >

Topic Last Modified: *2012-09-08*

Microsoft Lync Server 2013 uses certificates to mutually authenticate other servers and to encrypt data from server to server and server to client. Certificates require name matching of the domain name system (DNS) records associated with the servers and the subject name (SN) and subject alternative name (SAN) on the certificate. To successfully map servers, DNS records and certificate entries, you must carefully plan your intended server fully qualified domain names as registered in DNS and the SN and SAN entries on the certificate.

The certificate assigned to the external interfaces of the Edge Server is requested from a public certification authority (CA). Public CAs that have demonstrated success in supplying certificates for the purposes of Unified Communications are listed in the following article: http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=929395 When requesting the certificate, you can use the certificate request generated by the Lync Server Deployment Wizard or create the request manually or by a process provided by the public CA. When assigning the certificate, the certificate is assigned to the Access Edge service interface, the Web Conferencing Edge service interface, and the Audio/Video Authentication service. The Audio/Video Authentication service should not be confused with the A/V Edge service which does not use a certificate to encrypt the audio and video streams. The internal Edge Server interface can use a certificate from an internal (to your organization) CA or a certificate from a public CA. The internal interface certificate uses only the SN and does not need or use SAN entries.

Note:

The following table shows a second SIP entry (sip.fabrikam.com) in the subject alternative name list for reference. For each SIP domain in your organization, you need to add a corresponding FQDN listed in the certificate subject alternative name list.

Scaled Consolidated Edge using DNS Load Balancing with Public IP Addresses

Component	Subject name	Subject	Comments

		alternative names (SAN)/Order	
Scaled consolidated Edge (External Edge)	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com	Certificate must be from a Public CA, and must have the server EKU and client EKU if public IM connectivity with AOL is to be deployed. Additionally, for scaled Edge Servers, the certificate private key must be exportable and the certificate and private key copied to each Edge Server. The certificate is assigned to the external Edge interfaces for: • Access Edge • Conferencing Edge • A/V Edge Note that SANs are automatically added to the certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.
Scaled consolidated Edge (Internal Edge)	lsedge.contoso.net	No SAN required	Certificate can be issued by a public or private CA, and must contain the server EKU. The certificate is assigned to the internal Edge interface.

Certificate Summary – Public Instant Messaging Connectivity

Component	Subject name	Subject alternative names (SAN)/Order	Comments
External/Access Edge	sip.contoso.com	sip.contoso.com webcon.contoso.com sip.fabrikam.com	Certificate must be from a Public CA, and must have the server EKU and client EKU if public IM connectivity with AOL is to be deployed. The certificate is assigned to the external Edge interfaces for: • Access Edge • Conferencing Edge • A/V Edge Note that SANs are automatically added to the

			certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.

Certificate Summary for Extensible Messaging and Presence Protocol

Component	**Subject name**	**Subject alternative names (SAN)/Order**	**Comments**
Assign to Access Edge service of Edge Server or Edge pool	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com xmpp.contoso.com ***.contoso.com**	The first three SAN entries are the normal SAN entries for a full Edge Server. The contoso.com is the entry required for federation with the XMPP partner at the root domain level. This entry will allow XMPP for all domains with the suffix *.contoso.com.

1.3.9.10.4.2 Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

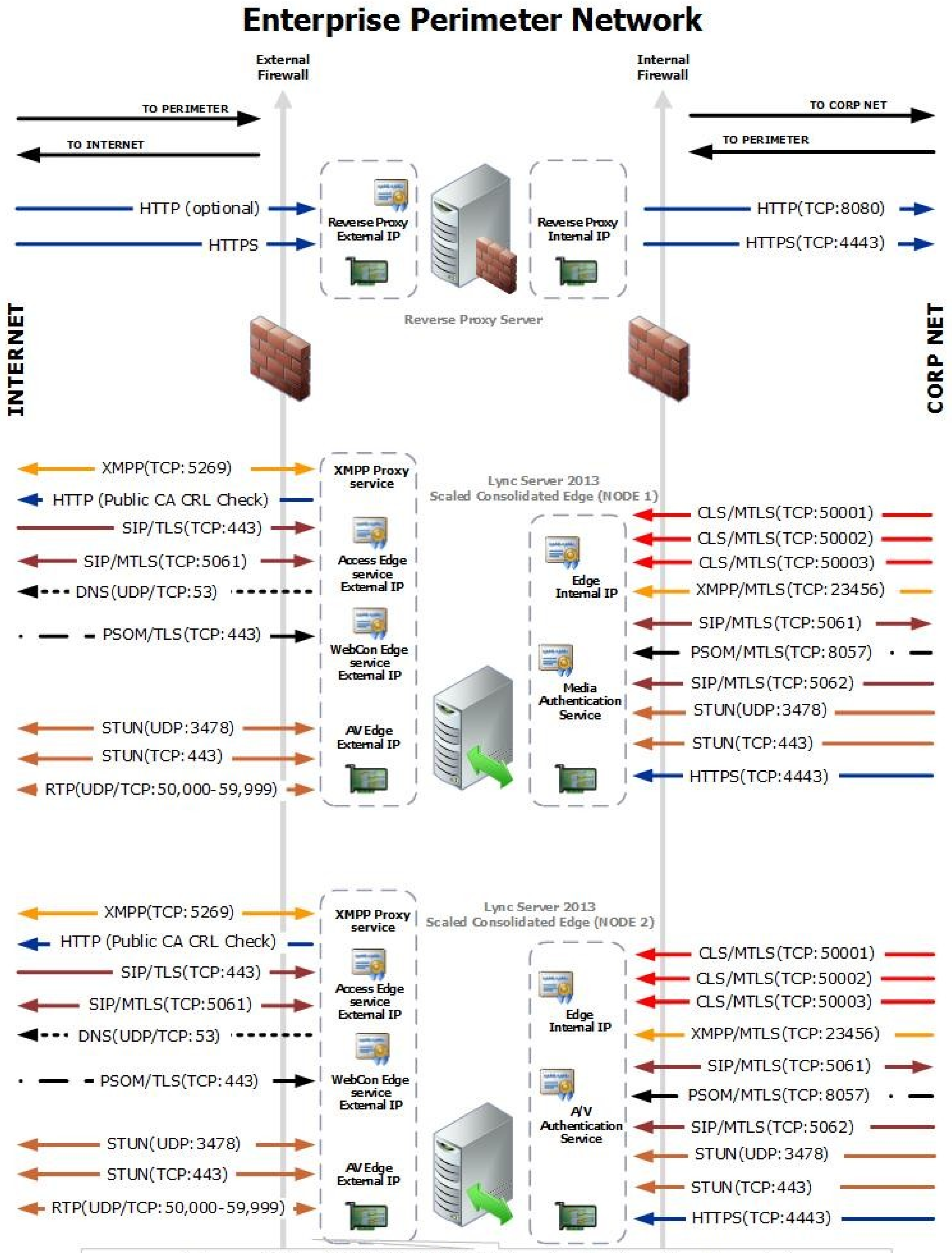
Port Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-12-04*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.



Port range TCP and UDP 50,000-59,999 inbound and outbound is only required when federating with partners still running Office Communications Server 2007. (Applies to all nodes in the pool.)

Port and Protocol Details

It is recommended that you open only the ports required to support the functionality for

which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bi-directionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V) and federation.

Firewall Summary for Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses: External Interface – Node 1 and Node 2 (Example)

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations
Access/HTTP/TCP/80	Edge Server Access Edge service public IP address	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service public IP address	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service public IP address	Any	DNS query over UDP
Access/SIP(TLS)/ TCP/443	Any	Edge Server Access Edge service public IP address	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Edge Server Access Edge service public IP address	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service public IP address	Any	For federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)TCP/443	Any	Edge Server Web Conferencing Edge service public IP address	Web Conferencing media
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service public IP address	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-59,999	Edge Server A/V Edge service public IP	Any	Required only for federation with

	address		partners running Office Communications Server 2007.
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service public IP address	Any	3478 outbound is used to determine the version of Edge Server that Lync Server is communicating with and also for media traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/ UDP/3478	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/ TCP/443	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/ TCP/443	Edge Server A/V Edge service	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses: Internal Interface – Node 1 and Node 2 (Example)

Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Comments

XMPP/MTLS/TCP/23456	Any (can be defined as Front End Server address, or Front End pool IP address running the XMPP Gateway service)	Edge Server internal interface	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
SIP/MTLS/TCP/5061	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Edge Server internal interface	Outbound SIP traffic (from Director, Director pool IP address, Front End Server or Front End pool IP address) to Edge Server internal interface
SIP/MTLS/TCP/5061	Edge Server internal interface	Any (can be defined as Director, Director pool IP address, Front End Server or Front End pool IP address)	Inbound SIP traffic (to Director, Director pool IP address, Front End Server or Front End pool IP address) from Edge Server internal interface
PSOM/MTLS/TCP/8057	Any (can be defined as Front End Server IP address, or each Front End Server IP address in a Front End pool)	Edge Server internal interface	Web conferencing traffic from Front End Server or each Front End Server if in a pool, to Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server internal interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/UDP/3478	Any	Edge Server internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server
STUN/MSTURN/TCP/443	Any	Edge Server internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server if UDP

			communication cannot be established, TCP is used for file transfer and desktop sharing
HTTPS/TCP/4443	Any (can be defined as the Front End Server IP address, or pool that holds the Central Management store)	Edge Server internal interface	Replication of changes from the Central Management store to the Edge Server
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Access Edge service public IP address	Any	For federated and public IM connectivity

			using SIP

Firewall Summary – Public Instant Messaging Connectivity

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Public IM connectivity partners	Edge Server Access Edge service	For federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Access Edge service	Public IM connectivity partners	For federated and public IM connectivity using SIP
Access/SIP(TLS)/ TCP/443	Clients	Edge Server Access Edge service	Client-to-server SIP traffic for external user access
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger
A/V/STUN,MSTURN/ UDP/3478	Live Messenger clients	Edge Server A/V Edge service	Required for public IM connectivity with Windows Live Messenger

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Edge Server Access Edge serviceinterface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Edge Server Access Edge serviceinterface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from the Edge Server XMPP

			proxy to federated XMPP partners
XMPP/MTLS/ TCP/23456	Any	Each internal Edge Server Interface IP	Internal XMPP traffic from the XMPP Gateway on the Front End Server or Front End pool to the Edge Server internal IP address or each Edge pool member's internal IP address

1.3.9.10.4.3 DNS Summary - Scaled Consolidated Edge, DNS Load Balancing w ith Public IP Addresses

DNS Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-10-20*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about configuring automatic configuration of Lync 2013 clients if split-brain DNS is not configured, see the "Automatic Configuration without Split Brain DNS" section in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the single consolidated edge topology shown in the Single Consolidated Edge Topology figure. Note that certain DNS records are required only for automatic configuration of Lync 2013 clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Scaled Consolidated Edge Scenario figure in Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses , the default gateway would point to the external firewall.

You can configure two network adapters in each of your Edge Server as follows:

- **Network adapter 1 - Node 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or

Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).

- **Network adapter 1 - Node 2 (Internal Interface)**
  Internal interface with 172.25.33.11 assigned.
  No default gateway is defined.
  Ensure that there is a route from the network containing the Edge internal interface to any networks that contain servers running Lync Server 2013 or Lync Server 2013 clients (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 Node 1 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 131.107.155.10 for Access Edge service, 131.107.155.20 for Web Conferencing Edge service, 131.107.155.30 for A/V Edge service.
  The Access Edge service public IP address is primary with default gateway set to the public router (131.107.155.1).
  Web Conferencing Edge service and A/V Edge service private IP addresses are additional IP addresses in the **Advanced** section of the properties of **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.

  Note:
  It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge service, 444/TCP for the Web Conferencing Edge service and 443/TCP for the A/V Edge service might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

- **Network adapter 2 Node 2 (External Interface)**
  Three private IP addresses are assigned to this network adapter, for example 131.107.155.11 for Access Edge service, 131.107.155.21 for Web Conferencing Edge service, 131.107.155.31 for A/V Edge service.
  The Access Edge service public IP address is primary with default gateway set to the public router (131.107.155.1).
  Web Conferencing Edge service and A/V Edge service private IP addresses are additional IP addresses in the **Advanced** section of the properties of **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** of the **Local Area Connection Properties** in Windows Server.

Tip:
Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10 and 131.107.155.11	Access Edge service external interface (Contoso) Repeat as necessary for all SIP domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20 and 131.107.155.21	Web Conferencing Edge service external

			interface
External DNS/A	av.contoso.com	131.107.155.30 and 131.107.155.31	A/V Edge service external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge service external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	Access Edge service external interface Required for automatic DNS discovery of federated partners known as “Allowed SIP Domain” (called enhanced federation in previous releases). Repeat as necessary for all SIP domains with Lync enabled users
Internal DNS/A	lsedge.contoso.net	172.25.33.10 and 172.25.33.11	Consolidated Edge internal interface

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	SIP Access Edge service external interface Required for automatic DNS discovery of your federation to other potential federation partners, and is known as “Allowed SIP Domains” (called enhanced federation in previous releases). **◆Important:** Repeat as necessary for all SIP domains with Lync enabled users and Microsoft Lync Mobile clients

			that use either the Push Notification Service or the Apple Push Notification service

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge service external interface (Contoso)Repeat as necessary for all SIP domains with Lync enabled users

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat as necessary for all internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An allowed XMPP domain must also be configured in the XMPP Federated Partners policy. See topics in **See Also** for additional details
External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service.

		proxy	Typically, the SRV record that you create will point to this host (A or AAAA) record

1.3.9.10.5 Scaled Consolidated Edge with Hardware Load Balancers

Scaled Consolidated Edge with Hardware Load Balancers

See Also

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2012-10-21*

In the Edge pool topology, two or more Edge Servers are deployed as a load-balanced pool in the perimeter network of the data center. Hardware load balancing is used for traffic to both the external and internal Edge Server interfaces.

If your organization requires support for more than 15,000 Access Edge service client connections, 1,000 active Web Conferencing Edge service client connections, or 500 concurrent A/V Edge service sessions, and high availability of the Edge Server is important, this topology offers the advantages of scalability and failover support.

The figure does not show Directors, an optional server role deployed in the internal network between the Edge Servers and your Front End pools or server. . For details about the topology for Directors, see Components Required for the Director.

Note:

The figure shown is for orientation and example IP addressing, but does not intend to represent actual communication flows with the correct incoming and outgoing traffic. The figure represents a high level view of possible traffic. Details for traffic flow as they pertain to incoming (to listening ports) and outgoing (to destination servers or clients) is represented in the Port Summary diagram in each scenario. For example, TCP 443 is actually inbound (to the Edge Server or reverse proxy) only, and is only a two-way flow from a protocol (TCP) perspective. Additionally, the figure shows the nature of traffic as it changes when NAT (network address translation) occurs (destination address is changed on inbound, source address is changed on outbound). Example external and internal firewall, and server interfaces are shown for reference purposes only. Finally, example default gateway and route relationships are shown, where applicable. Note also that the diagram uses the *.com* DNS zone to represent the external DNS zone for both reverse proxy and Edge Servers, and the *.net* DNS zone refers to the internal DNS zone.

New to Microsoft Lync Server 2013 is support for IPv6 addressing. Much like IPv4 addressing, IPv6 addresses must be assigned in such a way that the addresses are part of your assigned IPv6 address space. The addresses in this topic are for example only. You must acquire IPv6 addresses that will function in your deployment, provide the correct scope and will interoperate with internal and external addressing. Windows Server provides a feature that is important to transitional IPv6 operation and IPv4 to IPv6 communication called the *dual stack*. The dual stack is a separate and distinct network stack for IPv4 and for IPv6. The dual stack is what allows you to assign addressing for IPv4 and IPv6 concurrently, and allows the server to communicate with other hosts and clients based on what their requirements are.

Typical address types that you will use for IPv6 addressing will be the IPv6 global addresses (similar to public IPv4 addresses), IPv6 unique local addresses (similar to the private IPv4 address ranges) and IPv6 link-local addresses (similar to automatic private IP addresses in Windows Server for IPv4)

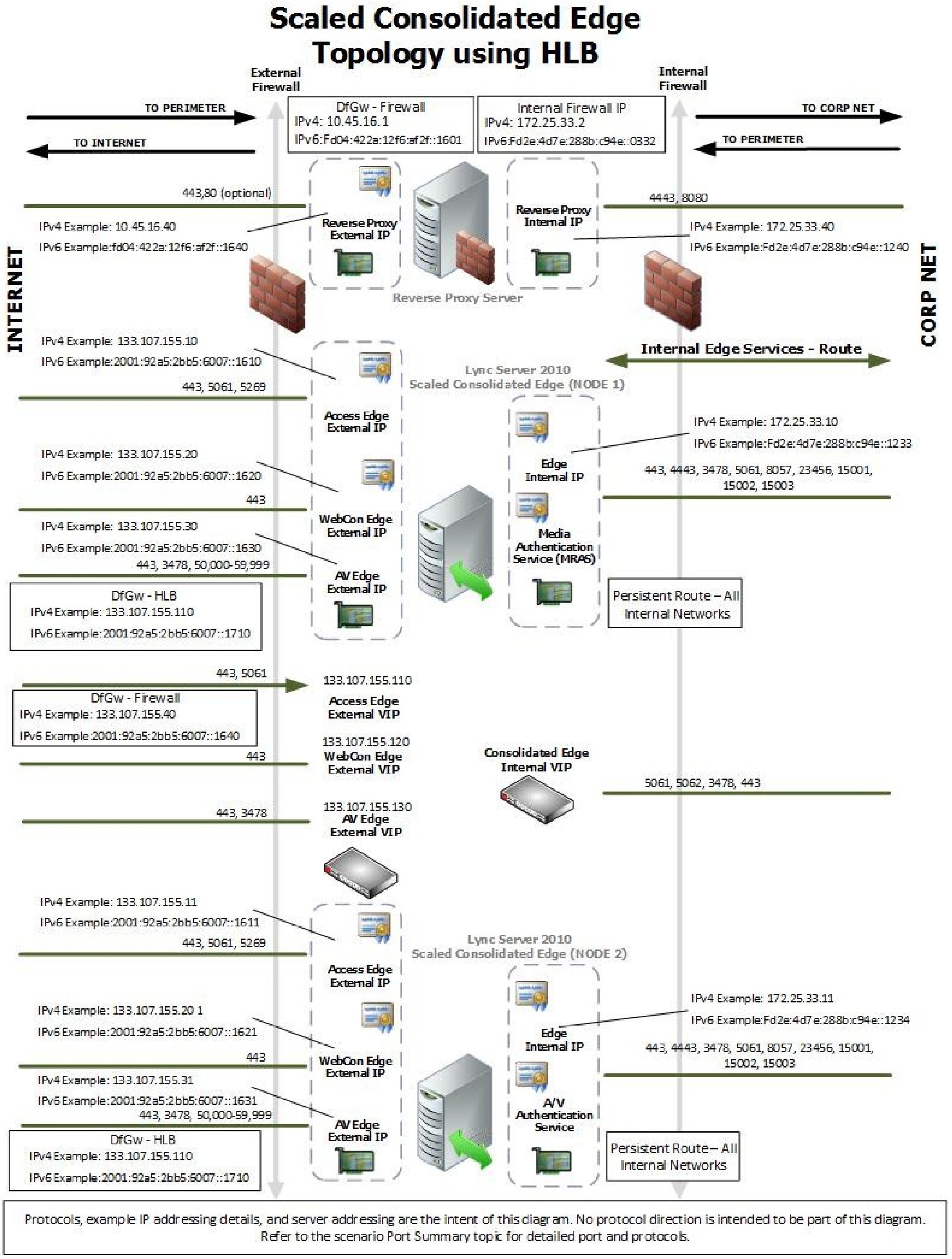
Network address translation technologies (NAT) for IPv6 exist that will allow for NAT IPv6 to IPv4 (commonly referred to as NAT64) and for NAT IPv6 to IPv6 (commonly referred to as NAT66). The existence of NAT technologies means that the five scenarios presented for Lync Server Edge Servers are still valid.

⚠**Warning:**

IPv6 is a complex topic and requires careful planning with your networking team and your Internet provider to ensure that the addresses you assign at the Windows server level and at the Lync Server 2013 level will work as expected. See the links at the end of this topic for additional resources on IPv6 addressing and planning.

Hardware Load Balancer Configuration

For details, see the “Hardware Load Balancer Requirements for A/V Edge” section in Components Required for External User Access.



Scaled Consolidated Edge Topology using HLB

External Firewall
Internal Firewall
TO PERIMETER
TO INTERNET
DfGw - Firewall
IPv4: 10.45.16.1
IPv6:Fd04:422a:12f6:af2f::1601
Internal Firewall IP
IPv4: 172.25.33.2
IPv6:Fd2e:4d7e:288b:c94e::0332
TO CORP NET
TO PERIMETER
443,80 (optional)
IPv4 Example: 10.45.16.40
IPv6 Example:fd04:422a:12f6:af2f::1640
Reverse Proxy External IP
Reverse Proxy Internal IP
Reverse Proxy Server
4443, 8080
IPv4 Example: 172.25.33.40
IPv6 Example:Fd2e:4d7e:288b:c94e::1240
INTERNET
CORP NET
IPv4 Example: 133.107.155.10
IPv6 Example:2001:92a5:2bb5:6007::1610
443, 5061, 5269
Access Edge External IP
Lync Server 2010 Scaled Consolidated Edge (NODE 1)
Internal Edge Services - Route
IPv4 Example: 172.25.33.10
IPv6 Example:Fd2e:4d7e:288b:c94e::1233
Edge Internal IP
443, 4443, 3478, 5061, 8057, 23456, 15001, 15002, 15003
IPv4 Example: 133.107.155.20
IPv6 Example:2001:92a5:2bb5:6007::1620
443
WebCon Edge External IP
IPv4 Example: 133.107.155.30
IPv6 Example:2001:92a5:2bb5:6007::1630
443, 3478, 50,000-59,999
AV Edge External IP
Media Authentication Service (MRAS)
DfGw - HLB
IPv4 Example: 133.107.155.110
IPv6 Example:2001:92a5:2bb5:6007::1710
Persistent Route – All Internal Networks
443, 5061
DfGw - Firewall
IPv4 Example: 133.107.155.40
IPv6 Example:2001:92a5:2bb5:6007::1640
133.107.155.110
Access Edge External VIP
443
133.107.155.120
WebCon Edge External VIP
Consolidated Edge Internal VIP
5061, 5062, 3478, 443
443, 3478
133.107.155.130
AV Edge External VIP
IPv4 Example: 133.107.155.11
IPv6 Example:2001:92a5:2bb5:6007::1611
443, 5061, 5269
Access Edge External IP
Lync Server 2010 Scaled Consolidated Edge (NODE 2)
IPv4 Example: 172.25.33.11
IPv6 Example:Fd2e:4d7e:288b:c94e::1234
Edge Internal IP
443, 4443, 3478, 5061, 8057, 23456, 15001, 15002, 15003
IPv4 Example: 133.107.155.20 1
IPv6 Example:2001:92a5:2bb5:6007::1621
443
WebCon Edge External IP
IPv4 Example: 133.107.155.31
IPv6 Example:2001:92a5:2bb5:6007::1631
443, 3478, 50,000-59,999
AV Edge External IP
A/V Authentication Service
DfGw - HLB
IPv4 Example: 133.107.155.110
IPv6 Example:2001:92a5:2bb5:6007::1710
Persistent Route – All Internal Networks

Protocols, example IP addressing details, and server addressing are the intent of this diagram. No protocol direction is intended to be part of this diagram. Refer to the scenario Port Summary topic for detailed port and protocols.

◆Important:

If you are using Call Admission Control (CAC), you still must assign IPv4 addresses to the Edge Server internal interface. CAC uses IPv4 addresses and must have them available to operate.

- Certificate Summary - Scaled Consolidated Edge with Hardware Load Balancers

- Port Summary - Scaled Consolidated Edge with Hardware Load Balancers
- DNS Summary - Scaled Consolidated Edge with Hardware Load Balancers

⊟See Also

Other Resources

IP Version 6 Addressing Architecture
IPv6 Global Unicast Address Format
Unique Local IPv6 Unicast Addresses

1.3.9.10.5.1 Certificate Summary - Scaled Consolidated Edge with Hardware Load Balancers

Certificate Summary - Scaled Consolidated Edge with Hardware Load Balancers

Planning for External User Access > Scenarios for External User Access > Scaled Consolidated Edge with Hardware Load Balancers >

Topic Last Modified: *2012-10-22*

Microsoft Lync Server 2013 uses certificates to mutually authenticate other servers and to encrypt data from server to server and server to client. Certificates require name matching of the domain name system (DNS) records associated with the servers and the subject name (SN) and subject alternative name (SAN) on the certificate. To successfully map servers, DNS records and certificate entries, you must carefully plan your intended server fully qualified domain names as registered in DNS and the SN and SAN entries on the certificate.

The certificate assigned to the external interfaces of the Edge Server is requested from a public certification authority (CA). Public CAs that have demonstrated success in supplying certificates for the purposes of Unified Communications are listed in the following article: http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=929395. When requesting the certificate, you can use the certificate request generated by the Lync Server Deployment Wizard or create the request manually or by a process provided by the public CA. When assigning the certificate, the certificate is assigned to the Access Edge service interface, the Web Conferencing Edge service interface, and the Audio/Video Authentication service. The Audio/Video Authentication service should not be confused with the A/V Edge service, which does not use a certificate to encrypt the audio and video streams. The internal Edge Server interface can use a certificate from an internal (to your organization) CA or a certificate from a public CA. The internal interface certificate uses only the SN and does not need or use SAN entries.

Note:
The following table shows a second SIP entry (sip.fabrikam.com) in the subject alternative name list for reference. For each SIP domain in your organization, you need to add a corresponding FQDN listed in the certificate subject alternative name list.

Certificates Required for Scaled Consolidated Edge with Hardware Load Balancers

Component	Subject name	Subject alternative names (SAN)/Order	Comments
Single	sip.contoso.com	webcon.contoso.com	Certificate must be from a Public CA, and must have the server

consolidated Edge Server (External Edge)		sip.contoso.com sip.fabrikam.com	EKU and client EKU if public IM connectivity with AOL is to be deployed. Additionally, for scaled Edge Servers, the certificate private key must be exportable and the certificate and private key copied to each Edge Server.The certificate is assigned to the external Edge interfaces for: • Access Edge service • Web Conferencing Edge service • A/V Edge service Note that SANs are automatically added to the certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.
Single consolidated Edge Server (Internal Edge)	lsedge.contoso.net	No SAN required	Certificate can be issued by a public or private CA, and must contain the server EKU. The certificate is assigned to the internal Edge Server interface.

Certificate Summary – Public Instant Messaging Connectivity

Component	Subject name	Subject alternative names (SAN)/Order	Comments
External/Access Edge service	sip.contoso.com	sip.contoso.com webcon.contoso.com sip.fabrikam.com	Certificate must be from a Public CA, and must have the server EKU and client EKU if public IM connectivity with AOL is to be deployed. The certificate is assigned to the external Edge interfaces for: • Access Edge service • Web Conferencing Edge service • A/V Edge service Note that SANs are automatically added to the certificate based on your definitions in Topology Builder.

			You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.

Certificate Summary for Extensible Messaging and Presence Protocol

Component	Subject name	Subject alternative names (SAN)/Order	Comments
Assign to Access Edge service of Edge Server or Edge pool	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com xmpp.contoso.com ***.contoso.com**	The first three SAN entries are the normal SAN entries for a full Edge Server. The contoso.com is the entry required for federation with the XMPP partner at the root domain level. This entry will allow XMPP for all domains with the suffix *.contoso.com.

1.3.9.10.5.2 Port Summary - Scaled Consolidated Edge w ith Hardw are Load Balancers

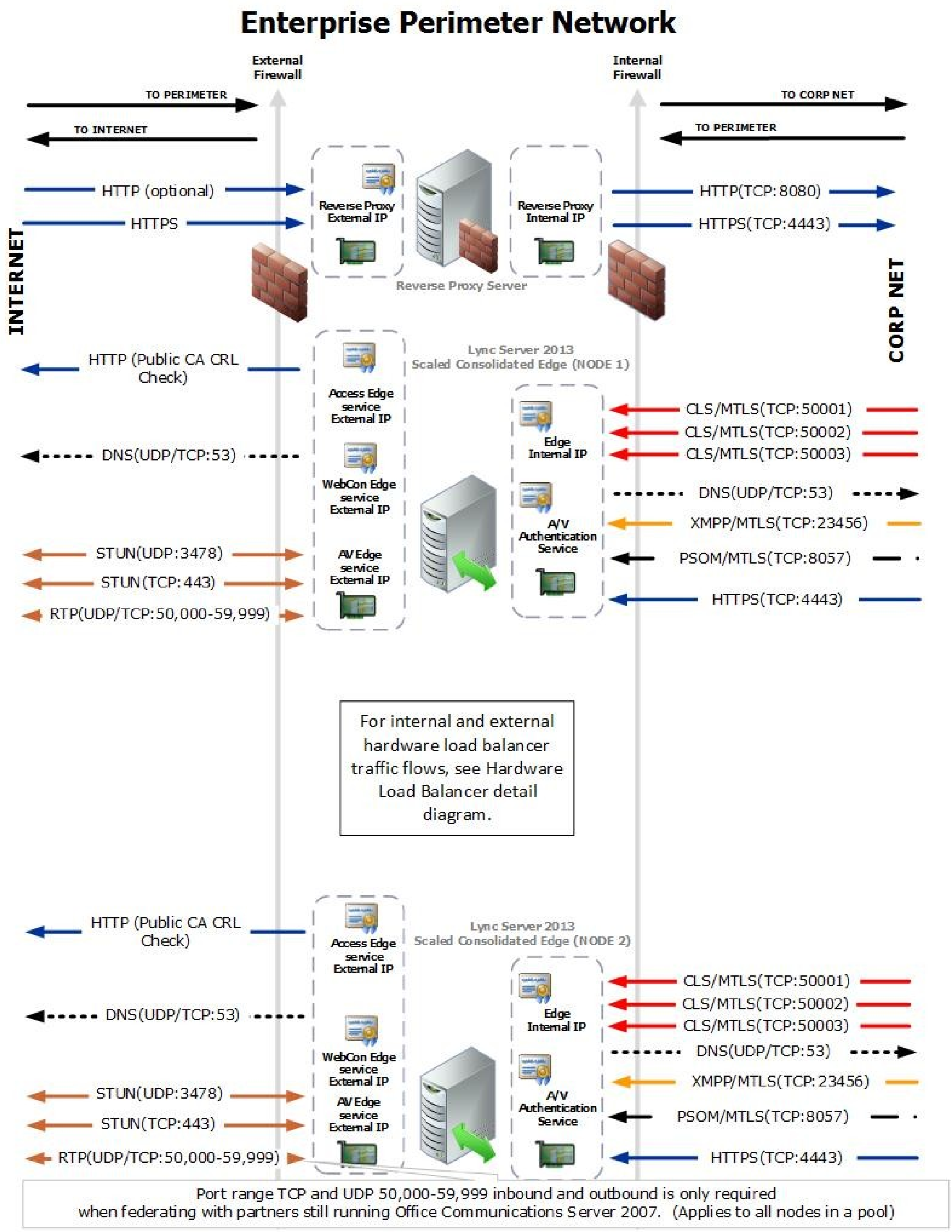
Port Summary - Scaled Consolidated Edge with Hardware Load Balancers

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-12-04*

The Lync Server 2013, Edge Server functionality described in this scenario architecture is very similar to what was implemented in Lync Server 2010. The most noticeable addition is the port **5269 over TCP** entry for the extensible messaging and presence protocol (XMPP). Lync Server 2013 optionally deploys an XMPP proxy on the Edge Server or Edge pool and the XMPP gateway server on the Front End Server or Front End pool.

In addition to IPv4, the Edge Server now supports IPv6. For clarity, only IPv4 is used in the scenarios.


Enterprise Perimeter Network
External Firewall
Internal Firewall
TO PERIMETER
TO INTERNET
TO CORP NET
TO PERIMETER
INTERNET
CORP NET
HTTP (optional)
HTTPS
Reverse Proxy External IP
Reverse Proxy Internal IP
Reverse Proxy Server
HTTP(TCP:8080)
HTTPS(TCP:4443)
Lync Server 2013
Scaled Consolidated Edge (NODE 1)
HTTP (Public CA CRL Check)
Access Edge service External IP
DNS(UDP/TCP:53)
WebCon Edge service External IP
STUN(UDP:3478)
STUN(TCP:443)
RTP(UDP/TCP:50,000-59,999)
AV Edge service External IP
Edge Internal IP
A/V Authentication Service
CLS/MTLS(TCP:50001)
CLS/MTLS(TCP:50002)
CLS/MTLS(TCP:50003)
DNS(UDP/TCP:53)
XMPP/MTLS(TCP:23456)
PSOM/MTLS(TCP:8057)
HTTPS(TCP:4443)
For internal and external hardware load balancer traffic flows, see Hardware Load Balancer detail diagram.
Lync Server 2013
Scaled Consolidated Edge (NODE 2)
HTTP (Public CA CRL Check)
Access Edge service External IP
DNS(UDP/TCP:53)
WebCon Edge service External IP
AV Edge service External IP
STUN(UDP:3478)
STUN(TCP:443)
RTP(UDP/TCP:50,000-59,999)
Edge Internal IP
A/V Authentication Service
CLS/MTLS(TCP:50001)
CLS/MTLS(TCP:50002)
CLS/MTLS(TCP:50003)
DNS(UDP/TCP:53)
XMPP/MTLS(TCP:23456)
PSOM/MTLS(TCP:8057)
HTTPS(TCP:4443)

Port range TCP and UDP 50,000-59,999 inbound and outbound is only required when federating with partners still running Office Communications Server 2007. (Applies to all nodes in a pool)

Port and Protocol Details

It is recommended that you open only the ports required to support the functionality for which you are providing external access.

For remote access to work for any edge service, it is mandatory that SIP traffic is allowed to flow bi-directionally as shown in the Inbound/Outbound edge traffic figure. Stated another way, the SIP messaging to and from the Access Edge service is involved in instant messaging (IM), presence, web conferencing, audio/video (A/V) and federation.

Firewall Summary for Scaled Consolidated Edge, Hardware Load Balanced: External Interface – Node 1 and Node 2 (Example)

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/HTTP/TCP/80	Edge Server Access Edge service public IP address	Any	Certificate revocation/ CRL check and retrieval
Access/DNS/TCP/53	Edge Server Access Edge service public IP address	Any	DNS query over TCP
Access/DNS/UDP/53	Edge Server Access Edge service public IP address	Any	DNS query over UDP
A/V/RTP/TCP/50,000-59,999	Edge Server A/V Edge service IP address	Any	Required for federating with partners running Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013.
A/V/RTP/UDP/50,000-59,999	Edge Server A/V Edge service public IP address	Any	Required only for federation with partners running Office Communications Server 2007.
A/V/RTP/TCP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007
A/V/RTP/UDP/50,000-59,999	Any	Edge Server A/V Edge service public IP address	Required only for federation with partners running Office Communications Server 2007
A/V/STUN,MSTURN/ UDP/3478	Edge Server A/V Edge service public IP address	Any	3478 outbound is used to determine the version of Edge Server that Lync Server is communicating with and also for media

			traffic from Edge Server-to-Edge Server. Required for federation with Lync Server 2010, Windows Live Messenger, and Office Communications Server 2007 R2, and also if multiple Edge pools are deployed within a company.
A/V/STUN,MSTURN/ UDP/3478	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/ TCP/443	Any	Edge Server A/V Edge service public IP address	STUN/TURN negotiation of candidates over TCP/443
A/V/STUN,MSTURN/ TCP/443	Edge Server A/V Edge service public IP address	Any	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Scaled Consolidated Edge, Hardware Load Balanced: Internal Interface Node 1 and Node 2

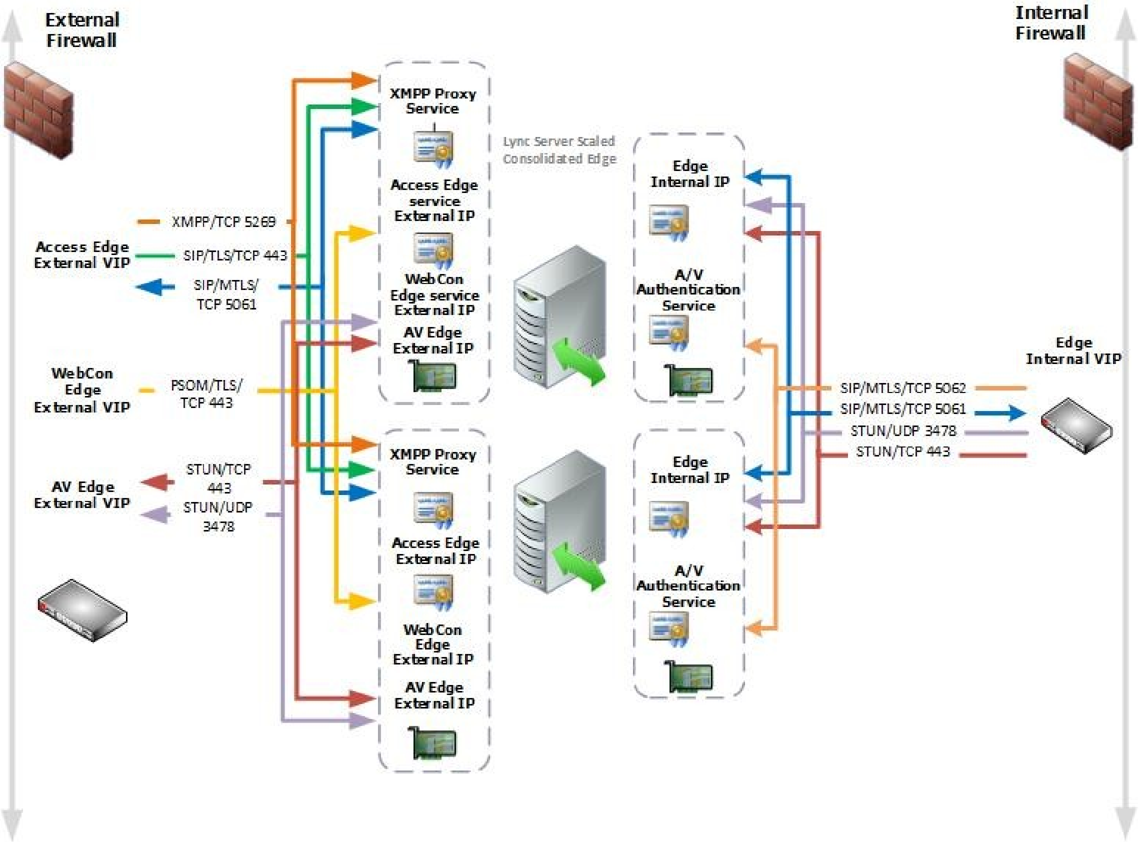
Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/MTLS/ TCP/23456	Any (can be defined as Front End Server address, or Front End pool virtual IP address running the XMPP Gateway service)	Edge Server internal interface	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
HTTPS/TCP/4443	Any (can be defined as the Front End Server server IP or pool that holds the Central Management store)	Edge Server Internal interface	Replication of changes from the Central Management store to the Edge Server
PSOM/MTLS/TCP/8057	Any (can be defined as Director IP, Front End Server IP or Pool virtual IP)	Edge Server Internal interface	Web conferencing traffic from Internal deployment to Internal Edge Server interface
STUN/MSTURN/ UDP/3478	Any (can be defined as Director IP, Front End Server IP or Pool virtual IP)	Edge Server Internal interface	Preferred path for A/V media transfer between internal and external users, Survivable Branch Appliance or

			Survivable Branch Server
STUN/MSTURN/ TCP/443	Any (can be defined as Director IP, Front End Server IP or Pool virtual IP)	Edge Server Internal interface	Fallback path for A/V media transfer between internal and external users, Survivable Branch Appliance or Survivable Branch Server if UDP communication cannot be established, TCP is used for file transfer and desktop sharing
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller using Lync Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

Hardware load balancers have specific requirements when deployed to provide availability and load balancing for Lync Server. The requirements are defined in the following figure and tables. Third party vendors may use different terminology for the requirements defined here. It will be necessary to map the requirements of Lync Server to the features and configuration options provided by your hardware load balancer vendor.

When configuring hardware load balancers, consider the following requirements:

- Source Network Address Translation (SNAT) can be configured on the hardware load balancer (HLB) for Access Edge service and Web Conferencing Edge service
- SNAT cannot be configured on the A/V Edge service– the A/V Edge service must respond with the real server address, not the HLB virtual IP (VIP), for simple traversal of UDP over NAT (STUN)/traversal using relay NAT (TURN)/ federation TURN (FTURN) to work properly
- Public IP addresses are used on each server interface and on the VIPs of the HLB, and your public IP address requirements are N+1, where there is a public IP address for each real server interface and one for each HLB VIP. Where you have 2 Edge servers in the pool, this results in 6 public IP addresses, where 3 are used for the HLB VIPs, and one for each Edge server interface (a total of six for the servers)
- For the Access Edge service and Web Conferencing Edge service, (and using NAT on the HLB) the client contacts the VIP, the VIP changes the source IP address from the client to its own IP address. The server interface addresses the return address to the VIP, the VIP changes the source address from the server interface IP address and sends the packet to the client
- For the A/V Edge service, the VIP must NOT change the source IP address, and the real server address is returned to the client directly – you cannot configure NAT on the HLB for AV traffic
- For AV, the external firewall will retain the real server public IP address for all packets
- Once established, client to A/V Edge service communication is to the real server, not the HLB
- Internal edge to internal servers and clients must be routed, and persistent routes are set for all internal networks that host servers or clients
- The HLB Access Edge service VIP will act as the default gateway for each Edge server interface



External Port Settings Required for Scaled Consolidated Edge, Hardware Load Balanced: External Interface Virtual IPs

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
XMPP/TCP/5269	Any	XMPP Proxy service (shares IP address with Access Edge service)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations
XMPP/TCP/5269	XMPP Proxy service (shares IP address with Access Edge service)	Any	XMPP Proxy service sends traffic to XMPP contacts in defined XMPP federations
Access/SIP(TLS)/ TCP/443	Any	Access Edge service public VIP address	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)/ TCP/5061	Any	Access Edge service public VIP address	SIP signaling, federated and public IM connectivity using SIP
Access/SIP(MTLS)/ TCP/5061	Access Edge service public VIP address	Federated partner	SIP signaling, federated and public IM connectivity using SIP

Web Conferencing/ PSOM(TLS)/TCP/443	Any	Edge Server Web Conferencing Edge service public VIP address	Web Conferencing media
A/V/STUN,MSTURN/ UDP/3478	Any	Edge Server A/V Edge service public VIP address	STUN/TURN negotiation of candidates over UDP/3478
A/V/STUN,MSTURN/ TCP/443	Any	Edge Server A/V Edge service public VIP address	STUN/TURN negotiation of candidates over TCP/443

Firewall Summary for Scaled Consolidated Edge, Hardware Load Balanced: Internal Interface Virtual IPs

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Any (can be defined as Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address)	Edge Server Internal VIP interface	Outbound SIP traffic (from Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address)to Internal Edge VIP
Access/SIP(MTLS)/ TCP/5061	Edge Server Internal VIP interface	Any (can be defined as Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address)	Inbound SIP traffic (to Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address) from Edge Server internal interface
SIP/MTLS/TCP/5062	Any (can be defined as Front End Server IP address, or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server)	Edge Server Internal VIP interface	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server
STUN/MSTURN/ UDP/3478	Any	Edge Server Internal VIP interface	Preferred path for A/V media transfer between internal and external users
STUN/MSTURN/ TCP/443	Any	Edge Server Internal VIP interface	Fallback path for A/V media transfer between internal and external users if UDP communication cannot

			be established, TCP is used for file transfer and desktop sharing
STUN/MSTURN/ TCP/443	Edge Server Internal VIP interface	Any	Fallback path for A/V media transfer between internal and external users if UDP communication cannot be established, TCP is used for file transfer and desktop sharing

1.3.9.10.5.3 DNS Summary - Scaled Consolidated Edge w ith Hardw are Load Balancers

DNS Summary - Scaled Consolidated Edge with Hardware Load Balancers

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2013-01-27*

DNS record requirements for remote access to Lync Server 2013 are fairly straightforward compared to those for certificates and ports. Also, many records are optional, depending on how you configure clients running Lync 2013 and whether you enable federation.

For details about Lync 2013 DNS requirements, see Determine DNS Requirements.

For details about configuring automatic configuration of Lync 2013 clients if split-brain DNS is not configured, see the "Automatic Configuration without Split Brain DNS" section in Determine DNS Requirements.

The following table contains a summary of the DNS records that are required to support the Scaled Consolidated Edge Topology (Hardware Load Balanced) figure. Note that certain DNS records are required only for automatic configuration for Lync clients. If you plan to use group policy objects (GPOs) to configure Lync clients, the associated records are not necessary.

IMPORTANT: Edge Server Network Adapter Requirements

To avoid routing issues, verify that there are at least two network adapters in your Edge Servers and that the default gateway is set only on the network adapter associated with the external interface. For example, as shown in the Scaled Consolidated Edge Scenario figure in Scaled Consolidated Edge with Hardware Load Balancers, the default gateway would point to the external firewall.

You can configure two network adapters in each of your Edge Servers as follows:

- **Network adapter 1 (Internal Interface)**
  Internal interface with 172.25.33.10 assigned.
  No default gateway.
  Ensure there is a route from the network containing the Edge Server internal interface to any networks that contain Lync Server clients or servers running Lync Server (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 (External Interface)**

Three public IP addresses are assigned to this network adapter, for example 131.107.155.10 for Access Edge service, 131.107.155.20 for Web Conferencing Edge service, 131.107.155.30 for A/V Edge service.

Note:

The IP addresses that are assigned to the actual external network interfaces of the Edge Server may depend on which hardware load balancer you choose. Refer to the documentation for your hardware load balancer to understand the actual IP address requirements.
It is possible, though not recommended, to use a single IP address for all three Edge service interfaces. Though this does save IP addresses, it requires different port numbers for each service. The default port number is 443/TCP, which ensures that most remote firewalls will allow the traffic. Changing the port values to (for example) 5061/TCP for the Access Edge service, 444/TCP for the Web Conferencing Edge service and 443/TCP for the A/V Edge service might cause problems for remote users where a firewall that they are behind does not allow the traffic over 5061/TCP and 444/TCP. Additionally, three distinct IP addresses makes troubleshooting easier due to being able to filter on IP address.

Access Edge service IP address is primary with default gateway set to Internet-facing router (131.107.155.1).
Web Conferencing Edge service and A/V Edge service IP addresses secondary.

Tip:

Configuring the Edge Server with two network adapters is one of two options. The other option is to use one network adapter for the internal side and three network adapters for the external side of the Edge Server. The main benefit of this option is a distinct network adapter per Edge Server service, and potentially more concise data collection when troubleshooting is necessary

DNS Records Required for Scaled Consolidated Edge, Hardware Load Balanced (Example)

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	131.107.155.10	Access Edge service external interface (Contoso). Repeat as necessary for all SIP domains with Lync enabled users
External DNS/A	webcon.contoso.com	131.107.155.20	Web Conferencing Edge service external interface
External DNS/A	av.contoso.com	131.107.155.30	A/V Edge service external interface
External DNS/ SRV/443	_sip._tls.contoso.com	sip.contoso.com	Access Edge service external interface. Required for automatic configuration of Lync 2013 and Lync 2010 clients to work externally. Repeat as necessary for all SIP domains with Lync enabled users.
External DNS/	_sipfederationtls._tcp	sip.contoso.com	SIP Access Edge

SRV/5061	.contoso.com		service external interface Required for automatic DNS discovery of federated partners known as "Allowed SIP Domain" (called enhanced federation in previous releases). Repeat as necessary for all SIP domains with Lync enabled users and Microsoft Lync Mobile clients that use either the Push Notification Service or the Apple Push Notification service
Internal DNS/A	lsedge.contoso.net	172.25.33.10	Consolidated Edge internal interface

1.3.9.10.6 Planning for Autodiscover

Planning for Autodiscover

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2013-02-16*

Autodiscover was introduced for Lync Server in the Cumulative Update for Lync Server 2010: November 2011. The primary purpose for this initial implementation of Autodiscover was to provide a means for Lync Mobile to locate the Mobility service (Mcx). The Autodiscover service in Lync Server 2013 is now a service used by all clients to locate server and user services. The Microsoft Lync Server 2013 Autodiscover service runs on Directors and Front End Servers.

💡**Tip:**
For a more technical understanding of Autodiscover and what is communicated to clients, see Understanding Autodiscover. Mobility is still a distinct scenario and the Mobility services still require some special planning. For additional details, see Planning for Mobility.

When Autodiscover was introduced in Lync Server 2010, there were compromises that needed to be made in order to implement a service that required potential certificate changes to existing server deployments. Autodiscover could be used over port TCP 443 for HTTPS or over port TCP 80 for HTTP. If the decision was made to use HTTPS, certificates on reverse proxies, Directors, and Front End Servers needed to be reissued in order to accommodate the required `lyncdiscover.<domain>` and `lyncdiscoverinternal.<domain>` DNS records. If the decision was to use HTTP, the reissue of certificates could be avoided by using DNS CNAME (or alias) records to use existing names on the certificates. Using HTTP did mean that the initial communications were unencrypted.

Because Lync Server 2013 uses Autodiscover for all clients, the main scenario is to use HTTPS exclusively and to create certificates with lyncdiscover.<domain> as part of the configuration of reverse proxies, Directors and Front End Servers. If you are implementing Autodiscover into an upgraded deployment from Lync Server 2010, you may want to use

HTTP to avoid reissuing certificates. Guidance for both scenarios is provided in the following sections.

Important:

The subject alternative name list on certificates used by the external web services publishing rule must contain a *lyncdiscover.<sipdomain>* entry for each SIP domain within your organization. For details about the subject alternative name entries that are required for Directors, Front End Servers, and reverse proxies, see Certificate Summary - Autodiscover.

- Certificate Summary - Autodiscover
- Port Summary - Autodiscover
- DNS Summary - Autodiscover
- Hybrid and Split-Domain - Autodiscover

1.3.9.10.6.1 Certificate Summary - Autodiscover

Certificate Summary - Autodiscover

Planning for External User Access > Scenarios for External User Access > Planning for Autodiscover >

Topic Last Modified: *2013-02-14*

The Lync Server 2013 Autodiscover Service runs on the Director and Front End pool servers, and when published in DNS, can be used by Lync clients to locate server and user services. If you are upgrading from Lync Server 2010 and did not deploy Mobility, before clients can use automatic discovery, you must modify certificate subject alternative name lists on any Director and Front End Server running the Autodiscover Service. In addition, it may be necessary to modify the subject alternative name lists on certificates used for external web service publishing rules on reverse proxies.

The decision about whether to use subject alternative name lists on reverse proxies is based on whether you publish the Autodiscover Service on port 80 or on port 443:

- **Published on port 80** No certificate changes are required if the initial query to the Autodiscover Service occurs over port 80. This is because mobile devices running Lync will access the reverse proxy on port 80 externally and then be bridged to a Director or Front End Server on port 8080 internally. For details, see the "Initial Autodiscover Process Using Port 80" section Technical Requirements for Mobility.
- **Published on port 443** The subject alternative name list on certificates used by the external web services publishing rule must contain a *lyncdiscover.<sipdomain>* entry for each SIP domain within your organization.

  Important:

  We highly recommend using HTTPS over HTTP. HTTPS uses certificates to encrypt traffic. HTTP does not provide for encryption, and any data sent will be plain text.

Reissuing certificates by using an internal certificate authority is typically a simple process. But for public certificates used on the web service publishing rule, adding multiple subject alternative name entries can become expensive. To work around this issue, we support the initial automatic discovery connection over port 80, which is then redirected to port 8080 on the Director or Front End Server.

Note:

If your Lync Server 2013 infrastructure uses internal certificates that are issued from an internal certification authority (CA) and you plan to support mobile devices connecting wirelessly, either the root certificate chain from the internal CA must be installed on the mobile devices or you must change to a public certificate on your Lync Server 2013 infrastructure.

This topic describes the added subject alternative names required for the Director, Front End Server and reverse proxy. Only the added subject alternative names (SAN) are referenced. Refer to the planning sections for guidance on the other entries on certificates. For details, see Scenarios for the Director, Scenarios for External User Access, and Scenarios for Reverse Proxy.

The following tables define the Autodiscover SAN entries for the Director pool, the Front End pool, and the reverse proxy:

Director Pool Certificate Requirements

Description	Subject alternative name entry
Internal Autodiscover Service URL	SAN=lyncdiscoverinternal.<*internal domain name*>
External Autodiscover Service URL	SAN=lyncdiscover.<*sipdomain*>

Note:
You assign the newly updated certificate with the new SAN entry to the Default certificate. Alternatively, you can use SAN=*.<*sipdomain*>.

Front End Pool Certificate Requirements

Description	Subject alternative name entry
Internal Autodiscover Service URL	SAN=lyncdiscoverinternal.<*internal domain name*>
External Autodiscover Service URL	SAN=lyncdiscover.<*sipdomain*>

Note:
You assign the newly updated certificate with the new SAN entry to the Default certificate. Alternatively, you can use SAN=*.<*sipdomain*>

Reverse Proxy (Public CA) Certificate Requirements

Description	Subject alternative name entry
External Autodiscover Service URL	SAN=lyncdiscover.<*sipdomain*>

Note:
You assign the newly updated certificate with the new SAN entry to the SSL Listener on the reverse proxy.

1.3.9.10.6.2 Port Summary - Autodiscover

Port Summary - Autodiscover

Planning for External User Access > Scenarios for External User Access > Planning for Autodiscover >

Topic Last Modified: *2013-03-05*

The Lync Server 2013 Autodiscover Service runs on the Director and Front End pool servers, and when published in DNS using the `lyncdiscover.<domain>` and `lyncdiscoverinternal.<domain>` host records, can be used by clients to locate Lync Server features. In order for mobile devices running Lync Mobile to use Autodiscover, you may first need to modify certificate subject alternative name lists on any Director and

Front End Server running the Autodiscover Service. In addition, it may be necessary to modify the subject alternative name lists on certificates used for external web service publishing rules on reverse proxies.

The decision about whether to use subject alternative name lists on reverse proxies is based on whether you publish the Autodiscover Service on port 80 or on port 443:

- **Published on port 80** For Mobile devices, no certificate changes are required if the initial query to the Autodiscover Service occurs over port 80. This is because mobile devices running Lync will access the reverse proxy on port 80 externally and then be redirected to a Director or Front End Server on port 8080 internally.
- **Published on port 443** The subject alternative name list on certificates used by the external web services publishing rule must contain a `lyncdiscover.<sipdomain>` entry for each SIP domain within your organization.

◆**Important:**
For new installations or upgrades from Lync Server 2010 where you deployed Mobility, you either used Port 80 for Autodiscover of the Mobility service, or reissued certificates with the proper subject name and subject alternative names in place. Review the certificates on your Director and Front End Server to confirm which path you chose.

Firewall Details for Reverse Proxy Server: External Interface

Protocol/TCP or UDP/Port	**Source IP Address**	**Destination IP Address**	**Notes**
HTTP/TCP/80	Any	Reverse proxy listener	(Optional) Redirection to HTTPS if user enters http://*<publishedSiteFQDN>*. Also required if using Office Web Apps for conferencing and the Autodiscover Service for mobile devices running Lync in situations where the organization does not want to modify the external web service publishing rule certificate.
HTTPS/TCP/443	Any	Reverse proxy listener	Address book downloads, Address Book Web Query service, Autodiscover, client updates, meeting content, device updates, group expansion, Office Web Apps for conferencing, dial-in conferencing, and meetings.

Firewall Details for Reverse Proxy Server: Internal Interface

Protocol/TCP or UDP/Port	Source IP Address	Destination IP Address	Notes
HTTP/TCP/8080	Internal reverse proxy interface	Front End Server, Front End pool, Director, Director pool, Office Web Apps for conferencing	Required if using the Autodiscover Service for mobile devices running Lync in situations where the organization does not want to modify the external web service publishing rule certificate. Traffic sent to port 80 on the reverse proxy external interface is redirected to a pool on port 8080 from the reverse proxy internal interface so that the pool Web Services can distinguish it from internal web traffic.
HTTPS/TCP/4443	Internal reverse proxy interface	Front End Server, Front End pool, Director, Director pool, Office Web Apps for conferencing	Traffic sent to port 443 on the reverse proxy external interface is redirected to a pool on port 4443 from the reverse proxy internal interface so that the pool web services can distinguish it from internal web traffic.

1.3.9.10.6.3 DNS Summary - Autodiscover

DNS Summary - Autodiscover

See Also

Planning for External User Access > Scenarios for External User Access > Planning for Autodiscover >

Topic Last Modified: *2013-02-13*

Autodiscover is a flexible service in that it will accept communication over HTTP or HTTPS. To accomplish this, the domain name system (DNS) and the certificates used by servers that host the Autodiscover service must be configured correctly. Certificate requirements are covered in Certificate Summary - Autodiscover.

Important:

DNS lookup logic for the Lync Server clients uses a specific order of resolution. You should always include both the lyncdiscoverinternal.<domain> and the lyncdiscover.<domain> in your DNS. Excluding the lyncdiscoverinternal.<domain> record will cause internal clients to fail to connect to the intended services or receive the incorrect Autodiscover response.

Internal DNS Records

Record type	Host name	Resolves to

CNAME	Lyncdiscoverinternal.*<internal domain name>*	Internal Web Services FQDN for your Director pool, if you have one, or for your Front End pool if you do not have a Director.
A (host, if IPv6, AAAA)	lyncdiscoverinternal.*<internal domain name>*	Internal Web Services IP address (virtual IP (VIP) address if you use a load balancer) of your Director pool, if you have one, or of your Front End pool if you do not have a Director.

You need to create one of the following external DNS records:

External DNS Records

Record type	Host name	Resolves to
CNAME	lyncdiscover.*<sipdomain>*	External Web Services FQDN for your Director pool, if you have one, or for your Front End pool if you do not have a Director.
A (host, if IPv6, AAAA)	lyncdiscover.*<sipdomain>*	External or public IP address of the reverse proxy.

Note:

External traffic goes through the reverse proxy.

Note:

Mobile device clients do not support multiple Secure Sockets Layer (SSL) certificates from different domains. Therefore, CNAME redirection to different domains is not supported over HTTPS. For example, a DNS CNAME record for lyncdiscover.contoso.com that redirects to an address of director.contoso.net is not supported over HTTPS. In such a topology, a mobile device client needs to use HTTP for the first request, so that the CNAME redirection is resolved over HTTP. Subsequent requests then use HTTPS. To support this scenario, you need to configure your reverse proxy with a web publishing rule for port 80 (HTTP). For details, see "To create a web publishing rule for port 80" in Configuring the Reverse Proxy for Mobility. CNAME redirection to the same domain is supported over HTTPS. In this case, the destination domain's certificate covers the originating domain.

Tasks

Configuring the Reverse Proxy for Mobility

Concepts

Certificate Summary - Autodiscover

1.3.9.10.6.4 Hybrid and Split-Domain - Autodiscover

Hybrid and Split-Domain - Autodiscover

Planning for External User Access > Scenarios for External User Access > Planning for Autodiscover >

Topic Last Modified: *2013-02-14*

A shared SIP address space, also known as a *split-domain* deployment, or a *hybrid* deployment, is a configuration where users are deployed across an on-premise deployment and an online environment. The desired outcome is to have a user, regardless of where their home server is located (on-premise or online), log into the deployment and be redirected to their home server location. To accomplish this, the Autodiscover feature of Lync Server 2013 is used to redirect the online user to the online topology. You can do this by configuring the Autodiscover uniform resource locator (URL) by using the Lync Server Management Shell, the **Get-CsHostingProvider** cmdlet, and the **Set-CsHostingProvider** cmdlet.

Mobility for the Split Domain Deployment

You will need to collect and record the following deployed attributes:

- From the Lync Server Management Shell, type

```
Get-CsHostingProvider
```

- In the results, find the online provider with the attribute **ProxyFQDN**. For example, sipfed.online.lync.com.
- Record the value of the ProxyFQDN.
- Enable federation in the on-premise Lync Server Control Panel, allowing federation with the online provider.
- Enable federation for the online provider. By default, all online users are enabled for domain federation and can communicate with all domains.
- If you will define blocked and allowed domains, determine the domains that you will explicitly allow or explicitly block.
- For online federation, you must plan for firewall exceptions, certificates, and DNS host (A or AAAA, if using IPv6) records. Additionally, you must configure federation policies. For details, see Planning for Lync Server and Office Communications Server Federation.

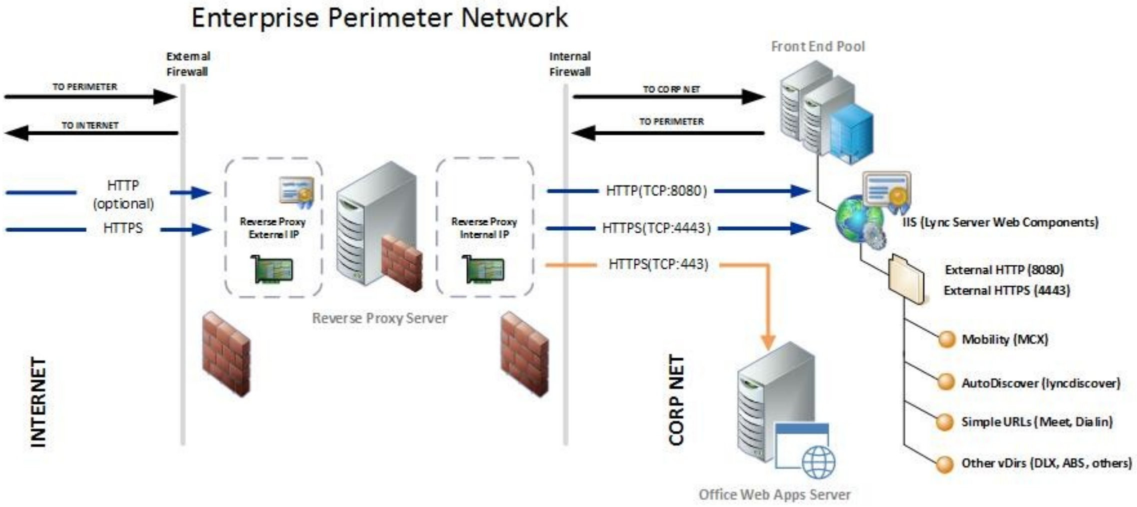
1.3.9.10.7 Scenarios for Reverse Proxy

Scenarios for Reverse Proxy

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2013-01-21*

Reverse proxies are required in Lync Server 2013 for providing access to services and resources such as the meeting and dial-in Simple URLs, address book, meeting content, distribution list expansion, mobility services, and others. The typical reverse proxy scenario in Lync Server 2013 is to allow external clients (for example, the desktop client or Lync Web App client) access to the Director or Front End Server external Web Services.



During the planning phase, you define the requirements for the reverse proxy in a Lync Server 2013 deployment. The reverse proxy enables access to features for the following external clients:

- Microsoft Lync 2013 desktop client
- Microsoft Lync Web App
- Microsoft Lync Mobile
- Lync Windows Store app

When planning your Lync Server 2013 deployment, you map the actual requirements for Lync Server 2013 to the reverse proxy features.

1. External clients will connect to the reverse proxy on port TCP 443 and will use secure socket layer (SSL) or transport layer security (TLS). Microsoft Lync Mobile clients can connect on port TCP 80, but only when performing the initial connection to the Lync discover services and the administrator has configured the proper domain name system (DNS) CNAME (or alias) records, and accepts that this communication will not be encrypted.
2. Lync Server 2013 external web services (deployed on the Front End Server and/or the Director) expect a connection from a reverse proxy on port TCP 4443, and it expects that the connection will be SSL/TLS.

> **Important:**
>
> The suggested default listening ports for the external web services are TCP 8080 for HTTP traffic, and TCP 4443 for HTTPS traffic. Topology Builder provides an opportunity to override the defaults and define your own listening ports for the external web services. It's important to note that the reverse proxy communicates with the external web services, and the external clients communicate with the reverse proxy. The external client communicates with the reverse proxy on port TCP 443, but you can redefine what port the reverse proxy communicates with the external web services on. The options in Topology Builder to override the default listening ports for the web services allows you to resolve listening port conflicts that may arise in your infrastructure.

3. Lync Server 2013 external web services expect an unmodified Host Header from the client to identify what service and web server directory the client is attempting to use. Requests should appear as if they came from the reverse proxy
4. The external web services use defined web server virtual directories (vDir) that provide the services offered to clients. Specific externally identifiable web services are:
   - The "Meet" vDir for web conference meetings

- The “Dialin” vDir for phone access and phone conferencing
- The “Autodiscover” vDir for Lync Windows Store app, Lync Mobile, and the desktop client Lync 2013. Autodiscover in Lync Server 2013 is known by the DNS name “lyncdiscover”
- Services not defined are accessed by the external client by direct calls to the external web services. For example, distribution group expansion (DLX) and the address book service (ABS) are accessed by direct calls to the external web services and associated vDirs. The client knows the actual path to the vDir and constructs a uniform record locator (URL) based on this information. The client would access the address book service using a URL similar to `https://externalweb.contoso.com/abs/handler`
- The Office Web Apps Server when conferencing is defined and configured as part of the Lync Server topology

> **Note:**
> The Office Web Apps Server is a separate role server and is not configured as part of the external web services. This server is separately published for client access.

5. Define SSL bridging for each service. The external port TCP 443 is mapped to the external web services port of TCP 4443. For unencrypted HTTP, port TCP 80 is mapped to the external web services port TCP 8080
6. Plan for reverse proxy listeners to publish web server resources
7. Request and configure the certificate for the reverse proxy based on the services that will be offered. If configured with the correct subject alternative names, this certificate can be shared by all configured listeners on the reverse proxy server

Resources available for planning your reverse proxy deployment:

- Data Collection
- Certificate Summary - Reverse Proxy
- Port Summary - Reverse Proxy
- DNS Summary - Reverse Proxy

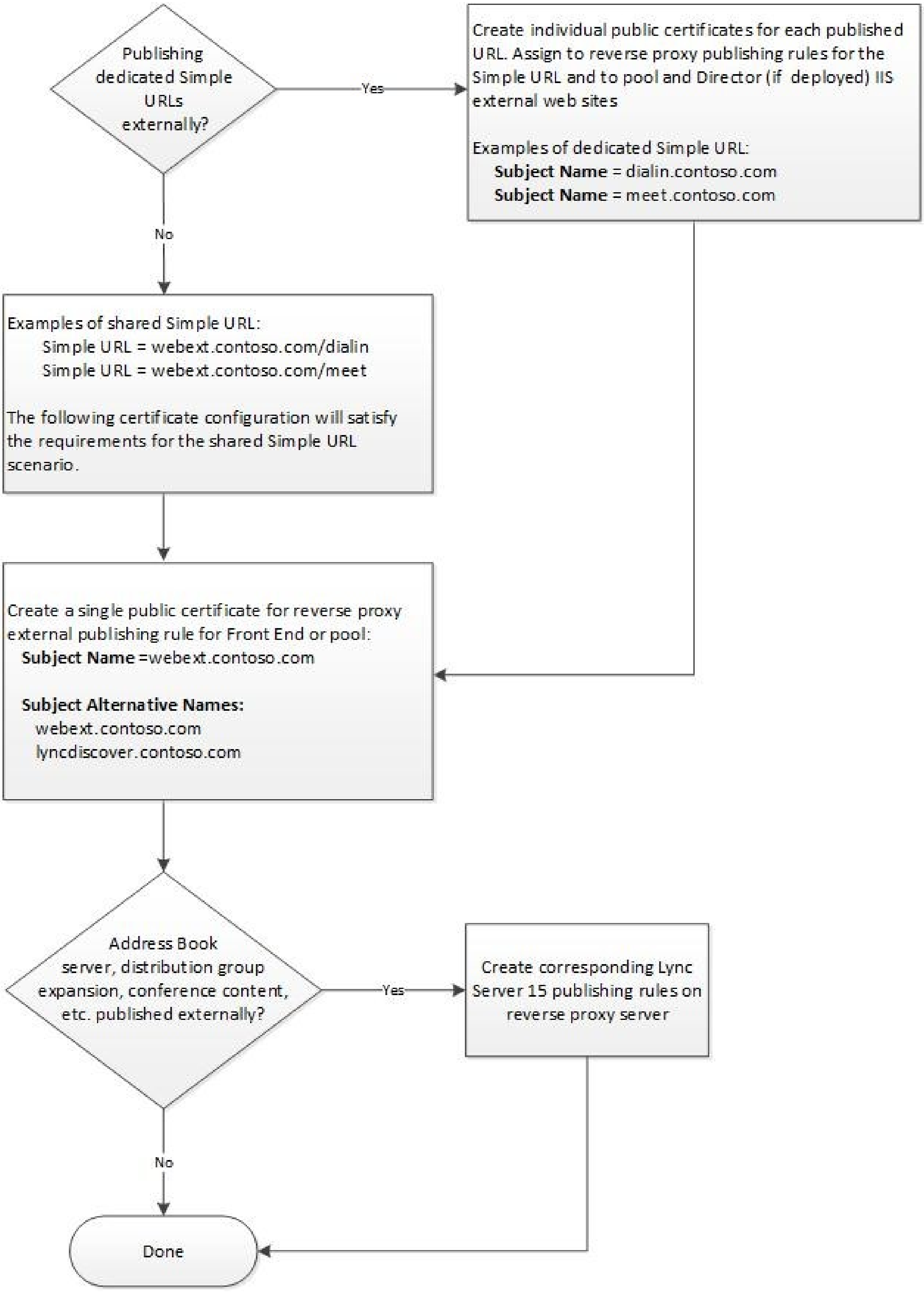
1.3.9.10.7.1 Certificate Summary - Reverse Proxy

Certificate Summary - Reverse Proxy

Planning for External User Access > Scenarios for External User Access > Scenarios for Reverse Proxy >

Topic Last Modified: *2012-11-14*

Certificate requirements for the reverse proxy are much simpler than that for the Edge Servers. The provided flowchart presents the requirements necessary. The accompanying table presents typical certificate subject name and subject alternative names in relation to the scenarios that we have been reviewed in the Edge Server discussions. For more details on the Edge Server scenarios, see Scenarios for External User Access.



Publishing dedicated Simple URLs externally?

Create individual public certificates for each published URL. Assign to reverse proxy publishing rules for the Simple URL and to pool and Director (if deployed) IIS external web sites

Examples of dedicated Simple URL:
Subject Name = dialin.contoso.com
Subject Name = meet.contoso.com

Examples of shared Simple URL:
Simple URL = webext.contoso.com/dialin
Simple URL = webext.contoso.com/meet

The following certificate configuration will satisfy the requirements for the shared Simple URL scenario.

Create a single public certificate for reverse proxy external publishing rule for Front End or pool:
Subject Name =webext.contoso.com

Subject Alternative Names:
webext.contoso.com
lyncdiscover.contoso.com

Address Book server, distribution group expansion, conference content, etc. published externally?

Create corresponding Lync Server 15 publishing rules on reverse proxy server

Reverse Proxy: External Interface

Component	Subject name	Subject alternative name (SAN)/Order	Comments
Reverse Proxy	webext.contoso.com	webext.contoso.com webdirext.contoso.com dialin.contoso.com meet.contoso.com officewebapps01.contoso.com lyncdiscover.contoso.com (Optional):*.contoso.com	Certificate must be issued by a public CA and with the server EKU. Services include Address Book Service, distribution group expansion Office Web Apps for conferencing, and Lync IP Device publishing rules. Subject alternative name includes: • External Web Services FQDN for Front End Server or Front End pool • External Web Services FQDN for Director or Director pool • Dial-in conferencing • Online meeting publishing rule • Office Web Apps for conferencing • Lyncdiscover (Autodiscover) The optional wildcard replaces both meet and dialin SAN

1.3.9.10.7.2 Port Summary - Reverse Proxy

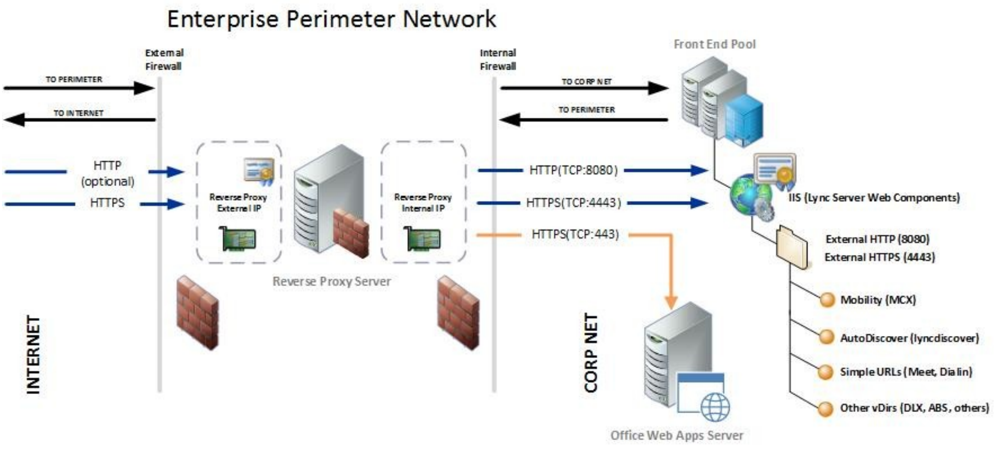
Port Summary - Reverse Proxy

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2013-02-15*

The reverse proxy has minimal requirements for firewall and port/protocol.

- External firewall requirements are the HTTPS/TCP/443 and the optional HTTP/TCP/80. HTTPS is used for SSL and TLS secure communications through the reverse proxy. HTTP is used if you choose to allow access to the Autodiscover Service when modifying certificates might prove difficult or not cost justified.
- Clients expect to contact the Office Web Apps Server on HTTPS. The Office Web Apps Server expects communication from internal clients on HTTPS/TCP/443. The recommended configuration is to allow HTTPS/TCP/443 from the reverse proxy to the Office Web Apps Server.
- Port 8080 is used to route traffic from the reverse proxy internal interface to the Front End Server, Front End pool virtual IP (VIP) or the optional Director or Director pool VIP. Port TCP 8080 is required for mobile devices running Lync to locate the Autodiscover Service in situations where modifying the external web service publishing rule certificate is undesirable (for example, if you have a large number of SIP domains). If you choose to acquire new certificates with the necessary SAN entries, the port TCP 8080 is not needed and is optional.
- Port 4443 is used for traffic from the reverse proxy internal interface to the Front End Server, Front End pool virtual IP (VIP) or the optional Director or Director pool VIP



Caution:

Do not confuse the 4443 over TCP from the reverse proxy to the internal deployment for the port 4443 over TCP traffic from the Standard Edition server or the Front End pool that manages the Central Management store role.

Port and Protocol Details

Firewall Details for Reverse Proxy Server: External Interface

Protocol/TCP or UDP/Port	Source IP Address	Destination IP Address	Notes
HTTP/TCP/80	Any	Reverse proxy listener	(Optional) Redirection to HTTPS if user enters http://*<publishedSiteFQDN>*. Also required if using Office Web Apps for conferencing and the Autodiscover Service for mobile devices running Lync in situations where the organization does not want to modify the external web service publishing rule certificate.
HTTPS/TCP/443	Any	Reverse proxy listener	Address book downloads, Address Book Web Query service, Autodiscover, client updates, meeting content, device updates, group expansion, Office Web Apps for conferencing, dial-in

			conferencing, and meetings.

Firewall Details for Reverse Proxy Server: Internal Interface

Protocol/TCP or UDP/Port	Source IP Address	Destination IP Address	Notes
HTTP/TCP/8080	Internal reverse proxy interface	Front End Server, Front End pool, Director, Director pool	Required if using the Autodiscover Service for mobile devices running Lync in situations where the organization does not want to modify the external web service publishing rule certificate. Traffic sent to port 80 on the reverse proxy external interface is redirected to a pool on port 8080 from the reverse proxy internal interface so that the pool Web Services can distinguish it from internal web traffic.
HTTPS/TCP/4443	Internal reverse proxy interface	Front End Server, Front End pool, Director, Director pool	Traffic sent to port 443 on the reverse proxy external interface is redirected to a pool on port 4443 from the reverse proxy internal interface so that the pool web services can distinguish it from internal web traffic.
HTTPS/TCP/443	Internal reverse proxy interface	Office Web Apps for conferencing	

1.3.9.10.7.3 DNS Summary - Reverse Proxy

DNS Summary - Reverse Proxy

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-10-31*

You configure two network adapters in your reverse proxy as follows:

Reverse Proxy Network Adapter

Requirements

- **Network adapter 1 (Internal Interface)** example
  Internal interface with 172.25.33.40 assigned.
  No default gateway is defined.
  Ensure there is a route from the network containing the reverse proxy internal interface to any networks that contain Lync Server Front End pool servers (for example, from 172.25.33.0 to 192.168.10.0).
- **Network adapter 2 (External Interface)** example
  A minimum of one public IP address is assigned to this network adapter.
  Gateway is defined to point to the router or integrated firewall in your outer perimeter. (10.45.16.1 in the scenario examples)

DNS Records Required for Reverse Proxy

Location/TYPE/Port	FQDN	IP address	Maps to/comments
External DNS/A	webext.contoso.com	Assigned listener for externally published resources	External web services from the internal deployment. Additional records can be defined and created for all pools and single servers for any SIP domain that will use this reverse proxy, and has defined external web services.
External DNS/A	webdirext.contoso.com	Assigned listener for externally published resources	External web services for the Directors or Director pools in your deployment. You can define as many Directors as there are distinct Directors, of which may be associated with other SIP domains. **Important:** Defining the DNS records for and publishing the Directors is not an either the Front End pool or the Director decision. You must define and publish both the Director and the Front End pool external web services if you are using Directors. Specific traffic types (for authentication and other uses) will be sent to the Director first, if it is defined in the topology.

External DNS/A	dialin.contoso.com	Assigned listener for externally published resources	Dial-in conferencing published externally
External DNS/A	meet.contoso.com	Assigned listener for externally published resources	Conferences published externally
External DNS/A	officewebapps01.contoso.com	Assigned listener for Office Web Apps Server	Office Web Apps Server deployed internally or in the perimeter, and published for external client access
External DNS/A	lyncdiscover.contoso.com	Assigned listener for externally published resources	Lync Discover External record for externally published AutoDiscover, and includes Mobility, Microsoft Lync Web App, and scheduler Web app
External DNS/A	lsrp.contoso.com	Assigned listener for externally published resources	Reference record for the reverse proxy external name

1.3.9.10.8 Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation

Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2012-10-20*

Edge Servers can be configured to allow your internal and external users access to contacts at partner organizations or services. Federations, as these partner agreements are known, can provide any or all of the following to the contacts in your organization on the partner federation or contacts in the partner federation to yours:

- Instant messaging and presence
- Collaboration and conferencing, for example – Web conferencing
- Audio conferencing, video conferencing, or both

In some cases the communication, for example instant messaging (IM) and presence between a Microsoft Lync Server 2013 and an extensible messaging and presence protocol (XMPP) contact, is peer-to-peer only - supporting only you and the contact at the federated partner. In other cases, such as a Lync Server, Lync Server 2010 to Lync Server 2013 federation, multiple participants can be invited to join into the conversation.

In this section are resources to assist you in planning for federation:

- Planning for Lync Server and Office Communications Server Federation
- Planning for Public Instant Messaging Connectivity
- Planning for Extensible Messaging and Presence Protocol (XMPP) Federation

1.3.9.10.8.1 Planning for Lync Server and Office Communications Server Federation

Planning for Lync Server and Office Communications Server Federation

See Also

Planning for External User Access > Scenarios for External User Access > Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation >

Topic Last Modified: *2013-02-13*

Federation between Microsoft Lync Server 2013, Lync Server 2010 and Office Communications Server supports peer-to-peer and multi-party communications. Peer-to-peer conversations can be escalated to multi-party conversations, allowing for ad hoc meetings. Meetings – Web conferencing or audio/visual conferences – can be scheduled to include contacts inside your organization as well as contacts in partners that you federate with.

Federation first appeared in Microsoft Office Live Communications Server 2005 and supported one kind of federation, Direct Federation. Direct Federation required you to know the federation partner's session initiation protocol (SIP) domain and the fully qualified domain name (FQDN) of the partner's Edge Server. Live Communications Server 2005 with SP1 introduced additional federation types, all of which required domain name system (DNS) SRV records to be published by the federated partner to locate their Edge Server. The terminology for that release was:

- *Open Enhanced Federation*: Accept any SIP domain name and use DNS SRV to locate the partner Edge Server
- *Enhanced Federation*: Configure the partner's SIP domain name as a federation partner for your organization and use DNS SRV to find the partner Edge Server
- *Direct Federation*: Configure the partner's SIP domain name and the FQDN to the partner's Edge Server
- *Server Allow List*: Accept any domain, use DNS SRV to find the Edge Server of a hosting provider or a public instant messaging (IM) connectivity provider

Microsoft Office Communications Server 2007 introduced updated naming for federation types to better define what each federation type actually accomplished:

- Open Enhanced Federation became known as *Discovered Partner Domain*
- Enhanced Federation became known as *Allowed Partner Domain*
- Direct Federation became known as *Allowed Partner Server*
- Server Allow List became known as *Hosting Provider* and *Public IM Provider*

Microsoft Lync Server 2010 introduced a narrower definition of Hosting Provider in accordance with Microsoft Lync Online 2010 and Microsoft Office 365 and also made it subject to the same allowed list defined by the Allowed Partner Domain federation type.

Enabling federation between Microsoft Lync Server 2013, Lync Server 2010 and Office Communications Server uses the Edge Servers and reverse proxies to enforce the rules and allowed partner domains that you define. From a planning perspective, federating with other Lync Server, Office Communications Server requires the following:

- Enable federation in Topology Builder. For details, see the Deployment topic Configuring SIP Federation, XMPP Federation and Public Instant Messaging.
- Determine your requirements for federated domain discovery:
  - For manual configuration of federation, you must have the fully qualified domain name (FQDN) of the partner's Edge Server and domain name, or online domain name, which is entered in the Lync Server Control Panel, **Federation and External Access**, **SIP Federated Domains**. Create a **New** policy or **Edit** an existing policy to either allow or block domains by FQDN.

> **⚠Warning:**
>
> Manual configuration of a federation partner's Edge Server is prone to failure in the event that the partner changes the IP address of their Edge Server.

> **Note:**
>
> For **New SIP Federated Domains**, you must provide the **Domain name (or FQDN)** for Microsoft Lync Online, Microsoft Office 365. For Microsoft Lync Server 2013, Lync Server 2010 and Office Communications Server you must also provide an **Access Edge service (FQDN)**

- For discovered partner federation, where partners can discover your Edge Server, you create an SRV record in your external DNS - _sipfederationtls._tcp.contoso.com – which points to the port 5061 and the host (A) record of your Edge Server

> **Important:**
>
> If you are supporting Microsoft Lync Mobile clients on either Windows Phone or Apple iPhone, iPad, or other Apple devices and are using the Push Notification Service or Push Notification Service, you must plan for _sipfederationtls._tcp. <*SIP domain*> SRV records for each SIP domain that you have Lync Mobile clients. Android and Nokia Symbian Lync Mobile do not use push notification and are not subject to this requirement.

- Configure external user access policies to support federated domains
- Open firewall ports for session initiation protocol (SIP), web conferencing and audio/visual to accommodate the federation or contacts that you are enabling. For details, see: Determine External A/V Firewall and Port Requirements

The following information will aid you in defining the certificate, port/protocol and DNS requirements for federation with Microsoft Lync Server 2013 and Lync Server 2010.

Planning for certificates, firewall and port/protocol requirements and DNS requirements is generally a straight forward process if you have planned or deployed your Microsoft Lync Server 2013 Edge Servers. Because federation is an additional feature that uses the existing Edge Server, the planning requirements are generally met by the Edge Server planning and deployment. You should use the following tables to determine that your requirements are met and make changes in port/protocol and DNS accordingly.

> **Important:**
>
> If you have a pool of Edge Servers and are federating with Lync Server 2013 or Lync Server 2010 partners, then you can use either DNS load balancing or hardware load balancers on the internal and external facing sides of the Edge Servers. If you are federating with Office Communications Server 2007 or Office Communications Server 2007 R2, hardware load balancing will provide failover support in the event of an Edge Server. Office Communications Server 2007 and Office Communications Server 2007 R2 are not DNS load balancing aware. The partner Edge Servers will establish communication with the first Edge Server in your pool that responds. If that Edge Server fails, communication does not automatically failover.

Certificate requirements are typically met through the planning of certificates for your chosen Edge Server or pooled Edge Server plan.

- Certificate Summary - Lync Server and Office Communications Server Federation
- Port Summary - Lync Server and Office Communications Server Federation
- DNS Summary - Lync Server and Office Communications Server Federation

⊟See Also

Tasks

Configure Policies to Control Federated User Access

Concepts

Scenarios for External User Access
Determine External A/V Firewall and Port Requirements
Determine DNS Requirements

Other Resources

Manage Access Edge Configuration for Your Organization
Manage SIP Federated Domains for Your Organization
Manage SIP Federated Providers for Your Organization

Certificate Summary - Lync Server and Office Communications Server Federation

See Also

Scenarios for External User Access > Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation > Planning for Lync Server and Office Communications Server Federation >

Topic Last Modified: *2012-09-08*

The certificates that you need for Microsoft Lync Server 2013, Lync Server 2010 and Office Communications Server will typically be met by the certificates that you configure, request and assign to your Edge Server.

To confirm that you have met the correct certificate requirements for your Edge Server deployment, review the topics listed in the section titled **See Also**.

Concepts

Plan for Edge Server Certificates
Certificate Summary - Single Consolidated Edge with Private IP Addresses Using NAT
Certificate Summary - Single Consolidated Edge with Public IP Addresses
Certificate Summary - Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT
Certificate Summary - Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses
Certificate Summary - Scaled Consolidated Edge with Hardware Load Balancers

Port Summary - Lync Server and Office Communications Server Federation

See Also

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-10-20*

Port, protocol and firewall requirements for federation with Microsoft Lync Server 2013, Lync Server 2010 and Office Communications Server are similar to those for the deployed Edge Server. Clients initiate communication with the Access Edge service over TLS/SIP/TCP 443. Federated partners however, will initiate communications to the Access Edge service over MTLS/SIP/TCP 5061.

Firewall Summary for Federation

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/ TCP/5061	Access Edge service public IP address	Any	For federated and public IM connectivity using SIP

⊟See Also

Concepts

Scenarios for External User Access

DNS Summary - Lync Server and Office Communications Server Federation

See Also

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-10-20*

The domain name system (DNS) records that will be required for defining a federation with Office Communications Server or Lync Server partners is determined by your decision to either allow automatic DNS discovery of your domain by other perspective partners. If you publish the _sipfederationtls._tcp. <*SIP domain name*> SRV record, any other SIP federated domain will be able to "discover" your federation. You can control which federated domains can communicate with you by using the Allows domains and Blocked Domains settings in the Lync Server Control Panel, or by setting the allowed or blocked domains configuration using the Lync Server Management Shell and the **Get**, **Set**, **New**, **Remove-CsAllowedDomain** and **-CsBlockedDomain** PowerShell cmdlets. For additional information on how to configure theses settings and the use of the PowerShell cmdlets, see **Related Topics** at the end of this topic.

The DNS records summary table depicts the required entries for an open, or discoverable, federation. If you do not want to implement Federation Discovery, You can decide to not configure the _sipfederationtls._tcp. <*SIP domain name*> record.

◆**Important:**
There are specific scenarios in which you must have the _sipfederationtls._tcp. <*SIP domain name*> SRV record, but you do not want to have a discoverable federation. One such instance is where you have deployed mobility for your users. The mobility push notification clearinghouse (PNCH) is a special type of federation that is used for Microsoft Lync Mobile clients on Apple iPhone or Windows Phone. The _sipfederationtls._tcp. <*SIP domain name*> SRV record is used in the case of mobility and PNCH. To mitigate this issue and control your discoverability, clear the setting **Enable partner domain discovery** to turn off discovery.

Records Required for Federation

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5061	_sipfederationtls._tcp .contoso.com	sip.contoso.com	Access Edge service external interface Required for automatic DNS discovery of your federation to other potential federation

			partners, and is known as “Allowed SIP Domains” (called enhanced federation in previous releases).Repeat as necessary for all SIP domains with Lync enabled users ◆**Important:** This SRV record is required for mobility and the push notification clearing house. In cases where there is more than one SIP domain, create and publish an SRV record for each domain that will have Lync Mobile clients. The Push Notification Service and Apple Push Notification service may not operate as expected if there is not an explicit SRV record for each SIP domain that the deployment supports.

See Also

Tasks

Configuring for Push Notifications
Enable or Disable Discovery of Federation Partners

Other Resources

Manage SIP Federated Domains for Your Organization

1.3.9.10.8.2 Planning for Public Instant Messaging Connectivity

Planning for Public Instant Messaging Connectivity

Planning for External User Access > Scenarios for External User Access > Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation >

Topic Last Modified: *2013-02-17*

Public Instant Messaging Connectivity is a class of federation, and is configured to allow your internal and external Lync Server 2013 users to add contacts from any of the following:

- Messenger contacts
- Yahoo! contacts
- America Online (AOL) contacts

◆**Important:**

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User

Subscription License (PIC USL) is no longer available for the purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shutdown date (exact date is still to be decided, but no sooner than June 2013).
- The PIC USL is a per-user, per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which will not be renewed.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people through IM and voice.

This class of federation requires the following planning considerations:

- Windows Live Messenger users can have peer-to-peer audio/visual communication with Lync Server 2013 users, in addition to instant messaging. Your Edge Servers must meet specific port and protocol requirements. For details, see Determine External A/V Firewall and Port Requirements.
- Yahoo instant messaging has no unique requirements, other than those typically used in the planning and deployment of the typical Edge Server that is providing federation.
- America Online requires that your Edge Server certificate assigned to the Access Edge service has a client enhanced key usage (EKU).
- Certificate Summary - Public Instant Messaging Connectivity
- Port Summary - Public Instant Messaging Connectivity
- DNS Summary - Public Instant Messaging Connectivity

Certificate Summary - Public Instant Messaging Connectivity

See Also

Scenarios for External User Access > Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation > Planning for Public Instant Messaging Connectivity >

Topic Last Modified: *2013-02-19*

To configure certificates for public Instant Messaging connectivity, you should first notice that there is nothing different from other SIP federation types or even standard Edge Server certificates, except that America Online (AOL) requires a unique certificate configuration. In addition to the usual server enhanced key usage (EKU), America Online requires the certificate or certificates (in the case of an Edge pool) to also contain the client EKU. The client EKU is an addition to the certificate, and is part of the external public certificate that is assigned to your Edge Server.

Certificate Summary – Public Instant Messaging Connectivity

Component	**Subject name**	**Subject alternative names (SAN)/Order**	**Comments**
External/Access Edge	sip.contoso.com	sip.contoso.com webcon.contoso.c	The certificate must be from a Public CA, and must have the server EKU and client EKU if

		om sip.fabrikam.com	public IM connectivity with AOL is to be deployed. The certificate is assigned to the external Edge Server interfaces for: • Access Edge service • Web Conferencing Edge service • A/V Edge service Note that SANs are automatically added to the certificate based on your definitions in Topology Builder. You add SAN entries as needed for additional SIP domains and other entries that you need to support. The subject name is replicated in the SAN and must be present for correct operation.

⊟See Also

Concepts

Scenarios for External User Access

Port Summary - Public Instant Messaging Connectivity

See Also

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2013-02-16*

To configure your firewall for ports and protocols necessary to support public instant messaging connectivity, first note that SIP/MTLS/TCP 5061 is bidirectional to account for the ability of contacts in the public IM provider to contact Lync clients, or for Lync to contact public IM contacts.

Windows Live Messenger can participate in audio/video communications with Lync clients. This accounts for the very similar firewall port and protocol configuration that you would typically have on the firewall to support Lync clients as external users.

◆**Important:**
More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard Client Access License (CAL). Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice. Federation with Messenger client contacts will officially end on March 15, 2013, except for mainland China. Skype will become the federation client for federated users who previously used Messenger.

Firewall Summary – Public Instant Messaging Connectivity

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
Access/SIP(MTLS)/TCP/5061	Public IM connectivity partners	Edge Server Access interface	For federated and public IM connectivity that use SIP.
Access/SIP(MTLS)/TCP/5061	Edge Server Access interface	Public IM connectivity partners	For federated and public IM connectivity that use SIP.
Access/SIP(TLS)/TCP/443	Clients	Edge Server Access interface	Client-to-server SIP traffic for external user access.
A/V/RTP/TCP/50,000-59,999	Edge Server Access interface	Live Messenger clients	Used for A/V sessions with Windows Live Messenger if public IM connectivity is configured.
A/V/STUN,MSTURN/UDP/3478	Edge Server Access interface	Live Messenger clients	Required for public IM connectivity with Windows Live Messenger.
A/V/STUN,MSTURN/UDP/3478	Live Messenger clients	Edge Server Access interface	Required for public IM connectivity with Windows Live Messenger.

⊟See Also

Concepts

Scenarios for External User Access
Determine External A/V Firewall and Port Requirements

DNS Summary - Public Instant Messaging Connectivity

See Also

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2013-02-16*

When you configure domain name system (DNS) for public instant messaging connectivity, you will find that the configuration that supports external users will support public IM connectivity. If you have already configured your Edge Server or Edge pool, you should have the DNS records necessary to support public IM connectivity.

DNS Summary – Public Instant Messaging Connectivity

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
External DNS/A	sip.contoso.com	Access Edge service interface	Access Edge service external interface

			(Contoso). Repeat as necessary for all SIP domains with Lync enabled users.

⊟See Also

Concepts

Scenarios for External User Access

1.3.9.10.8.3 Planning for Extensible Messaging and Presence Protocol (XMPP) Federation

Planning for Extensible Messaging and Presence Protocol (XMPP) Federation

See Also

Planning for External User Access > Scenarios for External User Access > Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation >

Topic Last Modified: *2012-10-22*

Previous versions of Lync Server and Office Communications Server provided an extensible messaging and presence protocol (XMPP) gateway that could be deployed as a separate server role to allow federating with XMPP deployments. In Microsoft Lync Server 2013, the XMPP functionality can be deployed as a feature. XMPP functionality is installed in two parts: an XMPP proxy that runs on the Edge Server and the XMPP gateway that runs on the Front End Servers.

Deployment and configuration of XMPP is covered in Deploying External User Access You plan for supporting XMPP in your organization by defining port and protocol rules on your firewall, configuration of certificates, and adding DNS records. The following topics in this section summarize the information that you will need to successfully plan XMPP federation for your deployment.

Important:

The XMPP capability of Lync Server 2013 is tested and supported by Microsoft for instant messaging federation with Google Talk. For any other XMPP systems contact the third-party vendor to verify that they support federation with Lync Server 2013, and for any deployment or troubleshooting recommendations.

- Certificate Summary - Extensible Messaging and Presence Protocol (XMPP) Federation
- Port Summary - Extensible Messaging and Presence Protocol (XMPP) Federation
- DNS Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

⊟See Also

Tasks

Setting Up XMPP Federation
Configure Policies to Control XMPP Federated User Access

Other Resources

Manage XMPP Federated Partners for Your Organization
Get-CsExternalAccessPolicy
Get-CsXmppAllowedPartner
Get-CsXmppGatewayConfiguration

Certificate Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

See Also

Scenarios for External User Access > Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation > Planning for Extensible Messaging and Presence Protocol (XMPP) Federation >

Topic Last Modified: *2012-12-23*

Certificate requirements for enabling and establishing communications with extensible messaging and presence protocol (XMPP) partners require the additional record of your XMPP domains. The record that is included on the certificate as a subject alternative name (SAN) will be the domain that can participate in XMPP communications. The domain can be the root-level domain (for example, contoso.com) if you want to enable XMPP for your entire domain, or can be selected child domains (for example, corp.contoso.com, finance.contoso.com) if you are enabling XMPP for a subset of users.

Certificate Summary for Extensible Messaging and Presence Protocol

Component	Subject name	Subject alternative names (SAN)/Order	Comments
Assign to Access Edge service of Edge Server or Edge pool	sip.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com contoso.com	The first three SAN entries are the normal SAN entries for a full Edge Server. The contoso.com is the entry required for federation with the XMPP partner at the root domain level. This entry will allow XMPP for all domains with the suffix contoso.com.

⊟See Also

Tasks

Example XMPP Configuration – XMPP Federation with Google Talk

Concepts

Plan for Edge Server Certificates

Other Resources

Set Up Edge Certificates
Request-CsCertificate
Set-CsCertificate

Port Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

See Also

Planning > Network Planning for Lync Server > Port Requirements >

Topic Last Modified: *2012-10-20*

The ports and protocols defined for the extensible messaging and presence protocol (XMPP) proxy deployed on the Edge Server allow communications from the XMPP federated partner to the Edge Server, and also allows communication from your Edge Server to the XMPP federated partner. A rule is also defined on the internal-facing firewall from the Front End Server or Front End pool to the Edge Server or Edge pool.

Firewall Summary for Extensible Messaging and Presence Protocol

Protocol/TCP or UDP/Port	Source (IP address)	Destination (IP address)	Comments
XMPP/TCP/5269	Any	Access Edge service interface IP address	Standard server-to-server communication port for XMPP. Allows communication to the Edge Server XMPP proxy from federated XMPP partners
XMPP/TCP/5269	Access Edge service interface IP address	Any	Standard server-to-server communication port for XMPP. Allows communication from the Edge Server XMPP proxy to federated XMPP partners
XMPP/MTLS/23456	Any	Internal Edge Server Interface IP	Internal XMPP traffic from the XMPP Gateway on the Front End Server or Front End pool to the Edge Server

⊟See Also

Tasks

Example XMPP Configuration – XMPP Federation with Google Talk

Other Resources

Manage XMPP Federated Partners for Your Organization

DNS Summary - Extensible Messaging and Presence Protocol (XMPP) Federation

See Also

Network Planning for Lync Server > Domain Name System (DNS) Requirements > DNS Requirements for Edge Servers and Features >

Topic Last Modified: *2012-10-20*

To configure extensible messaging and presence protocol (XMPP) for your deployment, you create two domain name system (DNS) records in an external DNS server that will resolve the records to the Access Edge service of your Edge Server or Edge pool.

DNS Summary for Extensible Messaging and Presence Protocol

Location/TYPE/Port	FQDN	IP address/FQDN host record	Maps to/Comments
External DNS/ SRV/5269	_xmpp-server._tcp.contoso.com	xmpp.contoso.com	XMPP proxy external interface on the Access Edge service or Edge pool.Repeat as necessary for all internal SIP domains with Lync enabled users where contact with XMPP contacts is allowed through the configuration of the External Access Policy through a global policy, site policy where the user is located, or user policy applied to the Lync-enabled user. An allowed XMPP domain must also be configured in the XMPP Federated Partners policy. See topics in **See Also** for additional details
External DNS/A	xmpp.contoso.com (for example)	IP address of Access Edge service on your Edge Server or Edge pool hosting XMPP proxy	Points to the Access Edge service or Edge pool that hosts the XMPP proxy service. Typically, the SRV record that you create will point to this host (A or AAAA) record

⊟See Also

Tasks

Setting Up XMPP Federation

Concepts

Determine DNS Requirements

1.3.9.10.9 Planning for Mobility

Planning for Mobility

Planning > Planning for External User Access > Scenarios for External User Access >

***Topic Last Modified:** 2013-02-14*

With Lync Server 2013, you can deploy the mobility feature to provide Lync 2013 functionality on mobile devices. This section provides details about the mobility feature and how to plan for your deployment.

- Mobility Features and Capabilities
- Topologies and Components for Mobility
- Technical Requirements for Mobility
- Defining Your Mobility Requirements
- Deployment Process for Mobility

1.3.9.10.9.1 Mobility Features and Capabilities

Mobility Features and Capabilities

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

***Topic Last Modified:** 2013-02-19*

`The information in this topic pertains to Cumulative Updates for Lync Server 2013`

The mobility feature introduced in the Cumulative Updates for Lync Server 2013: February 2013 supports Lync 2010 Mobile and Lync 2013 Mobile clients functionality. When you deploy the Lync Server 2013 Mobility Service, users can use supported Apple iOS, Android, and Windows Phone, or Nokia Symbian mobile devices to perform activities such as sending and receiving instant messages, viewing contacts, and viewing presence. In addition, mobile devices support some Enterprise Voice features, such as click to join a conference, Call via Work, single number reach, voice mail, and missed calls. New features introduced in the Cumulative Updates for Lync Server 2013: February 2013 include Voice over IP (VoIP) capability and video (H.264) for meeting attendee.

The mobility feature introduced in the Cumulative Updates for Lync Server 2013: February 2013 supports Lync 2013 Mobile client functionality. The Cumulative Updates for Lync Server 2013: February 2013 install Unified Communications Web API, or UCWA. UCWA is the component used for Lync 2013 Mobile clients. In Lync Server 2013, Mcx is used for Lync 2010 Mobile clients. Cumulative Updates for Lync Server 2013: February 2013 introduce UCWA as the new entry point for mobility services. Lync Server 2013 concurrently implements the Mobility Service (Mcx), introduced in the Cumulative Updates for Lync Server 2010: November 2011, and provides support for Lync 2010 Mobile. When you deploy the Cumulative Updates for Lync Server 2013: February 2013, users can use supported Apple iOS, Android, and Windows Phone mobile devices to perform such activities as:

> **Important:**
>
> Features supported by the Mobility Service from the Cumulative Updates for Lync Server 2010: November 2011 are noted with (Mcx). All listed features are supported by the UCWA, introduced in the Cumulative Updates for Lync Server 2013: February 2013.

- Send and receive instant messages (Mcx)
- View presence (Mcx)
- View contacts (Mcx)
- Click to join a conference (Mcx)
- Call via work (Mcx)
- Single number reach (Mcx)

- Voice mail (Mcx)
- Missed call notification (Mcx)
- Voice over IP (VoIP)
- Attendee video (H.264)

Note:
Lync 2010 Mobile provided a client for Nokia Symbian devices. Lync 2013 Mobile will not have a client for Nokia Symbian-based devices.

Apple iPad users will have access to enhanced capabilities. After joining a meeting by using audio call back, an iPad user will be able to view uploaded Microsoft PowerPoint presentations within a meeting, share applications and desktops, view the meeting participant list, and receive notifications of other content types that are being shared within the meeting.

Tip:
With single number reach, a user receives calls on a mobile phone that were dialed to the work number. With Call via Work, the user places an outbound call from the Lync Mobile client by using a work phone number instead of the mobile phone number. With dial-out, the client sends a request to Mcx or UCWA (based on the Lync Mobile version) to make the call for them. The server initiates the call and then calls the user back on the mobile phone. When the user answers, the server completes the call by dialing the other party. By using Call via Work, users can maintain their work identity during a call, which means that the call recipient does not see the caller's mobile number, and the caller avoids incurring outbound calling charges.

Note:
Not all features work exactly the same on all mobile devices. For details about features supported on mobile devices, see the Mobile Client Comparison Tables at http://go.microsoft.com/fwlink/p/?LinkId=234777. For details about supported devices and operating systems, see the requirements topics under Planning for Mobile Clients.

When you use the Lync Server 2013 Autodiscover feature, mobile applications can automatically locate Lync Server 2013 Web Services without requiring users to manually enter the URLs in their device settings. Manually entering URLs in mobile device settings is also supported, primarily for troubleshooting purposes.

Important:
The Mcx and UCWA are complimentary services and both are deployed to support Lync 2010 Mobile and Lync 2013 Mobile clients. Lync 2013 Mobile will not be able to sign in to Lync Server 2010 deployments. Lync 2010 Mobile and Lync 2013 Mobile will be able to use a Lync Server 2013 deployment with the Cumulative Updates for Lync Server 2013: February 2013 applied.

The mobility feature also supports *push notifications* for mobile devices that do not support applications running in the background. A push notification is a notification that is sent to a mobile device about an event that occurs while a mobile application is inactive. For example, a missed instant messaging (IM) invitation can result in a push notification.

Mcx, UCWA, Autodiscover Service, and support for push notifications are provided in Lync Server 2013. Updated client features, capabilities, and the use of UCWA as the mobility entry point are introduced in the Cumulative Updates for Lync Server 2013: February 2013.

1.3.9.10.9.2 Topologies and Components for Mobility

Topologies and Components for Mobility

See Also

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-17*

`The information in this topic pertains to Cumulative Updates for Lync Server 2013`

To support Lync mobile applications on mobile devices, Lync Server 2013 provides three services: Lync Server 2013 Mcx Mobility Service, Lync Server 2013 Autodiscover Service, and Lync Server 2013 Push Notification Service. The Cumulative Updates for Lync Server 2013: February 2013 adds a complimentary, but advanced, service for Lync 2013 Mobile clients—mobility support through the use of the Unified Communications Web API, or UCWA. This section briefly describes these components and identifies the Lync Server 2013 topologies that support mobility.

Note:

Mobility services are also available in hybrid deployments. You are not required to deploy services for supporting mobility if your users are homed online. You do need to define a setting for the Autodiscover Service to enable mobile users to find their online identity.

Important:

If you are planning any external user connectivity (for example, federation, external user access, or mobility features), you must use Edge Servers with Standard Edition server and the Front End Server or Front End pool. The Standard Edition server and the Front End Server or Front End pool do not have the necessary components to enable external users to access your internal deployment, or for the internal deployment to communicate with your external users. For all scenarios that include external users collaborating or communicating with internal users, including mobility, you must deploy at least one Edge Server and one reverse proxy.

Push notification uses a type of federation to the Lync Online services, which hosts the Push Notification Clearing House (PNCH). Push notification refers to the sound alerts, on-screen alerts (text), and badges that are pushed by applications to the Apple iPhone, iPad, and Windows Phone, when the mobile device is inactive. PNCH receives push notifications from Lync Server. When PNCH receives a notification of a message, PNCH forwards a notification to mobile clients through either the Apple Push Notification Services or Lync Server 2013 Push Notification Service, based on the mobile client that the message is intended for. PNCH is a required service for these mobile clients. To federate to Lync Online, PNCH uses Edge Servers and certificates to ensure confidentiality and authentication, policies, and correctly configured domain name system (DNS) records. Nokia Symbian and Android-based Lync Mobile clients do not use PNCH.

For details about planning and deploying Edge Servers, see Planning for External User Access and Deploying External User Access.

The Lync 2013 Mobile clients for Apple devices introduced with the Cumulative Updates for Lync Server 2013: February 2013 no longer use push notification or the push notification clearing house (PNCH). Lync 2013 Mobile clients on Windows Phone still use push notification and the (PNCH).

Mobility Components

The services that support mobility are as follows:

- **Lync Server 2013 Unified Communications Web API (UCWA)** Provides services for real-time communications with mobile and web clients in Lync Server 2013. When you deploy the Cumulative Updates for Lync Server 2013: February 2013 to the Front End Server and Director, the installation creates a virtual directory in the internal and external web services (Ucwa). A web component that is part of the Ucwa virtual directory accepts calls from UCWA-enabled clients. The client apps communicate over a REST interface for presence, contacts, instant messaging, VoIP, video conferencing, and collaboration. UCWA uses a P-GET based channel to send events, such as an incoming call, incoming instant message, or a message to the client app.

> **Note:**
> *REST* or representational state transfer, is a software architectural style for distributed systems that has been widely adopted in many forms and is well suited to the requirements of Web services in general.

- **Lync Server 2013 Mobility Service (Mcx)** This service supports Lync functionality, such as instant messaging (IM), presence, and contacts, on mobile devices. The Mobility Service is installed on every Front End Server in each pool that is to support Lync functionality on mobile devices. When you install Lync Server 2013, a new virtual directory (Mcx) is created under both the internal website and the external website on your Front End Servers.

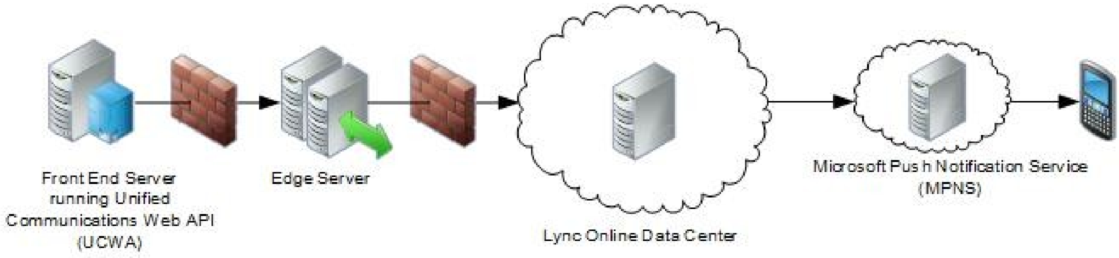
> **Important:**
> Lync Server 2013 with the Cumulative Updates for Lync Server 2013: February 2013 supports both the Mobility service introduced in the Cumulative Update for Lync Server 2010: November 2011, commonly known as Mcx, and the UCWA web component. The combination of these two mobility services provides interoperability and use by users with Lync 2010 Mobile and Lync 2013 Mobile clients on Lync Server 2013.

- **Lync Server 2013 Autodiscover Service** This service identifies the location of the user and enables mobile devices and other Lync clients to locate resources—such as the internal and external URLs for Lync Server 2013 Web Services, and the URL for the Mcx or UCWA—regardless of network location. Automatic discovery uses hardcoded host names (lyncdiscoverinternal for users inside the network; lyncdiscover for users outside the network) and the SIP domain of the user. It supports client connections that use either HTTP or HTTPS.
  The Autodiscover Service is installed on every Front End Server and on every Director in each pool that is to support Lync functionality on mobile devices. When you install the Autodiscover Service, a new virtual directory (Autodiscover) is created under both the internal website and the external website, on both Front End Servers and Directors.

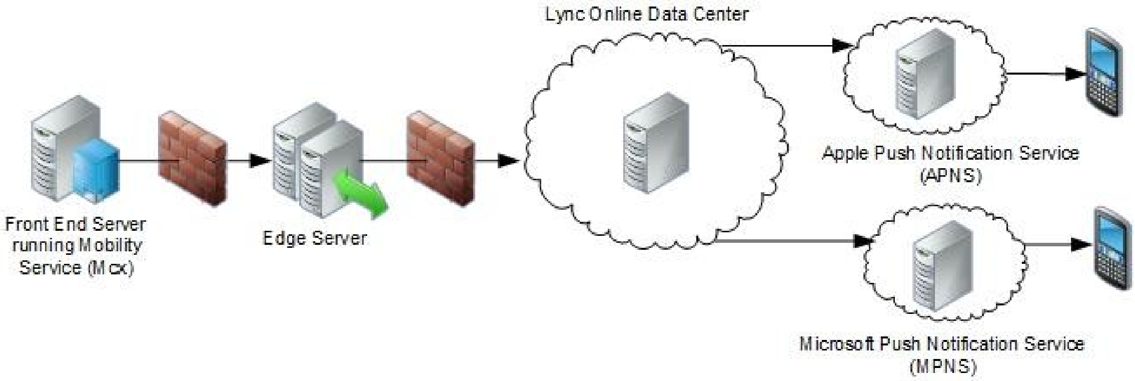
> **Note:**
> The Autodiscover Service is listed here because it remains a critical component when providing mobile client services. The role of Autodiscover in Lync Server 2013 has been expanded to provide services for all clients. For details about planning for the Autodiscover Service, see Planning for Autodiscover.

- **Push Notification Service** This service is a cloud-based service that is located in the Lync Online data center. When the Lync mobile application on a supported Apple iOS device or Windows Phone is inactive, it cannot respond to new events, such as a new instant messaging (IM) invitation, a missed instant message, a missed call, or voice mail, because these devices do not support mobile applications running in the background. In these cases, a notification of the new event—called a *push notification*—is sent to the mobile device. The Mobility Service sends the notification to the cloud-based Push Notification Service, which then sends the notification either to the Apple Push Notification Service (APNS) (for supported Apple iOS devices) or to the Microsoft Push Notification Service (MPNS) (for Windows Phone), which then sends it on to the mobile device. The user can then respond to the notification on the mobile device to activate the application.
  The Lync 2010 Mobile on Apple and Windows Phone devices use push notifications. The Lync 2013 Mobile client for Apple devices introduced with the Cumulative Updates for Lync Server 2013: February 2013 no longer uses push notification or the push notification clearing house (PNCH).

The following diagram illustrates how the Push Notification Service fits within a Lync Server 2013 topology that uses UCWA and Lync 2013 Mobile clients.


Front End Server running Unified Communications Web API (UCWA)
Edge Server
Lync Online Data Center
Microsoft Push Notification Service (MPNS)

Introduced in Cumulative Update for Lync Server 2010: November 2011, the Mcx service provides services to Lync 2010 Mobile clients. The following diagram illustrates the Push Notification Service as it applies to a topology using Mcx and Lync 2010 Mobile clients.


Lync Online Data Center
Apple Push Notification Service (APNS)
Front End Server running Mobility Service (Mcx)
Edge Server
Microsoft Push Notification Service (MPNS)

Supported Topologies

Applying the Cumulative Updates for Lync Server 2013: February 2013 adds the UCWA web components to support mobility for Lync 2013 Mobile client features in the following topologies:

- Lync Server 2013 Standard Edition
- Lync Server 2013 Enterprise Edition

The Edge Server can be a Lync Server 2010 Edge Server.

A Lync Server 2013 deployment without the Cumulative Updates for Lync Server 2013: February 2013 will use the Mcx Mobility Service and can provide services only for Lync 2010 Mobile.

Important:
The Mobility Service is supported on Front End Servers that is collocated with the Mediation Server role with two network interfaces, but you must take appropriate steps to configure the interfaces. You must assign the IP addresses to the specific interface that will communicate as the Mediation Server, and the network interface IP that will communicate as the Front End Server. You can do this in Topology Builder by selecting the correct IP address for each service, instead of using the default **Use all configured IP addresses**.

See Also

Other Resources

Planning for External User Access
Deploying External User Access
Planning for Autodiscover

1.3.9.10.9.3 Technical Requirements for Mobility

Technical Requirements for Mobility

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-19*

Some information in this topic pertains to Cumulative Updates for Lync Server 201

Mobile users encounter various mobile application scenarios that require special planning. For example, someone might start using a mobile application while away from work by connecting through the 3G network, then switch to the corporate Wi-Fi network when arriving at work, and then switch back to 3G when leaving the building. You need to plan your environment to support such network transitions and guarantee a consistent user experience. This section describes the infrastructure requirements that you must have in order to support mobile applications and automatic discovery of mobility resources.

Note:

Although mobile applications can also connect to other Lync Server 2013 services, the requirement to send all mobile application web requests to the same external web fully qualified domain name (FQDN) applies only to the Lync Server 2013 Mobility Service. Other mobility services do not require this configuration.

The requirement for cookie affinity in hardware load balancers is dramatically reduced, and you substitute Transmission Control Protocol (TCP) affinity if you are using the Lync Mobile delivered with Lync Server 2013. Cookie affinity can still be used, but the web services no longer require it.

Important:

All Mobility Service traffic goes through the reverse proxy, regardless of where the origination point is—internal or external. In the case of a single reverse proxy or a farm of reverse proxies, or a device that is providing the reverse proxy function, an issue can arise when the internal traffic is egressing through an interface and attempting to immediately ingress on the same interface. This often leads to a Security rule violation known as TCP packet spoofing or just spoofing. *Hair pinning* (the egress and immediate ingress of a packet or series of packets) must be allowed in order for mobility to function. One way to resolve this issue is to use a reverse proxy that is separate from the firewall (the spoofing prevention rule should always be enforced at the firewall, for security purposes). The hairpin can occur at the external interface of the reverse proxy instead of the firewall external interface. You detect the spoofing at the firewall, and relax the rule at the reverse proxy, thereby allowing the hairpin that mobility requires.
Use the Domain Name System (DNS) host or CNAME records to define the reverse proxy for the hairpin behavior (not the firewall), if at all possible.

Lync Server 2013 supports mobility services for Lync 2010 Mobile and Lync 2013 mobile clients. Both clients use the Lync Server 2013 Autodiscover Service to find its mobility entry point, but differ on which mobility service they use. Lync 2010 Mobile uses the Mobility Service known as *Mcx*, introduced with the Cumulative Update for Lync Server 2010: November 2011. Lync 2013 mobile clients use the Unified Communications Web API, or *UCWA*, as their mobility service provider.

Internal and External DNS Configuration

The Mobility Services Mcx (introduced with the Cumulative Update for Lync Server 2010: November 2011) and UCWA (introduced in the Cumulative Updates for Lync Server 2013: February 2013) use DNS in the same way.

When you use Automatic Discovery, mobile devices use DNS to locate resources. During the DNS lookup, a connection is first attempted to the FQDN that is associated with the internal DNS record (lyncdiscoverinternal.<*internal domain name*>). If a connection cannot be made by using the internal DNS record, a connection is attempted by using the external DNS record (lyncdiscover.<*sipdomain*>). A mobile device that is internal to the network connects to the internal Autodiscover Service URL, and a mobile device that is external to the network connects to the external Autodiscover Service URL. External Autodiscover requests go through the reverse proxy. The Lync Server 2013 Autodiscover Service returns all Web Services URLs for the user's home pool, including the Mobility Service (Mcx and UCWA) URLs. However, both the internal Mobility Service URL and the external Mobility Service URL are associated with the external Web Services FQDN. Therefore, regardless of whether a mobile device is internal or external to the network, the device always connects to the Lync Server 2013 Mobility Service externally through the reverse proxy.

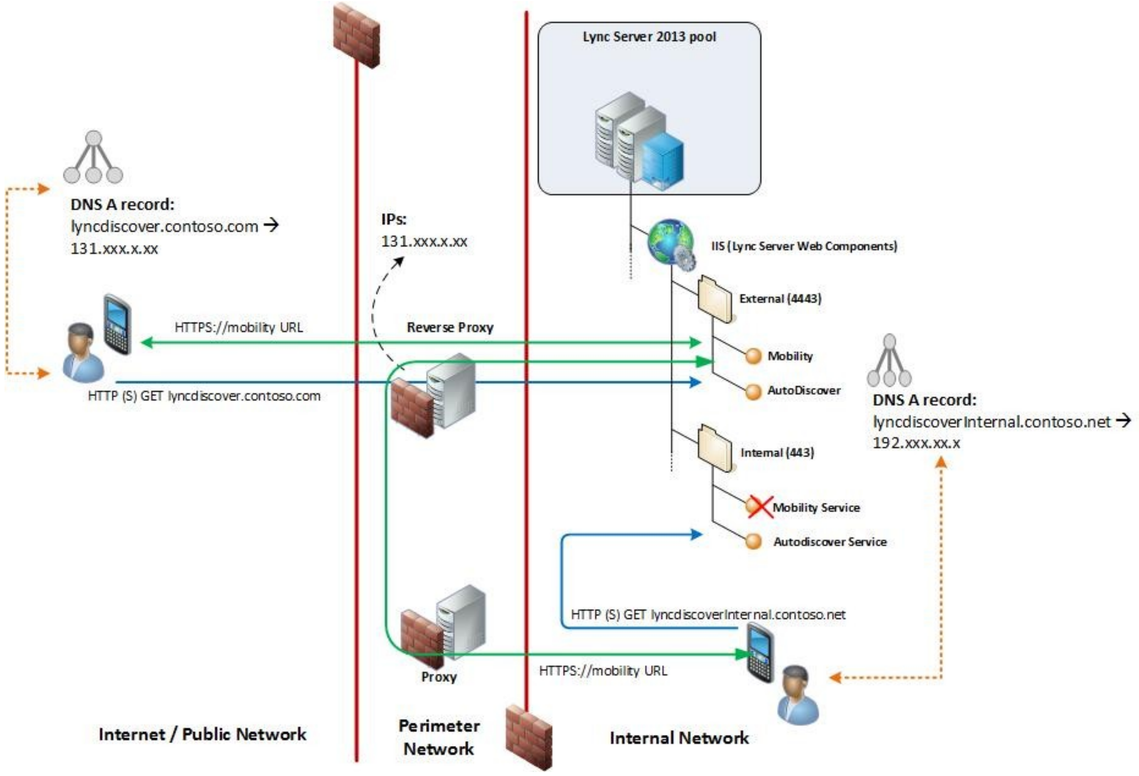
Note:

It is important to understand that your deployment can consist of multiple distinct namespaces for internal and external use. Your SIP domain name may be different than the internal deployment domain name. For example, your SIP domain may be **contoso.com**, while your internal deployment may be **contoso.net**. Users who log in to Lync Server will use the SIP domain name, such as **john@contoso.com**. When addressing the external web services (defined in Topology Builder as **External web services**), the domain name and the SIP domain name will be consistent, as defined in DNS. When addressing the internal Web services (defined in Topology Builder as **Internal web services**), the default name of the internal web services will be the FQDN of the Front End Server, Front End pool, Director, or Director pool. You have the option to override the internal web services name. You should use the internal domain name (and not the SIP domain name) for internal web services and define the DNS host A (or, for IPv6, AAAA) record to reflect the overridden name. For example, the default internal web services FQDN may be **pool01.contoso.net**. An overridden internal web services FQDN may be **webpool.contoso.net**. Defining the web services in this way helps to ensure that the internal and external locality of the services—and not the locality of the user who is using them—is observed.

However, because the web services are defined in Topology Builder and the internal web services name can be overridden, as long as the resulting web services name, the certificate that validates it, and the DNS records that define it, are consistent, you can define the internal web services with any domain name—including the SIP domain name—that you want. Ultimately, the resolution for the name to the IP address is determined by DNS host records and a consistent namespace.

For the purposes of this topic and the examples, the internal domain name is used to illustrate the topology and the DNS definitions.

The following diagram illustrates the flow of mobile application web requests for the Mobility Service and for the Autodiscover Service when using an internal and external DNS configuration.



Note:

The diagram illustrates generic web services. A virtual directory named Mobility depicts the Mobility services Mcx and/or UCWA. If you have not applied the Cumulative Updates for Lync Server 2013: February 2013, you may or may not have the virtual directory Ucwa defined on your internal and external Web services. You will have a virtual directory Autodiscover, and you may have a virtual directory Mcx.
Autodiscover and the discovery of services work the same way, regardless of the mobility services technology that you have deployed.

To support mobile users from both inside and outside the corporate network, your internal and external web FQDNs must meet some prerequisites. In addition, you may need to meet other requirements, depending on the features you choose to implement:

- New DNS, CNAME or A (host, if IPv6, AAAA) records, for automatic discovery.
- New firewall rule, if you want to support push notifications through your Wi-Fi network.
- Subject alternative names on internal server certificates and reverse proxy certificates, for automatic discovery.
- Front End Server hardware load balancer configuration changes source affinity.
- .

Your topology must meet the following requirements to support the Mobility Service and the Autodiscover Service:

- The Front End pool internal web FQDN must be distinct from the Front End pool external web FQDN.
- The internal web FQDN must only resolve to and be accessible from inside the corporate network.
- The external web FQDN must only resolve to and be accessible from the Internet.
- For a user who is inside the corporate network, the Mobility Service URL must be addressed to the external web FQDN. This requirement is for the Mobility

Service and applies only to this URL.
- For a user who is outside the corporate network, the request must go to the external web FQDN of the Front End pool or Director.

If you support automatic discovery, you need to create the following DNS records for each SIP domain:

- An internal DNS record to support mobile users who connect from within your organization's network.
- An external, or public, DNS record to support mobile users who connect from the Internet.

The internal automatic discovery URL should not be addressable from outside your network. The external automatic discovery URL should not be addressable from within your network. However, if you cannot meet this requirement for the external URL, mobile client functionally will probably not be affected, because the internal URL is always tried first.

The DNS records can be either CNAME records or A (host, if IPv6, AAAA) records.

Note:
Mobile device clients do not support multiple Secure Sockets Layer (SSL) certificates from different domains. Therefore, CNAME redirection to different domains is not supported over HTTPS. For example, a DNS CNAME record for lyncdiscover.contoso.com that redirects to an address of director.contoso.net is not supported over HTTPS. In such a topology, a mobile device client needs to use HTTP for the first request, so that the CNAME redirection is resolved over HTTP. Subsequent requests then use HTTPS. To support this scenario, you need to configure your reverse proxy with a web publishing rule for port 80 (HTTP). For details, see "To create a web publishing rule for port 80" in Configuring the Reverse Proxy for Mobility. CNAME redirection to the same domain is supported over HTTPS. In this case, the destination domain's certificate covers the originating domain.

For details about the DNS records required for your scenario, see DNS Summary - Autodiscover.

Port and Firewall Requirements

If you support push notifications and want Apple mobile devices to receive push notifications over your Wi-Fi network, you also need to open port 5223 on your enterprise Wi-Fi network. Port 5223 is an outbound TCP port used by the Apple Push Notification Service (APNS). The mobile device initiates the connection. For details, see http://support.apple.com/kb/TS1629 .

⚠**Warning:**
An Apple device using the Lync 2013 Mobile client does not require push notifications.

For additional details and guidance on port and protocol requirements for Autodiscover, see Port Summary - Autodiscover.

Certificate Requirements

If you support automatic discovery for Lync mobile clients, you need to modify the subject alternative name lists on certificates to support secure connections from the mobile clients. You need to request and assign new certificates, adding the subject alternative name entries described in this section, for each Front End Server and Director that runs the Autodiscover Service. The recommended approach is to also modify the subject alternative names lists on certificates for your reverse proxies. You need to add subject alternative name entries for every SIP domain in your organization.

Reissuing certificates by using an internal certificate authority is typically a simple process, but adding multiple subject alternative name entries to public certificates used by the reverse proxy can be expensive. If you have many SIP domains, making the addition of subject alternative names very expensive, you can configure the reverse proxy to make the initial Autodiscover Service request over port 80 using HTTP, instead of port 443 using HTTPS (the default configuration). The request is then redirected to port 8080 on the Director or Front End pool. When you publish the initial Autodiscover Service request on port 80, you do not need to change certificates for the reverse proxy, because the request uses HTTP rather than HTTPS. This approach is supported, but we do not recommend it.

Internet Information Services (IIS) Requirements

We recommend that you use IIS 7.5 or IIS 8.0 for mobility. The Mobility Service installer sets flags in ASP.NET to improve performance. IIS 7.5 is installed by default on Windows Server 2008 R2 and IIS 8.0 is installed on Windows Server 2012. The Mobility Service installer automatically changes the ASP.NET settings.

Hardware Load Balancer Requirements

On the hardware load balancer that is supporting the Front End pool, the external Web Services virtual IPs (VIPs) for Web Services traffic must be configured for source. Source affinity helps to ensure that multiple connections from a single client are sent to one server to maintain session state. For details about affinity requirements, see Load Balancing Requirements.

If you plan to support Lync mobile clients only over your internal Wi-Fi network, you should configure the internal Web Services VIPS for source as described for external Web Services VIPs. In this situation, you should use source_addr (or TCP) affinity for the internal Web Services VIPs on the hardware load balancer. For details, see Load Balancing Requirements.

Reverse Proxy Requirements

If you support automatic discovery for Lync mobile clients, you need to update the current publishing rule as follows:

- If you decide to update the subject alternative names lists on the reverse proxy certificates and use HTTPS for the initial Autodiscover Service request, you must update the web publishing rule for lyncdiscover.<*sipdomain*>. Typically, this is combined with the publishing rule for the external Web Services URL on the Front End pool.
- If you decide to use HTTP for the initial Autodiscover Service request so that you do not need to update the subject alternative names list on the reverse proxy certificates, you must create a new web publishing rule for port HTTP/ TCP 80, if one does not already exist. If a rule for HTTP/TCP 80 does already exist, you can update that rule to include the lyncdiscover.<*sipdomain*> entry.

1.3.9.10.9.4 Autodiscover Service Requirements

Autodiscover Service Requirements

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-25*

The Microsoft Lync Server 2013 Autodiscover Service runs on the Director and Front End pool servers, and when published in DNS, can be used by mobile devices running Lync Mobile to locate mobility services. Before mobile devices running Lync Mobile can take advantage of automatic discovery, you need to modify certificate subject alternative name lists on any Director and Front End Server running the Autodiscover Service. In addition, it may be necessary to modify the subject alternative name lists on certificates used for external web service publishing rules on reverse proxies.

For details about the subject alternative name entries that are required for Directors, Front End Servers, and reverse proxies, see Technical Requirements for Mobility in Planning for Mobility.

The decision about using subject alternative name lists on reverse proxies is based on whether you publish the Autodiscover Service on port 80 or on port 443:

- **Published on port 80** No certificate changes are required if the initial query to the Autodiscover Service occurs over port 80. This is because mobile devices running Lync will access the reverse proxy on port 80 externally and then be redirected to a Director or Front End Server on port 8080 internally. For details, see the "Initial Autodiscover Process Using Port 80" section later in this topic.
- **Published on port 443** The subject alternative name list on certificates used by the external web services publishing rule must contain a *lyncdiscover.<sipdomain>* entry for each SIP domain within your organization.

Reissuing certificates using an internal certificate authority is typically a simple process but for public certificates used on the web service publishing rule, adding multiple subject alternative name entries can become expensive. To work around this issue, we support the initial automatic discovery connection over port 80, which is then redirected to port 8080 on the Director or Front End Server.

For example, assume that a mobile client running Lync Mobile is configured to sign in to Lync Server 2013 using the automatic discovery feature using HTTP for the initial request.

Initial Autodiscover Process for Mobile Devices Using Port 80

1. Mobile device running Lync Mobile looks up lyncdiscover.contoso.com using DNS, where an A record exists.
2. External DNS returns the IP address for the external web services to the client.
3. Mobile device running Lync Mobile sends request http:// lyncdiscover.contoso.com?sipuri=lyncUser1@contoso.com to the reverse proxy
4. The web publishing rule will bridge the request from port 80 externally to port 8080 internally, which will then route it to either a Director or Front End Server.
   Since the request is HTTP and not HTTPS, no modifications are needed to the certificate on the external web service publishing rule to support the Autodiscover Service.
5. The Autodiscover Service returns the external web service URLs (in HTTPS format).
6. The mobile device running Lync Mobile can then reconnect to the reverse proxy on port 443 and is redirected over 4443 to the mobility service running on the user's home pool.
   Since the HTTPS query is to the external web services URL vs. the Autodiscover Service URL, it succeeds because the certificate will already

contain subject alternative name entries for the external web services fully qualified domain names (FQDNs).
In this scenario, there are no certificate changes required to support mobility.

> **Note:**
> If the target web server has a certificate that does not have a matching value for lyncdiscover.contoso.com as a subject alternative name list value:
> a. Web server responds with a "Server Hello" and no certificate.
> b. Mobile device running Lync Mobile immediately terminates the session.
> If the target web server has a certificate that includes lyncdiscover.contoso.com as a subject alternative name list value:
> a. Web server responds with a "Server hello" and a certificate.
> b. Mobile device running Lync Mobile validates the certificate and completes the handshake.

To support an initial connection to the Autodiscover Service using port 80 on your reverse proxy server, you can create an http publishing rule similar to this example for a Forefront Threat Management Gateway 2010 reverse proxy web publishing rule:

1. Create a new web publishing rule (for example, **Lync Server Autodiscover (HTTP)**).
2. In **Public Name**, enter lyncdiscover.contoso.com.
3. On the **Bridging** tab, select only the option to bridge requests from Port 80 to Port 8080.
4. On the **Authentication** tab, select **No authentication**, and **Client cannot authenticate directly**.
5. Commit changes, and move the rule to the top of the list of Lync rules (first in processing order).

Mobility for the Split Domain Deployment

A shared SIP address space, also known as a *split-domain*, or a *hybrid deployment* is a configuration where users are deployed across an on-premise deployment and an online environment. The desired outcome is to have a user, regardless of where their home server is located (on-premise or online), to log into the deployment and be redirected to their home server location. To accomplish this, the Autodiscover feature of Microsoft Lync Server 2013 is used to redirect the online user to the online topology. This is done by configuring the Autodiscover uniform resource locator (URL) by using the Lync Server Management Shell and the cmdlets **Get-CsHostingProvider** and **Set-CsHostingProvider**.

You will need to collect and record the following deployed attributes:

- From the Lync Server Management Shell, type

```
Get-CsHostingProvider
```

- In the results, find the online provider with the attribute **ProxyFQDN**. For example, sipfed.online.lync.com
- Record the value of the ProxyFQDN
- Enable federation in the on-premise Lync Server Control Panel, allowing federation with the online provider
- Enable federation for the online provider. By default, all online users are enabled for domain federation and can communicate with all domains
- If you will define blocked and allowed domains, determine the domains that you will explicitly allow or explicitly block
- For online federation, you must plan for firewall exceptions, certificates and DNS host (A or AAAA, if using IPv6) records. Additionally, you must configure federation policies. For details, see Planning for Lync Server and Office Communications Server Federation

1.3.9.10.9.5 Defining Your Mobility Requirements

Defining Your Mobility Requirements

See Also

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-14*

Some information in this topic pertains to Cumulative Updates for Lync Server 201

During the planning phase for the Lync Server 2013 mobility feature, when you are using Lync 2010 Mobile and Lync 2013 Mobile clients, you make decisions that determine your deployment steps.

Here are the decisions that you must consider:

- **Do you want to use automatic discovery for Lync mobile clients?**
  If you want to support automatic discovery, you need to create new internal and external Domain Name System (DNS) records, add subject alternative names to certificates on the Front End Servers, Directors, and reverse proxy, and modify the existing publishing rules on the reverse proxy. For details, see Technical Requirements for Mobility. With automatic discovery, users can automatically locate Lync Server 2013 Web Services from anywhere inside or outside the corporate network, without entering URLs in their mobile device settings.
  If you use manual settings instead of automatic discovery, mobile users need to manually enter the following URLs in their mobile devices:
    - https://<ExtPoolFQDN>/Autodiscover/autodiscoverservice.svc/Root for external access
    - https://<IntPoolFQDN>/AutoDiscover/ autodiscoverservice.svc/Root for internal access

  We strongly recommend using automatic discovery. The primary use of manual settings is for troubleshooting.
- **If you decide to support automatic discovery, are you willing to update certificates on the reverse proxy with subject alternative names for each SIP domain?**
  If you have many SIP domains, updating public certificates on the reverse proxy can become very expensive. If this is the case, you can choose to implement automatic discovery so that the initial Autodiscover Service request uses HTTP on port 80, instead of using HTTPS on port 443. However, this is not the recommended approach. If you decide to choose this alternative, you do not need to update the certificates on the reverse proxy, but you need to create a web publishing rule for HTTP on port 80. For more details, see Technical Requirements for Mobility.
- **Do you want to support Lync mobile clients both internal and external to the corporate network, or support clients only inside the corporate network?**
  If you want to support mobile clients internal and external to your network, mobile devices can access mobility features from any location. The default configuration is to support clients both internal and external to the corporate network.
  Although the default configuration enables mobile client traffic to go through the external site, you can restrict mobile client traffic to the internal corporate network. When you restrict the traffic to the internal network, users can use Lync mobile applications on their mobile devices only when they are inside the network.
  For deployments that support mobility using the Mcx mobility service and Lync 2010 Mobile, you run the **Set-CsMcxConfiguration** cmdlet. To set mobility for internal use only, you would use a command similar to the following:

```
Set-CsMcxConfiguration -Identity site:Redmond -ExposedWebURL Internal
```

Note:

There are no additional configurations required for UCWA. UCWA does not have an equivalent internal-only configuration.

Important:

If you are using a Lync Server 2013 Front End Server or Front End pools and **you do not have** any Lync Server 2010 Front End Servers or Front End pools, **there is no requirement for cookie-based persistence**. If you need to retain any Lync Server 2010 Front End Servers or Front End pools, the same rules still apply as in Lync Server 2010 for cookie-based persistence.

- **Do you want to support push notifications for Apple iOS devices and Windows Phones?**
  If you support push notifications, supported Apple iOS devices and Windows Phones receive a notification of events that occur when the mobile application is inactive. You must configure your Edge Server to have a federation relationship with the cloud-based Lync Server Push Notification Service, which is located in the Lync Online datacenter, and run a cmdlet to enable push notifications.
  If you want to support push notifications over your Wi-Fi network, in addition to supporting push notifications over the mobile device providers' 3G or data networks, you must open port 5223 outbound on your enterprise Wi-Fi network. Supporting push notifications over the Wi-Fi network supports mobile devices that use only Wi-Fi and mobile devices that have poor indoor reception.

  Important:

  Opening port TCP 5223 is required only when supporting Apple devices running the Lync 2010 Mobile client.

  If you do not support push notifications, users of Apple mobile devices and Windows Phones will not find out about events—such as instant message invitations or missed messages—that occur when the mobile application is inactive.

  Note:

  Lync 2013 Mobile clients on Apple devices do not require push notification. The Lync 2013 Mobile clients on Windows Phone use push notification. Planning for push notification and the push notification clearinghouse remain the same for Lync Mobile on Windows Phone and Apple devices that are not able to run the Lync 2013 Mobile client.

- **Do you want all users to have access to mobility features, or do you want to be able to specify which users have access to these features?**
  The table describes features available to users in Lync Server 2013. The defaults allow Call via Work, allow Voice over IP (VoIP), and enable Mobility. Here is the full set of available options:

Feature/Paramater Name/Scope (Policy parameter names may not be the same)	Description	Introduced
Enable Mobility Parameter Name : `EnableMobility` Scope: Global/Site/User	Administrative setting to control users in a given scope that have the Lync Mobile installed, If the policy is set to False, the user would not be able to sign into the client. The default setting is	Cumulative Update for Lync Server 2010: November 2011

	True.	
Enable Outside Voice Parameter Name : `EnableOutsideVoice` Scope: Global/Site/User	Controls a user's ability to use Call Via Work, a feature that enables users to make and receive calls by using their work number instead of their mobile number. If set to False, the user will not be able to make or receive calls by using their work number from their mobile device. The default setting is True	Cumulative Update for Lync Server 2010: November 2011
Enable IP Audio and Video Parameter Name : `EnableIPAudioVideo` Scope: Global/Site/User	Controls whether a user can use VoIP to make or receive voice or video calls on their mobile device. If set to False, the user will not be able to make or receive VoIP or video calls on their device. The default setting is True.	Microsoft Lync Server 2013
Require WiFi for IP Audio Parameter Name : `RequireWiFiForIPAudio` Scope: Global/Site/User	This setting defines whether the client will be required to make and receive calls over VoIP on WiFi instead of the cellular data network. If set to True, the user can make and receive VoIP calls only when connected to a WiFi network. The default setting is False.	Microsoft Lync Server 2013
Require WiFi for IP Video Parameter Name : `RequireWiFiForIPVideo` Scope: Global/Site/User	This setting defines whether the client will be required to make and receive video calls on Wi-Fi instead of on the cellular data network. If set to True, the user can make and receive video calls only when connected to a Wi-Fi network. The default setting is False.	Microsoft Lync Server 2013

For a description of the policy settings that you can configure, and how to manage the policies, see New-CsMobilityPolicy, Set-CsMobilityPolicy, Get-CsMobilityPolicy, Grant-CsMobilityPolicy and Remove-CsMobilityPolicy.

- **Do you want users who are not enabled for Enterprise Voice to be able to**

use Click to Join to join conferences?
For users to have access to mobility features and Call via Work, they must be enabled for Enterprise Voice. However, users who are not enabled for Enterprise Voice can join conferences by clicking the link on their mobile device, if they have an appropriate voice policy assigned to them. You can either assign a specific voice policy to these users or make sure that a global policy or site-level policy exists that applies to them. The voice policy that you assign must have public switched telephone network (PSTN) usage records and routes that define the areas to which users can dial out to join a conference. For details about setting voice policy, PSTN usage records, and routes, see Configuring Voice Policies, PSTN Usage Records, and Voice Routes.

> **Note:**
> Mobile users who want to use Click to Join require a voice policy, along with the related PSTN usage records and voice routes, because clicking the link on the mobile device results in an outbound call from Lync Server 2013.

Concepts

Technical Requirements for Mobility

Other Resources

Configuring Voice Policies, PSTN Usage Records, and Voice Routes

1.3.9.10.9.6 Deployment Process for Mobility

Deployment Process for Mobility

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-19*

```
Some information in this topic pertains to Cumulative Updates for Lync Server 201
```

This section describes the sequence of steps required to deploy the Lync Server 2013 mobility feature.

Mobility Deployment Process

Phase	Steps	Permissions	Deployment documentation
Create Domain Name System (DNS) records	• Create an internal DNS CNAME or A (host, if IPv6, AAAA) record to resolve the internal Autodiscover Service URL. • Create an external DNS CNAME or A (host, if IPv6, AAAA) record to resolve the external Autodiscover Service URL.	Domain Admins DnsAdmins	Creating DNS Records for the Autodiscover Service
Modify certificates	Add subject alternative name entries to the following certificates to support secure connections for mobile users: • Director certificate • Front End pool certificate	Local administrator	Modifying Certificates for Mobility

	• Reverse proxy certificate		
Configure the reverse proxy	• Assign certificates updated with subject alternative names to the Secure Sockets Layer (SSL) Listener. • Reconfigure the web publishing rule for the external Autodiscover Service URL. • Be sure that a web publishing rule exists for the external Lync Server 2013 Web Services URL on your Front End pool. Or • If you choose to use HTTP for the initial Autodiscover request and do not update subject alternative name lists on the certificates, configure a new web publishing rule or reconfigure an existing publishing rule for port 80 HTTP.	Local administrator	Configuring the Reverse Proxy for Mobility
Test your mobility deployment for Lync 2010 Mobile using the Mcx Mobility Service	Run **Test-CsMcxP2PIM** to test sending an instant message from one person to another. See the Lync Server Management Shell cmdlet documentation for Test-CsMcxP2PIM for a complete list of options.	CsAdministrator	Verifying Your Mobility Deployment
Test your mobility deployment for Lync 2013 Mobile clients using the UCWA Web components	Use the **Test-CsUcwaConference** cmdlet to test and verify that pre-defined test users or a pair of actual users can use UCWA to create and participate in a conference. See the Lync Server Management Shell cmdlet documentation for Test-CsUcwaConference for a complete list of options.	CsAdministrator	Verifying Your Mobility Deployment

Configure for push notifications	- For Lync Server 2013 Edge Servers, add a Lync Server online hosting provider and configure hosting provider federation. - For Lync Server 2010 Edge Servers, add a Lync Server online hosting provider and configure hosting provider federation. - For Office Communications Server 2007 R2 Edge Servers, add a federated partner. - If you want to support push notifications over a Wi-Fi network, configure a firewall rule outbound for TCP port 5223. - Use the **Set-CsPushNotificationConfiguration** cmdlet to enable push notifications to the Apple Push Notification Service (APNS) and Microsoft Push Notification Service (MPNS). This feature is disabled by default. - Use the **Test-CsFederatedPartner** cmdlet to test the federation configuration and the **Test-CsMCXPushNotification** cmdlet to test push notifications. **Note:** Push notifications are used for Lync 2010 Mobile clients on Apple devices and Windows Phone Push notification is required for Lync 2013 Mobile clients on Windows Phone	RtcUniversalServerAdmins	Configuring for Push Notifications

	only		
Configure mobility policy	Use the **Set-CsMobilityPolicy** cmdlet to allow or disallow: • Call via Work • Enable IP Audio and IP Video • Require WiFi for IP Audio and/or IP Video	CsAdministrator	Configuring Mobility Policy

1.3.9.10.10 Scenarios for the Director

Scenarios for the Director

See Also

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2012-10-22*

A Director is a server running Microsoft Lync Server 2013 communications software that can authenticate user requests, but does not home any user accounts. The Director also hosts web services similar to the Front End Server and will authenticate web ticket requests and provide other services.

Important:

If you deploy Directors, you must publish the Director web services externally through the reverse proxy as well as the web services of the Front End Server. The topics following describe the planning process for the possible Director topologies.

- Overview of the Director
- Components Required for the Director
- Hardware and Software Requirements for the Director
- Single Director
- Scaled Director Pool

See Also

Concepts

Supported Lync Server 2013 Topologies
Server Hardware Platforms

1.3.9.10.10.1 Overview of the Director

Overview of the Director

Planning for External User Access > Scenarios for External User Access > Scenarios for the Director >

Topic Last Modified: *2012-09-08*

A Director is a server running Lync Server 2013 that authenticates user requests, but does not home any user accounts. You optionally can deploy a Director in the following two scenarios:

- If you enable access by external users by deploying Edge Servers, you should also deploy a Director. In this scenario, the Director authenticates the external users, and then passes their traffic on to internal servers. When a Director is used to authenticate external users, it relieves Front End pool servers from

the overhead of performing authentication of these users. It also helps insulate internal Front End pools from malicious traffic such as denial-of-service attacks. If the network is flooded with invalid external traffic in such an attack, this traffic ends at the Director.
- If you deploy multiple Front End pools at a central site, by adding a Director to that site you can streamline authentication requests and improve performance. In this scenario, all requests go first to the Director, which then routes them to the correct Front End pool.

1.3.9.10.10.2 Components Required for the Director

Components Required for the Director

Planning for External User Access > Scenarios for External User Access > Scenarios for the Director >

Topic Last Modified: *2012-09-08*

The only component required to create and configure a Director is to deploy the Director server role. You do this by using Topology Builder and define either a single computer pool or a multiple computer pool in the Director pool node. After you have defined the Director or Director pool, run the Lync Server Deployment Wizard on the computer that will be a Director. In the case of a Director pool, you run the Lync Server Deployment Wizard on each server that will be a member of the pool.

Topologies

You can implement a single Director server or a Director pool. The Director is always a separate server or pool, not collocated with any other server role in Lync Server 2013.

Note:

If you do not deploy Directors, the Front End Server or Front End pool will assume the Director role.

A pool of Directors must be load balanced. You can do one of the following:

- Create a topology that uses a hardware load balancer for web services and Domain Name System (DNS) load balancing for the other traffic types.
  Scaled Director Pool - DNS Load Balancing and Hardware Load Balancer
- Create a topology that uses a hardware load balancer for load balancing needed for the Director pool.
  Scaled Director Pool - Hardware Load Balancer

1.3.9.10.10.3 Hardw are and Softw are Requirements for the Director

Hardware and Software Requirements for the Director

Planning for External User Access > Scenarios for External User Access > Scenarios for the Director >

Topic Last Modified: *2012-10-20*

This section details the hardware and software requirements for the Director, and the supported collocation scenarios for the Director.

Hardware Requirements for the Director

The following table lists the hardware requirements for the Director:

Hardware Requirements for the Director

Hardware component	Minimum requirement
CPU	• 64-bit processor, quad-core, 2.0 GHz or higher • 64-bit dual processor, dual-core, 2.0 GHz or higher
Memory	4 gigabytes (GB)
Disk	• 10K RPM hard disk drive (HDD) • High-performance solid state drive (SSD) with performance equal to or better than 10K RPM HDD • 2x RAID 10 (striped and mirrored) 15K RPM disks for database data files
Network	• Dual 1 gigabit per second (Gbps) network adapters (recommended) • Single 1 Gbps network adapter (supported)

Software Requirements for the Director

The Director role can be deployed only on servers running Lync Server 2013 Enterprise Edition.

One of the following 64-bit operating systems is required for the Directors:

- The Windows Server 2008 R2 Standard operating system with Service Pack 1
- The Windows Server 2008 R2 Enterprise operating system with Service Pack 1
- The Windows Server 2008 R2 Datacenter operating system with Service Pack 1
- The Windows Server 2012 Standard operating system
- The Windows Server 2012 Datacenter operating system

Lync Server 2013 also requires installation of the following programs and updates detailed in the topic Additional Server Support and Requirements.

Supported Collocation

The Director server role cannot be collocated with any other server role in Lync Server 2013. However, if you do not deploy a Director, the Front End Servers will assume the role.

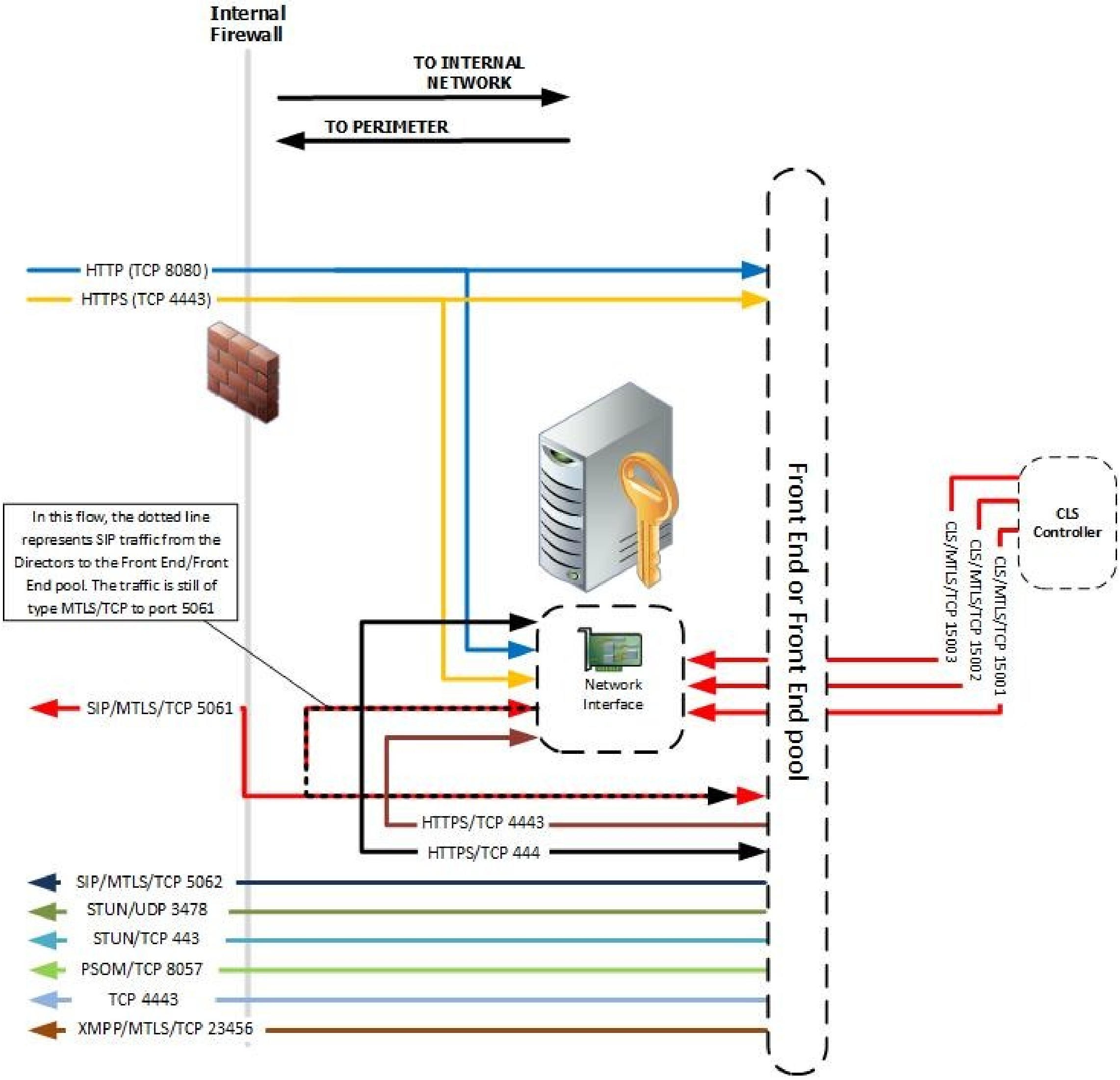
1.3.9.10.10.4 Single Director

Single Director

Planning for External User Access > Scenarios for External User Access > Scenarios for the Director >

Topic Last Modified: *2012-10-22*

The Director can be deployed in either a single Director configuration or as a Director pool. This section defines a topology and configuration for a single Director. If you are planning on deploying a pool of Directors for the purposes of handling higher capacity and for high availability, see the topic Scaled Director Pool for planning considerations for that topology.



In this flow, the dotted line represents SIP traffic from the Directors to the Front End/Front End pool. The traffic is still of type MTLS/TCP to port 5061

- Certificate Summary - Single Director
- Port Summary - Single Director
- DNS Summary - Single Director

Certificate Summary - Single Director

Scenarios for External User Access > Scenarios for the Director > Single Director >

Topic Last Modified: *2012-09-08*

Certificate requirements for a single Director consist of a default certificate that has a subject name and subject alternative names for services that the Director can receive. Additionally, there is an OAuth Token certificate for server to server authentication purposes.

Certificates for Director

Component	Subject name (SN)	Subject alternative names (SAN)	Comments
Default	dir01.contoso.net	dir01.contoso.net dialin.contoso.com meet.contoso.com lyncdiscoverinternal.contoso.com lyncdiscover.contoso.com (Optionally) *.contoso.com	Director certificates can be requested from either an internally managed certification authority (CA) or from a public CA. The Director responds to requests from the reverse proxy in the perimeter or from the Edge Server. Internal clients will not use the Director. Or, a wildcard entry for the simple URLs
OAuthTokenIssuer	dir01.contoso.net	No Entry	**Important:** Note that the minimum key length is 1024, but you may receive a warning that the minimum recommended key length is 2048 bits. The OAuthTokenIssuer certificate is a single-purpose certificate for the purpose of authenticating servers in a large-scale environment, and can be requested from an internal CA or from a public CA. The certificate is required.

Port Summary - Single Director

Scenarios for External User Access > Scenarios for the Director > Single Director >

Topic Last Modified: *2012-10-20*

Firewall port requirements for a single Director consist of the ports that are used to establish communication with the Director from the internal interface or internal-facing network of the reverse proxy. Microsoft Lync Server 2013 by default expects ports HTTP/ TCP 8080 and HTTPS/TCP 4443 to be open from the reverse proxy to the Director, as well as the Front End pool and Front End Server. Additionally, there must be session initiation protocol (SIP) communication from the Edge Server internal interface to the Director and to the Front End pool and Front End Server. The SIP protocol uses SIP/MTLS/TCP 5061 from the Edge Server to the Front End pool and Front End Server. A rule that allows SIP/ MTLS/TCP 5061 communication from the Director, Front End pool and Front End Server to the Edge Server internal interface must be created as well.

Single Director Ports and Protocols for Firewall Definitions

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
HTTP/TCP 8080	Reverse proxy internal interface	Director	Initially received by the external side of the reverse proxy, the communication is sent on to the Director and Front End Server web services
HTTPS/TCP 4443	Reverse proxy internal interface	Director	Initially received by the external side of the reverse proxy, the communication is sent on to the Director and Front End Server web services
HTTPS/TCP 444	Director	Front End server or Front End pool	Inter-server communication between the Director and the Front End Server
HTTP/TCP 80	Internal Clients	Director web services	The Director provides web services to internal and external clients.
HTTPS/TCP 443	Internal Clients	Director web services	The Director provides web services to internal and external clients.
SIP/MTLS/TCP 5061	Edge Server internal interface	Director	SIP communication from the Edge Server to the Director, and the Front End Server.
MTLS/TCP/50001	Any	Edge Server internal interface	Centralized Logging Service controller (ClsController.exe) or agent (ClasAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Edge Server internal interface	Centralized Logging Service controller (ClsController.exe) or agent (ClasAgent.exe) commands and log collection

MTLS/TCP/50003	Any	Edge Server internal interface	Centralized Logging Service controller (ClsController.exe) or agent (ClasAgent.exe) commands and log collection

DNS Summary - Single Director

Scenarios for External User Access > Scenarios for the Director > Single Director >

Topic Last Modified: *2012-10-20*

The following table contains a summary of the DNS records that are required to support the single Director. The role of the Director requires similar DNS records as the Front End Server. The number of records needed is reflected in the subject alternative names required on the Director certificate. Different from the Front End Server, the Director does not host user accounts or host the Mobility Services.

DNS Records Required for the Director

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
Internal DNS/A	dir01.contoso.net	Director	Director host record used for replication and server to server
Internal DNS/A	sip.contoso.com	Director	Inbound session initiation protocol (SIP) from the internal Edge interface of the Edge Server
Internal DNS/A	dialin.contoso.com	Director	Published dialin web services from reverse proxy
Internal DNS/A	meet.contoso.com	Director	Published meet web services from reverse proxy
Internal DNS/A	webdirexternal.contoso.com	Director	Published and defined by the reverse proxy Web Ticket external web services for the Director

1.3.9.10.10.5 Scaled Director Pool

Scaled Director Pool

Planning for External User Access > Scenarios for External User Access > Scenarios for the Director >

Topic Last Modified: *2012-09-08*

The Director can be deployed in either a single Director configuration, or as a Director pool. This section defines a topology and configuration for two pooled Director topologies.

If you are planning on deploying a single Director, see the topic Single Director for planning considerations for that topology.

- Scaled Director Pool - DNS Load Balancing and Hardware Load Balancer
- Scaled Director Pool - Hardware Load Balancer

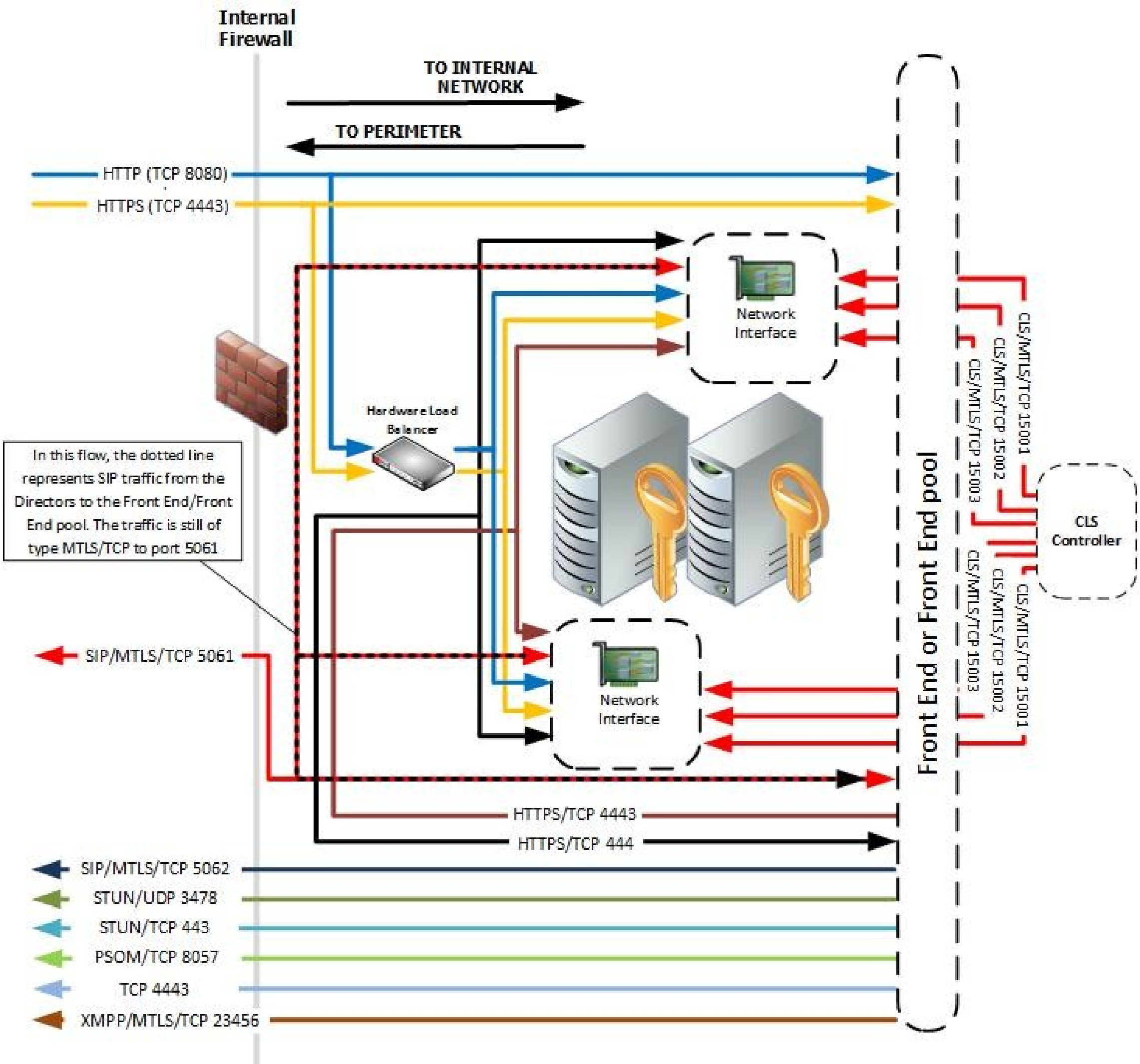
Scaled Director Pool - DNS Load Balancing and Hardware Load Balancer

Scenarios for External User Access > Scenarios for the Director > Scaled Director Pool >

Topic Last Modified: *2012-10-22*

A scaled Director pool, where there are more than one Director deployed to handle additional capacity and to provide high availability, requires load balancing to distribute client and server communication to all members of the pool. A Director hosts web services much like a Front End pool. To provide the load balancing, you can use either hardware load balancing or domain name system (DNS) load balancing and hardware load balancing. Hardware load balancing is required for the web services, and DNS load balancing alone does not provide the capabilities required for the web services.

The following topics describe the planning considerations for deploying a Director pool using DNS load balancing in conjunction with hardware load balancing. If you intend to use hardware load balancing, but not DNS load balancing for the Director pool, see the topic Scaled Director Pool - Hardware Load Balancer that describes the planning requirements for that topology.



In this flow, the dotted line represents SIP traffic from the Directors to the Front End/Front End pool. The traffic is still of type MTLS/TCP to port 5061

- Certificate Summary - DNS and HLB Load Balanced
- Port Summary - DNS and HLB Load Balanced
- DNS Summary - DNS and HLB Load Balanced

Certificate Summary - DNS and HLB Load Balanced

Scenarios for the Director > Scaled Director Pool > Scaled Director Pool - DNS Load Balancing and Hardware Load Balancer >

Topic Last Modified: *2012-10-22*

Certificate requirements for a Director with DNS load balancing and a hardware load balancer will use a default certificate that has a subject name and subject alternative names for services that the Director can receive. A certificate is requested for each Director in the pool. It is important to remember that the hardware load balancer is load balancing only the traffic from the reverse proxy. Additionally, there is an OAuth Token certificate for server to server authentication purposes that is installed on each server.

Certificates for Director

Component	Subject name (SN)	Subject alternative names (SAN)	Comments
Default	dirpool01.contoso.net	dirpool01.contoso.net dir01.contoso.net dialin.contoso.com meet.contoso.com lyncdiscoverinternal.contoso.com lyncdiscover.contoso.com (Optionally) *.contoso.com	Director certificates can be requested from either an internally managed certification authority (CA) or from a public CA. The Director responds to requests from the reverse proxy in the perimeter or from the Edge Server. Internal clients will not use the Director. Or, a wildcard entry for the simple URLs
OAuthTokenIssuer	dir01.contoso.net	No Entry	**Important:** Note that the minimum key length is 1024, but you may receive a warning that the minimum recommended key length is 2048 bits. The OAuthTokenIssuer certificate is a single-purpose certificate for the purpose of authenticating servers in a large-scale environment, and can be requested from an internal CA or from a public CA. The certificate is required.

Port Summary - DNS and HLB Load Balanced

Scenarios for the Director > Scaled Director Pool > Scaled Director Pool - DNS Load Balancing and Hardware Load Balancer >

Topic Last Modified: *2012-10-22*

Firewall port requirements for a single Director consist of the ports that are used to establish communication with the Director from the internal interface or internal-facing network of the reverse proxy. Microsoft Lync Server 2013 by default expects ports HTTP/TCP 8080 and HTTPS/TCP 4443 to be open from the reverse proxy to the Director, as well as the Front End pool and Front End Server. Additionally, there must be session initiation protocol (SIP) communication from the Edge Server internal interface to the Director and to the Front End pool and Front End Server. The SIP protocol uses SIP/MTLS/TCP 5061 from the Edge Server to the Front End pool and Front End Server. A rule that allows SIP/

MTLS/TCP 5061 communication from the Director, Front End pool and Front End Server to the Edge Server internal interface must be created as well.

Single Director Ports and Protocols for Firewall Definitions

Role/Protocol/TCP or UDP/Port	Source IP address	Destination IP address	Notes
HTTP/TCP 8080	Reverse proxy internal interface	Director Hardware Load Balancer VIP	Initially received by the external side of the reverse proxy, the communication is sent on to the Director HLB VIP and Front End Server web services.
HTTPS/TCP 4443	Reverse proxy internal interface	Director Hardware Load Balancer VIP	Initially received by the external side of the reverse proxy, the communication is sent on to the Director HLB VIP and Front End Server web services.
HTTPS/TCP 444	Director	Front End pool or Front End Server	Inter-server communication between the Director HLB VIP and the Front End Server or Front End Servers.
HTTP/TCP 80	Internal Clients	Director Hardware Load Balancer VIP	The Director provides web services to internal as well as external clients.
HTTPS/TCP 443	Internal Clients	Director Hardware Load Balancer VIP	The Director provides web services to internal as well as external clients.
SIP/MTLS/TCP 5061	Edge Server internal interface	Director	SIP communication from the Edge Server to the Director, as well as the Front End Servers.
MTLS/TCP/50001	Any	Director	Centralized Logging Service controller (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Director	Centralized Logging Service controller (ClsController.exe) or agent (ClsAgent.exe) commands and log

			collection
MTLS/TCP/50003	Any	Director	Centralized Logging Service controller (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

DNS Summary - DNS and HLB Load Balanced

Scenarios for the Director > Scaled Director Pool > Scaled Director Pool - DNS Load Balancing and Hardware Load Balancer >

Topic Last Modified: *2012-10-20*

The following table contains a summary of the DNS records that are required to support the DNS load balanced and hardware load balanced Director. The role of the Director requires similar DNS records as the Front End Server. The number of records needed is reflected in the subject alternative names required on the Director certificate. Different from the Front End Server, the Director pool does not host user accounts or host the Mobility Services.

DNS Records Required for the Director Pool using DNS Load Balancing and Hardware Load Balancer

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
Internal DNS/A	dir01.contoso.net	Director	Director host record used for replication and server to server
Internal DNS/A	dirpool01.contoso.net	Director pool	Host record for the DNS load balanced Director pool for server to server
Internal DNS/A	sip.contoso.com	Director pool	Inbound session initiation protocol (SIP) from the internal interface of the Edge Server
Internal DNS/A	dialin.contoso.com	Director pool HLB VIP	Hardware load balanced published dialin web services from reverse proxy
Internal DNS/A	meet.contoso.com	Director pool HLB VIP	Hardware load balanced published meet web services from reverse proxy
Internal DNS/A	webdirexternal.contoso.com	Director pool HLB VIP	Hardware load balanced published and defined by the reverse proxy Web Ticket external web

			services for the Director pool

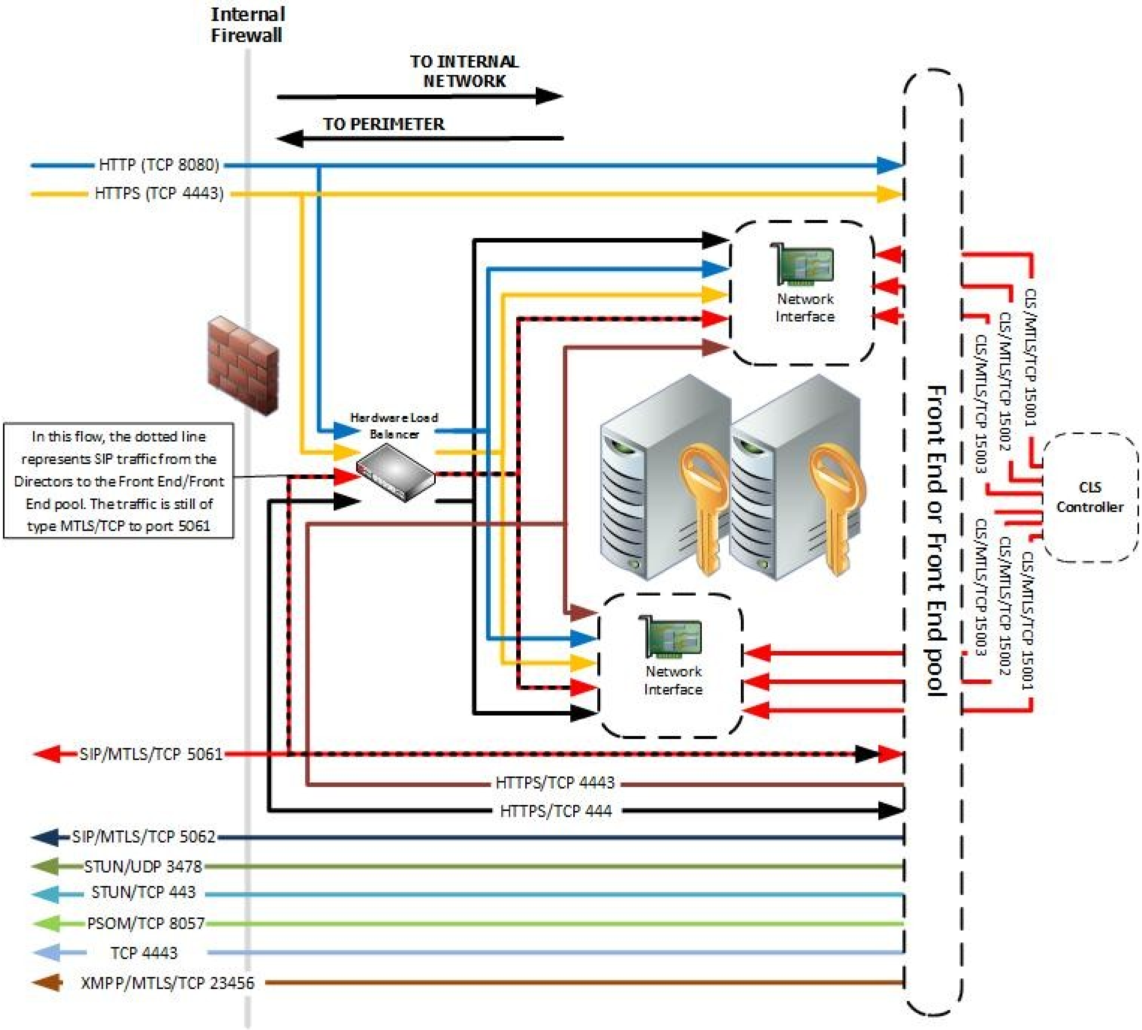
Scaled Director Pool - Hardware Load Balancer

Scenarios for External User Access > Scenarios for the Director > Scaled Director Pool >

Topic Last Modified: *2012-09-08*

A scaled Director pool, where there are more than one Director is deployed to handle additional capacity and to provide high availability, requires load balancing to distribute client and server communication to all members of the pool. A Director hosts web services much like a Front End pool. Hardware load balancing is required for the web services.

The following topics describe the planning considerations for deploying a Director pool using hardware load balancing. If you intend to use hardware load balancing and DNS load balancing for the Director pool, see the topic Scaled Director Pool - DNS Load Balancing and Hardware Load Balancer that describes the planning requirements for that topology.



In this flow, the dotted line represents SIP traffic from the Directors to the Front End/Front End pool. The traffic is still of type MTLS/TCP to port 5061

- Certificate Summary - Scaled Director Pool, Hardware Load Balancer
- Port Summary - Scaled Director Pool, Hardware Load Balancer
- DNS Summary - Scaled Director Pool, Hardware Load Balancer

Certificate Summary - Scaled Director Pool, Hardware Load Balancer

Scenarios for the Director > Scaled Director Pool > Scaled Director Pool - Hardware Load Balancer >

Topic Last Modified: *2012-10-20*

Certificate requirements for a Director with a hardware load balancer will use a default certificate that has a subject name and subject alternative names for services that the Director pool can receive. A certificate is requested for each Director in the pool. Additionally there is an OAuth Token certificate for server to server authentication purposes that is installed on each server.

Certificates for a Scaled Director Using a Hardware Load Balancer

Component	Subject name (SN)	Subject alternative names (SAN)	Comments
Default	dirpool01.contoso.net	dirpool01.contoso.net dir01.contoso.net dialin.contoso.com meet.contoso.com lyncdiscoverinternal.contoso.com lyncdiscover.contoso.com (Optionally) *.contoso.com	Director certificates can be requested from either an internally managed certification authority (CA) or from a public CA. The Director responds to requests from the reverse proxy in the perimeter or from the Edge Server. Or, a wildcard entry for the simple URLs
OAuthTokenIssuer	dir01.contoso.net	No Entry	**◆Important:** Note that the minimum key length is 1024, but you may receive a warning that the minimum recommended key length is 2048 bits. The OAuthTokenIssuer certificate is a single-purpose certificate for the purpose of authenticating servers in a large-scale environment, and can be requested from an internal CA or from a

			public CA. The certificate is required.

Port Summary - Scaled Director Pool, Hardware Load Balancer

Scenarios for the Director > Scaled Director Pool > Scaled Director Pool - Hardware Load Balancer >

Topic Last Modified: *2012-10-21*

Firewall port requirements for a Director pool consist of the ports that are used to establish communication with the Director from the internal interface of the Edge Server or internal-facing interface of the reverse proxy. Microsoft Lync Server 2013 by default expects ports HTTP/TCP 8080 and HTTPS/TCP 4443 to be open from the reverse proxy to the Director, as well as the Front End pool and Front End Server. Additionally, there must be session initiation protocol (SIP) communication from the Edge Server internal interface to the Director and to the Front End pool and Front End Server. The SIP protocol uses SIP/MTLS/TCP 5061 from the Edge Server to the Front End pool and Front End Server. A rule that allows SIP/MTLS/TCP 5061 communication from the Director, Front End pool and Front End Server to the Edge Server internal interface must be created as well.

Director Ports and Protocols for Firewall Definitions

Role/Protocol/TCP or UDP/Port	**Source IP address**	**Destination IP address**	**Notes**
HTTP/TCP 8080	Reverse proxy internal interface	Director Hardware Load Balancer VIP	Initially received by the external side of the reverse proxy, the communication is sent on to the Director HLB VIP and Front End Servers web services
HTTPS/TCP 4443	Reverse proxy internal interface	Director Hardware Load Balancer VIP	Initially received by the external side of the reverse proxy, the communication is sent on to the Director HLB VIP and Front End Servers web services
HTTPS/TCP 444	Director	Front End Server or Front End pool	Inter-server communication between the Director HLB VIP and the Front End Servers
HTTP/TCP 80	Internal Clients	Director Hardware Load Balancer VIP	The Director provides web services to internal as well as external clients.
HTTPS/TCP 443	Internal Clients	Director Hardware Load Balancer VIP	The Director provides web services to

			internal as well as external clients.
SIP/MTLS/TCP 5061	Edge Server internal interface	Director Hardware Load Balancer VIP	SIP communication from the Edge Server to the Director, and Front End Servers.
MTLS/TCP/50001	Any	Director	Centralized Logging Service controller (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002	Any	Director	Centralized Logging Service controller (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003	Any	Director	Centralized Logging Service controller (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

DNS Summary - Scaled Director Pool, Hardware Load Balancer

Scenarios for the Director > Scaled Director Pool > Scaled Director Pool - Hardware Load Balancer >

Topic Last Modified: *2012-10-20*

The following table contains a summary of the DNS records that are required to support the hardware load balanced Director. The role of the Director requires similar DNS records as the Front End Server. The number of records needed is reflected in the subject alternative names required on the Director certificate. Different from the Front End Server, the Director pool does not host user accounts or host the Mobility Services.

DNS Records Required for the Director pool using a Hardware Load Balancer and DNS Load Balancing

Location/TYPE/Port	FQDN/DNS Record	IP Address/FQDN	Maps to/Comments
Internal DNS/A	dir01.contoso.net	Director	Director host record used for replication and server to server communication
Internal DNS/A	dirpool01.contoso.net	Director pool pool HLB VIP	Host record for the DNS load balanced Director pool
Internal DNS/A	sip.contoso.com	Director pool HLB VIP	Inbound session initiation protocol

			(SIP) from the internal interface of the Edge Server
Internal DNS/A	dialin.contoso.com	Director pool HLB VIP	Hardware load balanced published dialin web services from reverse proxy
Internal DNS/A	meet.contoso.com	Director pool HLB VIP	Hardware load balanced published meet web services from reverse proxy
Internal DNS/A	webdirexternal.contoso.com	Director pool HLB VIP	Hardware load balanced published and defined by the reverse proxy Web Ticket external web services for the Director pool

1.3.10 Planning for Enterprise Voice

Planning for Enterprise Voice

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-21*

The deployment process for Enterprise Voice depends on your existing topology, infrastructure, and the Enterprise Voice functionality that you want to support. The required procedures will depend on what features you choose, but there are other planning considerations that you must make at a high level.

In general, consider the type and number of sites that you want to deploy and their geographical locations, the call volume at each site, the types of network links that connect sites, whether you want to provide redundancy and failover for voice functionality for each site, and whether you want to use existing PBX equipment. There are certain considerations, such as high availability, that you should consider when you plan for Lync Server communications software as a whole. These considerations are discussed in topics throughout this section, as needed.

Planning Considerations

For planning decisions that pertain to the deployment of a particular Enterprise Voice capability or deployment scenario or component, consult the topics in this section.

- Defining Your Organization's Requirements for Enterprise Voice
- Estimating Voice Usage and Traffic
- Network Settings for the Advanced Enterprise Voice Features
- Planning for Enterprise Voice Resiliency
- Components Required for Enterprise Voice
- Deployment Guidelines for Enterprise Voice
- Deployment Process Overview for Enterprise Voice
- Moving Users to Enterprise Voice

1.3.10.1 Defining Your Organization's Requirements for Enterprise Voice

Defining Your Organization's Requirements for Enterprise Voice

See Also

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-08-07*

This topic provides an overview of the considerations you need to make about the regions, sites, and the links between sites in your topology and how those are important when you deploy Enterprise Voice. For details to help you make these decisions, see Network Settings for the Advanced Enterprise Voice Features in the Planning documentation.

Sites and Regions

First, identify the sites in your topology where you will deploy Enterprise Voice and the network regions to which those sites belong. In particular, consider how you will provide public switched telephone network (PSTN) connectivity to each site. For manageability and logistical reasons, the regions to which these sites belong can be a deciding factor. Decide where gateways will be deployed locally, where Survivable Branch Appliances (SBAs) will be deployed, and where you can configure SIP trunks (either locally or at the central site) to an Internet telephony service provider (ITSP).

Network Links Between Sites

You also need to consider the bandwidth usage that you expect on the network links between your central site and its branch sites. If you have, or plan to deploy, resilient WAN links between sites, we recommend that you deploy a gateway at each branch site to provide local direct inward dial (DID) termination for users at those sites. If you have resilient WAN links, but the bandwidth on a WAN link is likely to be constrained, configure call admission control for that link. If you do not have resilient WAN links, host fewer than 1000 users at your branch site, and do not have local trained Lync Server administrators available, we recommend that you deploy a Survivable Branch Appliance at the branch site. If you host between 1000 and 5000 users at your branch site, lack a resilient WAN connection, and have trained Lync Server administrators available, we recommend that you deploy a Survivable Branch Server with a small gateway at the branch site. Consider also enabling media bypass on constrained links if you have a gateway peer that supports media bypass.

⊟See Also

Concepts

Network Settings for the Advanced Enterprise Voice Features

1.3.10.2 Estimating Voice Usage and Traffic

Estimating Voice Usage and Traffic

Planning > Capacity Planning > Capacity Planning Using the User Models >

Topic Last Modified: *2012-08-07*

The Microsoft Lync Server 2013, Planning Tool uses the following metric to estimate user traffic at each site and the number of ports that are required to support that traffic.

- For **Light traffic** (one PSTN call per user per hour), figure 15 users per port.
- For **Medium traffic** (2 PSTN calls per user per hour), figure 10 users per port.
- For **Heavy traffic** (3 or more PSTN per user calls per hour), figure 5 users per port.

The number of ports in turn determines the number of Mediation Servers and gateways that will be required. The public switched telephone network (PSTN) gateways that most organizations consider deploying range in size from 2 ports to as many as 960 ports. (There are even larger gateways, but these are used mainly by telephony service providers.)

For example, an organization with 10,000 users and medium traffic would require 1000 ports. The number of gateways required would equal the total number of ports required as determined by the total capacity of the gateways.

1.3.10.3 Network Settings for the Advanced Enterprise Voice Features

Network Settings for the Advanced Enterprise Voice Features

See Also

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-10-10*

Lync Server has three advanced Enterprise Voice features: call admission control (CAC), emergency services (E9-1-1), and media bypass. These features share certain configuration requirements for network regions, network sites, and association of each subnet in the Lync Server topology with a network site. For details about planning for deployment of these features, see:

- Planning for Call Admission Control
- Planning for Emergency Services (E9-1-1)
- Planning for Media Bypass

For details about deploying each of these features, see Deploying Advanced Enterprise Voice Features in the Deployment documentation.

This topic provides an overview of the configuration requirements that are common to all three advanced Enterprise Voice features.

Network Regions

A network region is a network hub or network backbone used only in the configuration of call admission control (CAC), E9-1-1, and media bypass.

> **Note:**
> Network regions are not the same as Lync Server dial-in conferencing regions, which are required to associate dial-in conferencing access numbers with one or more Lync Server dial plans. For details about dial-in conferencing regions, see Dial-In Conferencing Requirements in the Planning documentation.

CAC requires that every network region have an associated Lync Server central site, which manages media traffic within the region (that is, it makes decisions based on policies that you have configured, regarding whether or not a real-time audio or video session can be established). Lync Server central sites do not represent geographical locations, but rather logical groups of servers that are configured as a pool or a set of pools. For details about central sites, see Reference Topologies in the Planning documentation. Also see Supported Lync Server 2013 Topologies in the Supportability documentation.

To configure a network region, you can either use the **Regions** tab on the **Network Configuration** section of Lync Server Control Panel, or run the **New-CsNetworkRegion** or **Set-CsNetworkRegion** Lync Server Management Shell cmdlets. For instructions, see Create or Modify a Network Region in the Deployment documentation, or refer to the Lync Server Management Shell documentation.

The same network region definitions are shared by all three advanced Enterprise Voice features. If you have already created network regions for one feature, you do not need to create new network regions for the other features. You may, however, need to modify an existing network region definition to apply feature-specific settings. For example, if you have created network regions for E9-1-1 (which do not require an associated central site) and, later, you deploy call admission control, you must modify each of the network region definitions to specify a central site.

To associate a Lync Server central site with a network region, you specify the central site name, either by using the **Network Configuration** section of Lync Server Control Panel, or by running the **New-CsNetworkRegion** or **Set-CsNetworkRegion** Lync Server Management Shell cmdlets. For instructions, see Create or Modify a Network Region in the Deployment documentation, or refer to the Lync Server Management Shell documentation.

Network Sites

A network site represents a geographical location, such as a branch office, a regional office, or a main office. Each network site must be associated with a specific network region.

Note:

Network sites are used only by the advanced Enterprise Voice features. They are not the same as the branch sites that you configure in your Lync Server topology. For details about branch sites, see Reference Topologies in the Planning documentation. Also see Supported Lync Server 2013 Topologies in the Supportability documentation.

To configure a network site and associate it with a network region, you can either use the **Network Configuration** section of Lync Server Control Panel, or run the Lync Server Management Shell **New-CsNetworkSite** or **Set-CsNetworkSite** cmdlets. For details, see Create or Modify a Network Site in the Deployment documentation, or refer to the Lync Server Management Shell documentation.

Identify IP Subnets

For each network site, you will need to work with your network administrator to determine which IP subnets are assigned to each network site. If your network administrator has already organized the IP subnets into network regions and network sites, then your work is significantly simplified.

For example, the New York site in the North America region can be assigned the following IP subnets: 172.29.80.0/23, 157.57.216.0/25, 172.29.91.0/23, 172.29.81.0/24. If Bob, who usually works in Detroit, travels to the New York office for training, turns on his computer and connects to the network, his computer will get an IP address in one of the four ranges that are allocated for New York—for example, 172.29.80.103.

Warning:

The IP subnets specified during network configuration on the server must match the format that is provided by client computers in order to be properly used for media bypass. A Lync client takes its local IP address and masks the IP address with the associated subnet mask. When determining the bypass ID associated with each client, the Registrar will compare the list of IP subnets associated with each network site against the subnet that is provided by the client for an exact match. For this reason, it is important that subnets entered during network configuration on the server are actual subnets instead of virtual subnets. (If you deploy call admission control, but not media bypass, call admission control will function properly even if you configure virtual subnets.)
For example, if a Lync client signs in on a computer with an IP address of 172.29.81.57 with an IP subnet mask of 255.255.255.0, it will request the bypass ID that is associated with subnet 172.29.81.0. If the subnet is defined as 172.29.0.0/16, although the client belongs to the virtual subnet, the Registrar will not consider this a match because the Registrar is specifically looking for subnet 172.29.81.0. Therefore, it is important that the administrator enters subnets exactly as provided by Lync clients (which are provisioned with subnets during network configuration, either statically or by Dynamic Host Configuration Protocol (DHCP).)

Associating Subnets with Network Sites

Every subnet in the enterprise network must be associated with a network site (that is, every subnet needs to be associated with a geographic location). This association of subnets enables the advanced Enterprise Voice features to locate the endpoints geographically. For example, locating the endpoints enables CAC to regulate the flow of real-time audio and video data going to and from the network site.

To associate subnets with network sites, you can either use the **Network Configuration** section of Lync Server Control Panel, or you can use the Lync Server Management Shell. For instructions, see Associate a Subnet with a Network Site in the Deployment documentation, or refer to the Lync Server Management Shell documentation.

⊟See Also

Other Resources

Planning for Call Admission Control
Planning for Emergency Services (E9-1-1)
Planning for Media Bypass

1.3.10.4 Components Required for Enterprise Voice

Components Required for Enterprise Voice

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-10-20*

This section describes all components that are used by one or more Enterprise Voice features. They include the following:

- Front End Server VoIP Components
- Mediation Server Component
- PSTN Connectivity Components
- Perimeter Network VoIP Components

Front End Server VoIP Components

Planning > Planning for Enterprise Voice > Components Required for Enterprise Voice >

Topic Last Modified: *2012-10-01*

The VoIP components located on Front End Servers are as follows:

- Translation Service
- Inbound Routing component
- Outbound Routing component
- Exchange UM Routing component
- Intercluster Routing component
- Mediation Server Component

Translation Service

The Translation Service is the server component that is responsible for translating a dialed number into the E.164 format or another format, according to the normalization rules that are defined by the administrator. The Translation Service can translate to formats other than E.164 if your organization uses a private numbering system or uses a gateway or PBX that does not support E.164.

Inbound Routing Component

The Inbound Routing component handles incoming calls largely according to preferences that are specified by users on their Enterprise Voice clients. It also facilitates delegate ringing and simultaneous ringing, if configured by the user. For example, users specify whether unanswered calls are forwarded or simply logged for notification. If call forwarding is enabled, users can specify whether unanswered calls should be forwarded to another number or to a Exchange UM server that has been configured to provide call answering. The Inbound Routing component is installed by default on all Standard Edition server and Front End Servers.

Outbound Routing Component

The Outbound Routing component routes calls to PBX or PSTN destinations. It applies call authorization rules, as defined by the user’s voice policy, to callers and determines the optimal PSTN gateway for routing each call. The Outbound Routing component is installed by default on all Standard Edition server and Front End Servers.

The routing logic that is used by the Outbound Routing component is in large measure configured by network or telephony administrators according to the requirements of their organizations.

Exchange UM Routing Component

The Exchange UM routing component handles routing between Lync Server and servers running Exchange Unified Messaging (UM), to integrate Lync Server with Unified Messaging features.

The Exchange UM routing component also handles rerouting of voice mail over the PSTN if Exchange UM servers are unavailable. If you have Enterprise Voice users at branch sites that do not have a resilient WAN link to a central site, the Survivable Branch Appliance that you deploy at the branch site provides voice mail survivability for branch users during a WAN outage. When the WAN link is unavailable, the Survivable Branch Appliance does the following:

- reroutes unanswered calls over the PSTN to the Exchange Unified Messaging server in the central site
- provides the ability for a user to retrieve voice mail messages over the PSTN
- queues missed call notifications, and then uploads them to the Exchange UM server when the WAN link is restored.

To enable voice mail rerouting, we recommend that your Exchange administrator configure Exchange UM Auto Attendant (AA) to accept messages only.

For details about these features, see Planning for Exchange Unified Messaging Integration and Planning for Enterprise Voice Resiliency, respectively.

Intercluster Routing Component

The Intercluster routing component is responsible for routing calls to the callee's primary Registrar pool. If that is unavailable, the component routes the call to the callee's backup Registrar pool. If the callee's primary and backup Registrar pools are unreachable over the IP network, the Intercluster routing component reroutes the call over the PSTN to the user's telephone number.

Other Front End Server Components Required for VoIP

Other components residing on the Front End Server or Director that provide essential support for VoIP, but are not themselves VoIP components, include the following:

- **User Services.** Perform reverse number lookup on the destination phone number of each incoming call and match that number to the SIP URI of the destination user. Using this information, the Inbound Routing component distributes the call to that user's registered SIP endpoints. User Services is a core component on all Front End Servers and Directors.
- **User Replicator.** Extracts user phone numbers from Active Directory Domain Services (AD DS) and writes them to tables in the RTC database, where they are available to User Services and Address Book Server. User Replicator is a core component on all Front End Servers.
- **Address Book Server.** Provides global address list information from Active Directory Domain Services (AD DS) to Lync Server clients. It also retrieves user and contact information from the RTC database, writes the information to the Address Book files, and then stores the files on a shared folder where they are downloaded by Lync clients. The Address Book Server writes the information to the RTCAb database, which is used by the Address Book Web Query service to respond to user search queries from Microsoft Lync 2010 Mobile. It optionally normalizes enterprise user phone numbers that are written to the RTC database for the purpose of provisioning user contacts in Lync. The Address Book service is installed by default on all Front End Servers. The Address Book Web Query service is installed by default with the Web services on each Front End Servers.

1.3.10.4.2 Mediation Server Component

Mediation Server Component

Planning > Planning for Enterprise Voice > Components Required for Enterprise Voice >

Topic Last Modified: *2012-09-21*

You must deploy Lync Server 2013, Mediation Server if you deploy the Enterprise Voice workload. This section describes basic functionality, dependencies, basic topologies, and planning guidelines.

The Mediation Server translates signaling and, in some configurations, media between your internal Lync Server 2013, Enterprise Voice infrastructure and a public switched telephone network (PSTN) gateway or a Session Initiation Protocol (SIP) trunk. On the Lync Server 2013 side, Mediation Server listens on a single mutual TLS (MTLS) transport address. On the gateway side, Mediation Server listens on all associated listening ports associated with trunks defined in the Topology document. All qualified gateways must support TLS, but can enable TCP as well. TCP is supported for gateways that do not support TLS.

If you also have an existing Public Branch Exchange (PBX) in your environment, Mediation Server handles calls between Enterprise Voice users and the PBX. If your PBX is an IP-PBX, you can create a direct SIP connection between the PBX and Mediation Server. If your PBX is a Time Division Multiplex (TDM) PBX, you must also deploy a PSTN gateway between Mediation Server and the PBX.

The Mediation Server is collocated with the Front End Server by default. The Mediation Server can also be deployed in a stand-alone pool for performance reasons, or if you deploy SIP trunking, in which case the stand-alone pool is strongly recommended.

If you deploy Direct SIP connections to a qualified PSTN gateway that supports media bypass and DNS load balancing, a stand-alone Mediation Server pool is not necessary. A stand-alone Mediation Server pool is not necessary because qualified gateways are capable of DNS load balancing to a pool of Mediation Servers and they can receive traffic from any Mediation Server in a pool.

We also recommend that you collocate the Mediation Server on a Front End pool when you have deployed IP-PBXs or connect to an Internet Telephony Server Provider’s Session Border Controller (SBC), as long as any of the following conditions are met:

- The IP-PBX or SBC is configured to receive traffic from any Mediation Server in the pool and can route traffic uniformly to all Mediation Servers in the pool.
- The IP-PBX does not support media bypass, but the Front End pool that is hosting the Mediation Server can handle voice transcoding for calls to which media bypass does not apply.

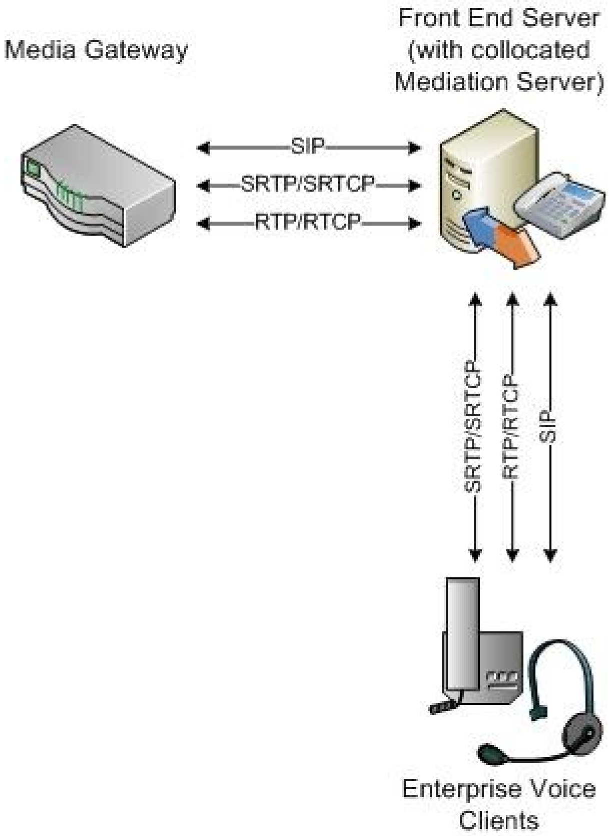
You can use the Microsoft Lync Server 2013, Planning Tool to evaluate whether the Front End pool where you want to collocate the Mediation Server can handle the load. If your environment cannot meet these requirements, then you must deploy a stand-alone Mediation Server pool.

The main functions of the Mediation Server are as follows:

- Encrypting and decrypting SRTP on the Lync Server side
- Translating SIP over TCP (for gateways that do not support TLS) to SIP over mutual TLS
- Translating media streams between Lync Server and the gateway peer of the Mediation Server
- Connecting clients that are outside the network to internal ICE components, which enable media traversal of NAT and firewalls
- Acting as an intermediary for call flows that a gateway does not support, such

as calls from remote workers on an Enterprise Voice client
- In deployments that include SIP trunking, working with the SIP trunking service provider to provide PSTN support, which eliminates the need for a PSTN gateway

The following figure shows the signaling and media protocols that are used by the Mediation Server when communicating with a basic PSTN gateway and the Enterprise Voice infrastructure.



Note:
If you are using TCP or RTP/RTCP (instead of SRTP or SRTCP) on the network between the PSTN gateway and the Mediation Server, we recommend that you take measures to help ensure the security and privacy of the network.

In This Section

- M:N Trunk
- Call Admission Control and Mediation Server
- Enhanced 9-1-1 (E9-1-1) and Mediation Server
- Media Bypass and Mediation Server
- Components and Topologies for Mediation Server
- Deployment Guidelines for Mediation Server

1.3.10.4.2.1 M:N Trunk

M:N Trunk

Planning for Enterprise Voice > Components Required for Enterprise Voice > Mediation Server Component >

Topic Last Modified: *2012-10-01*

Lync Server 2013 supports greater flexibility in the definition of a trunk for call routing purposes from previous releases. A trunk is a logical association between a Mediation Server and listening port number with a gateway and a listening port number. This implies several things: A Mediation Server can have multiple trunks to the same gateway; a Mediation Server can have multiple trunks to different gateways; conversely a gateway can have multiple trunks to different Mediation Servers.

A root trunk is still required to be created when a gateway is added to the Lync topology using Topology Builder. The number of gateways that a given Mediation Server can handle depends on the processing capacity of the server during peak busy hours. If you deploy a Mediation Server on hardware that exceeds the minimum hardware requirements for Lync Server 2013, as described in Supported Hardware in the Supportability documentation, then the estimate of how many active non-bypass calls a stand-alone Mediation Server can handle is approximately 1000 calls. When deployed on hardware meeting these specifications, the Mediation Server is expected to perform transcoding, but still route calls for multiple gateways even if the gateways do not support media bypass.

When defining a call route, you specify the trunks associated with that route, but you do not specify which Mediation Servers are associated with that route. Instead, you use Topology Builder to associate trunks with Mediation Servers. In other words, routing determines which trunk to use for a call, and, subsequently, the Mediation Server associated with that trunk is sent the signaling for that call.

The Mediation Server can be deployed as a pool; this pool can be collocated with a Front End pool, or it can be deployed as a stand-alone pool. When a Mediation Server is collocated with a Front End pool, the pool size can be at most 12 (the limit of the Registrar pool size). Taken together, these new capabilities increase the reliability and deployment flexibility for Mediation Servers, but they require associated capabilities in the following peer entities:

- **PSTN gateway.** A Lync Server 2013 qualified gateway must implement DNS load balancing, which enables a qualified public switched telephone network (PSTN) gateway to act as a load balancer for one pool of Mediation Servers, and thereby to load-balance calls across the pool.
- **Session Border Controller.** For a SIP trunk, the peer entity is a Session Border Controller (SBC) at an Internet telephony service provider. In the direction from the Mediation Server pool to the SBC, the SBC can receive connections from any Mediation Server in the pool. In the direction from the SBC to the pool, traffic can be sent to any Mediation Server in the pool. One method of achieving this is through DNS load balancing, if supported by the service provider and SBC. An alternative is to give the service provider the IP addresses of all Mediation Servers in the pool, and the service provider will provision these in their SBC as a separate SIP trunk for each Mediation Server. The service provider will then handle the load balancing for its own servers. Not all service providers or SBCs may support these capabilities. Furthermore, the service provider may charge extra for this capability. Typically, each SIP trunk to the SBC incurs a monthly fee.
- **IP-PBX.** In the direction from the Mediation Server pool to the IP-PBX SIP termination, the IP-PBX can receive connections from any Mediation Server in the pool. In the direction from the IP-PBX to the pool, traffic can be sent to any Mediation Server in the pool. Because most IP-PBXs do not support DNS load balancing, we recommend that individual direct SIP connections be defined from the IP-PBX to each Mediation Server in the pool. The IP-PBX will then handle its own load balancing by distributing traffic over the trunk group. The assumption is that the trunk group has a consistent set of routing rules at the IP-PBX. Whether a particular IP-PBX supports this trunk group concept and how it intersects with the IP-PBX's own redundancy and clustering architecture needs to be determined before you can decide whether a Mediation Server

cluster can interact correctly with an IP-PBX.

A Mediation Server pool must have a uniform view of the peer gateway with which it interacts. This means that all members of the pool access the same definition of the peer gateway from the configuration store and are equally likely to interact with it for outgoing calls. Therefore, there is no way to segment the pool so that some Mediation Servers communicate with only certain gateway peers for outgoing calls. If such segmentation is necessary, a separate pool of Mediation Servers must be used. This would be the case, for example, if the associated capabilities in PSTN gateways, SIP trunks, or IP-PBXs to interact with a pool as detailed earlier in this topic are not present.

A particular PSTN gateway, IP-PBX, or SIP trunk peer can route to multiple Mediation Servers or trunks. The number of gateways that a particular pool of Mediation Servers can control depends on the number of calls that use media bypass. If a large number of calls use media bypass, a Mediation Server in the pool can handle many more calls, because only signaling layer processing is necessary.

1.3.10.4.2.2 Call Admission Control and Mediation Server

Call Admission Control and Mediation Server

Planning for Enterprise Voice > Components Required for Enterprise Voice > Mediation Server Component >

Topic Last Modified: *2012-09-21*

Call admission control (CAC), first introduced in Lync Server 2010, manages real-time session establishment, based on available bandwidth, to help prevent poor Quality of Experience (QoE) for users on congested networks. To support this capability, the Mediation Server, which provides signaling and media translation between the Enterprise Voice infrastructure and a gateway or SIP trunking provider, is responsible for bandwidth management for its two interactions on the Lync Server side and on the gateway side. In call admission control, the terminating entity for a call handles the bandwidth reservation. The gateway peers (PSTN gateway, IP-PBX, SBC) that the Mediation Server interacts with on the gateway side do not support Lync Server 2013 call admission control. Thus, the Mediation Server has to handle bandwidth interactions on behalf of its gateway peer. Whenever possible, the Mediation Server will reserve bandwidth in advance. If that is not possible (for example, if the locality of the ultimate media endpoint on the gateway side is unknown for an outgoing call to the gateway peer), bandwidth is reserved when the call is placed. This behavior can result in oversubscription of bandwidth, but it is the only way to prevent false rings.

Media bypass and bandwidth reservation are mutually exclusive. If a media bypass is employed for a call, call admission control is not performed for that call. The assumption here is that there are no links with constrained bandwidth involved in the call. If call admission control is used for a particular call that involves the Mediation Server, that call cannot employ media bypass.

For details about media bypass or call admission control, see Planning for Media Bypass or Planning for Call Admission Control in the Planning documentation.

1.3.10.4.2.3 Enhanced 9-1-1 (E9-1-1) and Mediation Server

Enhanced 9-1-1 (E9-1-1) and Mediation Server

Planning for Enterprise Voice > Components Required for Enterprise Voice > Mediation Server

Component >

Topic Last Modified: *2012-09-29*

The Mediation Server has extended capabilities so that it can correctly interact with Enhanced 9-1-1 (E9-1-1) service providers. No special configuration is needed on the Mediation Server; the SIP extensions required for E9-1-1 interaction are, by default, included in the Mediation Server's SIP protocol for its interactions with a gateway peer (PSTN gateway, IP-PBX, or the SBC of an Internet Telephony Service Provider, including E9-1-1 Service Providers)

Whether the SIP trunk to an E9-1-1 Service Provider can be terminated on an existing Mediation Server pool or will require stand-alone Mediation Servers will depend on whether the E9-1-1 SBC can interact with a pool of Mediation Servers. For details, see M:N Trunk.

1.3.10.4.2.4 Media Bypass and Mediation Server

Media Bypass and Mediation Server

See Also

Planning for Enterprise Voice > Components Required for Enterprise Voice > Mediation Server Component >

Topic Last Modified: *2012-09-21*

Media bypass is a Lync Server capability that enables an administrator to configure call routing to flow directly between the user endpoint and the public switched telephone network (PSTN) gateway without traversing the Mediation Server. Media bypass improves call quality by reducing latency, unnecessary translation, possibility of packet loss, and the number of potential points of failure. Where a remote site without a Mediation Server is connected to a central site by one or more WAN links with constrained bandwidth, media bypass lowers the bandwidth requirement by enabling media from a client at a remote site to flow directly to its local gateway without first having to flow across the WAN link to a Mediation Server at the central site and back.This reduction in media processing also complements the Mediation Server's ability to control multiple gateways.

Media bypass and call admission control (CAC) are mutually exclusive. If media bypass is employed for a call, CAC is not performed for that call. The assumption is that there are no links with constrained bandwidth involved in the call.

Concepts

Call Admission Control and Mediation Server

Other Resources

Planning for Media Bypass

1.3.10.4.2.5 Components and Topologies for Mediation Server

Components and Topologies for Mediation Server

Planning for Enterprise Voice > Components Required for Enterprise Voice > Mediation Server Component >

Topic Last Modified: *2012-09-21*

This topic describes the components on which the Mediation Server is dependent and the topologies in which the Mediation Server can be deployed

Dependencies

The Mediation Server has the following dependencies:

- **Registrar.** Required. The Registrar is the next hop for signaling in the Mediation Server interactions with the Lync Server 2013 network. Note that Mediation Server can be collocated on a Front End Server along with the Registrar, in addition to being installed in a stand-alone pool consisting only of Mediation Servers. The Registrar is collocated with a Mediation Server and PSTN gateway on a Survivable Branch Appliance.
- **Monitoring Server.** Optional but highly recommended. The Monitoring Server allows the Mediation Server to record quality metrics associated with its media sessions.
- **Edge Server.** Required for external user support. The Edge Server allows the Mediation Server to interact with users who are located behind a NAT or firewall.

Topologies

The Lync Server 2013, Mediation Server is by default collocated with an instance of the Registrar on a Standard Edition server, a Front End pool, or Survivable Branch Appliance. All Mediation Servers in a Front End pool must be configured identically.

Where performance is an issue, it may be preferable to deploy one or more Mediation Servers in a dedicated stand-alone pool. Or, if you are deploying SIP trunking, we recommend that you deploy a stand-alone Mediation Server pool.

If you deploy Direct SIP connections to a qualified PSTN gateway that supports media bypass and DNS load balancing, a stand-alone Mediation Server pool is not necessary. A stand-alone Mediation Server pool is not necessary because qualified gateways are capable of DNS load balancing to a pool of Mediation Servers and they can receive traffic from any Mediation Server in a pool.

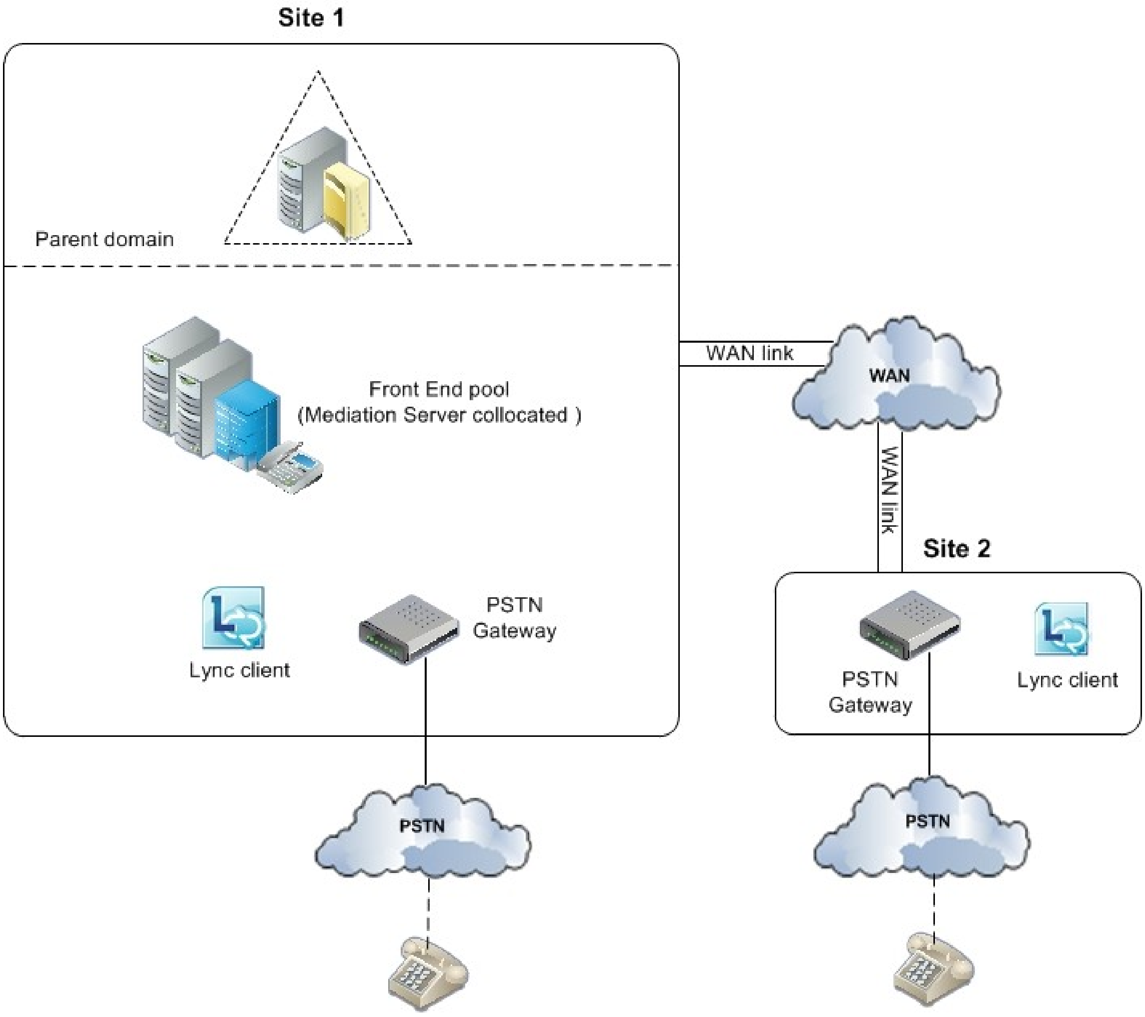
We also recommend that you collocate the Mediation Server on a Front End pool when you have deployed IP-PBXs or connect to an Internet Telephony Server Provider’s Session Border Controller (SBC), as long as any of the following conditions are met:

- The IP-PBX or SBC is configured to receive traffic from any Mediation Server in the pool and can route traffic uniformly to all Mediation Servers in the pool.
- The IP-PBX does not support media bypass, but the Front End pool that is hosting the Mediation Server can handle voice transcoding for calls to which media bypass does not apply.

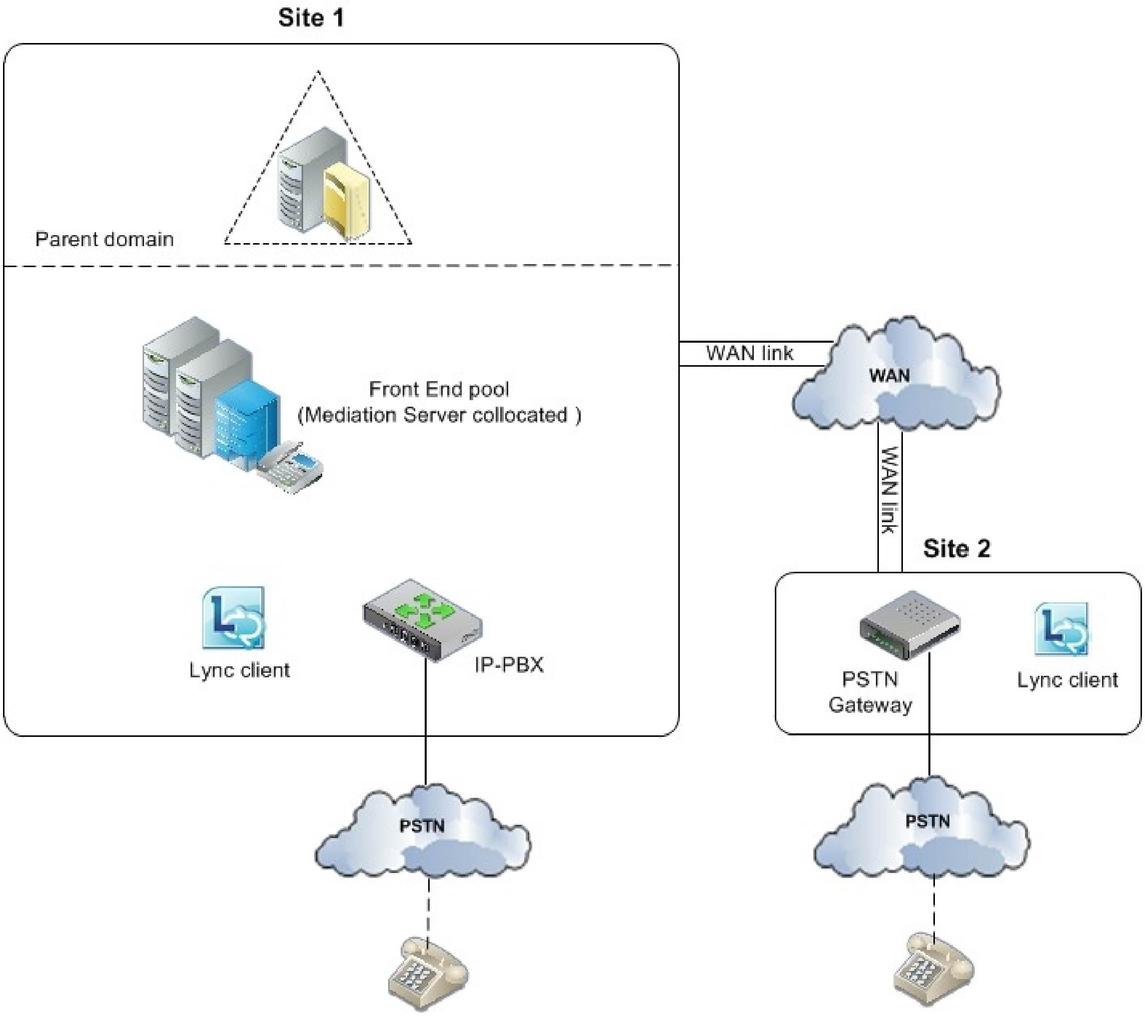
You can use the Microsoft Lync Server 2013, Planning Tool to evaluate whether the Front End pool where you want to collocate the Mediation Server can handle the load. If your environment cannot meet these requirements, then you must deploy a stand-alone Mediation Server pool.

For details about which topology to deploy, see Deployment Guidelines for Mediation Server.

The following figure shows a simple topology consisting of two sites connected by a WAN link. Mediation Server is collocated with the Registrar on a Front End pool at Site 1. The Mediation Servers at Site 1 controls both the PSTN gateway at Site 1 and the gateway at Site 2. In this topology, media bypass is enabled globally to use site and region information, and the trunks to each PSTN gateway (GW1 and GW2) have bypass enabled.



The next figure shows a simple topology where the Mediation Server is collocated with the Registrar on Front End pool at Site 1 and has a Direct SIP connection to the IP-PBX at Site 1. In this figure, the Mediation Server also controls a PSTN gateway at Site 2. Assume that Lync users exist at both Sites 1 and 2. Also assume that the IP-PBX has an associated media processor that must be traversed by all media originating from Lync endpoints before being sent to media endpoints controlled by the IP-PBX. In this topology, media bypass is enabled globally to use site and region information, and the trunks to the PBX and PSTN gateway have media bypass enabled.



For details about planning for PBX topologies, see Deployment Guidelines for Mediation Server and Direct SIP Deployment Options.

The last figure in this topic shows a topology where the Mediation Server is connected to the SBC of an Internet Telephony Service Provider. For details about SIP trunk topologies, see SIP Trunking.

1.3.10.4.2.6 Deployment Guidelines for Mediation Server

Deployment Guidelines for Mediation Server

Planning > Capacity Planning > Capacity Planning Using the User Models >

Topic Last Modified: *2012-10-12*

This topic describes planning guidelines for Mediation Server deployment. After reviewing these guidelines, we recommend that you use the Planning Tool to create and view possible alternative topologies, which can serve as models for what the final tailored topology that you decide to deploy would look like.

Collocated or Stand-alone Mediation Server?

Mediation Server is by default collocated on the Standard Edition server or Front End Server in a Front End pool at central sites. The number of public switched telephone network (PSTN) calls that can be handled and the number of machines required in the pool will depend on the following:

- The number of gateway peers that the Mediation Server pool controls
- The high-volume traffic periods through those gateways
- The percentage of calls that are calls whose media bypass the Mediation Server

When planning, be sure to take into account the media processing requirements for PSTN calls and A/V conferences that are not configured for media bypass, as well as the processing needed to handle signaling interactions for the number of busy-hour calls that need to be supported. If there is not enough CPU, then you must deploy a stand-alone pool of Mediation Servers; and PSTN gateways, IP-PBXs, and SBCs will need to be split into subsets that are controlled by the collocated Mediation Servers in one pool and the stand-alone Mediation Servers in one or more stand-alone pools.

If you deployed PSTN gateways, IP-PBXs, or Session Border Controllers (SBCs) that do not support the correct capabilities to interact with a pool of Mediation Servers, including the following, then they will need to be associated with a stand-alone pool consisting of a single Mediation Server:

- Perform network layer Domain Name System (DNS) load balancing across Mediation Servers in a pool (or otherwise route traffic uniformly to all Mediation Servers in a pool)
- Accept traffic from any Mediation Server in a pool

You can use the Microsoft Lync Server 2013, Planning Tool to evaluate whether collocating the Mediation Server with your Front End pool can handle the load. If your environment cannot meet these requirements, then you must deploy a stand-alone Mediation Server pool.

Central Site and Branch Site Considerations

Mediation Servers at the central site can be used to route calls for IP-PBXs or PSTN gateways at branch sites. If you deploy SIP trunks, however, you must deploy a Mediation Server at the site where each trunk terminates. Having a Mediation Server at the central site route calls for an IP-PBX or PSTN gateway at a branch site does not require the use of media bypass. However, if you can enable media bypass, doing so will reduce media path latency and, consequently, result in improved media quality because the media path is no longer required to follow the signaling path. Media bypass will also decrease the processing load on the pool.

Note:

Media bypass will not interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed on Unified Communications Open Interoperability Program – Lync Server at http://go.microsoft.com/fwlink/p/?LinkId=268730.

If branch site resiliency is required, a Survivable Branch Appliance or combination of a Front End Server, a Mediation Server, and a gateway must be deployed at the branch site. (The assumption with branch site resiliency is that presence and conferencing are not resilient at the site.) For guidance on branch site planning for voice, see Planning for Branch-Site Voice Resiliency.

For interactions with an IP-PBX, if the IP-PBX does not correctly support early media interactions with multiple early dialogs and RFC 3960 interactions, there can be clipping of the first few words of the greeting for incoming calls from the IP-PBX to Lync endpoints. This behavior can be more severe if a Mediation Server at a central site is routing calls for an IP-PBX where the route terminates at a branch site, because more time is needed for signaling to complete. If you experience this behavior, deploying a Mediation Server at the branch site is the only way to reduce clipping of the first few words.

Finally, if your central site has a TDM PBX, or if your IP-PBX does not eliminate the need for a PSTN gateway, then you must deploy a gateway on the call route connecting Mediation Server and the PBX.

Note:

To improve the media performance of standalone Mediation Server, you should enable receive-side scaling (RSS) on the network adapters on these servers. RSS enables incoming packets to be handled in parallel by multiple processors on the server. For details, see "Receive-Side Scaling Enhancements in Windows Server" at http://go.microsoft.com/fwlink/p/?LinkId=268731. For details about how to enable RSS, see your network adapter documentation.

1.3.10.4.3 PSTN Connectivity Components

PSTN Connectivity Components

Planning > Planning for Enterprise Voice > Components Required for Enterprise Voice >

Topic Last Modified: *2012-10-04*

An enterprise-grade VoIP solution must provide for calls to and from the public switched telephone network (PSTN) without any decline in Quality of Service (QoS). In addition, users should not be aware of the underlying technology when they place and receive calls. From the user's perspective, a call between the Enterprise Voice infrastructure and the PSTN should seem like just another SIP session.

For PSTN connections, you can either deploy a SIP trunk or a PSTN gateway (with a PBX, also known as a Direct SIP link, or without a PBX).

SIP Trunking

As an alternative to using PSTN gateways, you can connect your Enterprise Voice solution to the PSTN by using SIP trunking. SIP trunking enables the following scenarios:

- An enterprise user inside or outside the corporate firewall can make a local or long-distance call specified by an E.164-compliant number that is terminated on the PSTN as a service of the corresponding service provider.
- Any PSTN subscriber can contact an enterprise user inside or outside the corporate firewall by dialing a Direct Inward Dialing (DID) number associated with that enterprise user.

The use of this deployment solution requires a SIP trunking service provider.

PSTN gateways

PSTN gateways are third-party devices that translate signaling and media between the

Enterprise Voice infrastructure and a PSTN or a PBX. PSTN gateways work with the Mediation Server to present a PSTN or PBX call to an Enterprise Voice client. The Mediation Server also presents calls from Enterprise Voice clients to the PSTN gateway for routing to the PSTN or PBX. For a list of partners who work with Microsoft to provide devices that work with Lync Server, see the Microsoft Unified Communications Partners website at http://go.microsoft.com/fwlink/p/?linkId=202836.

Private Branch Exchanges

If you have an existing voice infrastructure that uses a private branch exchange (PBX), you can use your PBX with Lync Server Enterprise Voice.

The supported Enterprise Voice-PBX integration scenarios are as follows:

- IP-PBX that supports media bypass, with a Mediation Server.
- IP-PBX that requires a stand-alone PSTN gateway.
- Time division multiplexing (TDM) PBX, with a stand-alone PSTN gateway.

Note:

Media bypass will not interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed on Unified Communications Open Interoperability Program – Lync Server at http://go.microsoft.com/fwlink/p/?linkId=214406.

For details about partners who offer Enterprise Voice solutions, see the Microsoft Unified Communications Partners website at http://go.microsoft.com/fwlink/p/?linkId=202836.

For details about partners who offer Enterprise Voice hardware solutions, including PSTN gateways, see the Microsoft Unified Communications Partners website http://go.microsoft.com/fwlink/p/?linkId=202836.

1.3.10.4.4 Perimeter Network VoIP Components

Perimeter Network VoIP Components

Planning > Planning for Enterprise Voice > Components Required for Enterprise Voice >

Topic Last Modified: *2012-09-21*

Outside callers who use unified communications clients for individual or conference calls rely on Edge Server for voice communication with coworkers.

On an Edge Server, the Access Edge service provides SIP signaling for calls from Lync users who are outside your organization’s firewall. The A/V Edge service enables media traversal of NAT and firewalls. A caller who uses a unified communications (UC) client from outside the corporate firewall relies on the A/V Edge service for both individual and conference calls.

The A/V Authentication service is collocated with, and provides authentication services for, the A/V Edge service. Outside users who attempt to connect to the A/V Edge service require an authentication token that is provided by the A/V Authentication Service before their calls can go through.

1.3.10.5 Planning for PSTN Connectivity

Planning for PSTN Connectivity

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-09-21*

An enterprise-grade VoIP solution must provide for calls to and from the public switched telephone network (PSTN) without any decline in Quality of Service (QoS). Users who place and receive calls should not be aware of the underlying technology: from the user's perspective, a call between the Enterprise Voice infrastructure and the PSTN should seem like just another phone call.

Lync Server 2013 provides reliable, scalable PSTN connectivity by using the following options:

- **SIP trunks** to an Internet telephony service provider (ITSP)
- **Direct SIP connections** to a PSTN gateway
- **Direct SIP connections** to a PBX

Depending on its size, geographic coverage, and existing voice infrastructure, an enterprise may use one, two, or even all three of these options at various locations.

- SIP Trunking
- Direct SIP Connections
- M:N Trunk
- Translation Rules
- Planning Outbound Voice Routing

1.3.10.5.1 SIP Trunking

SIP Trunking

Planning > Planning for Enterprise Voice > Planning for PSTN Connectivity >

Topic Last Modified: *2012-08-13*

Session Initiation Protocol (SIP) is used to initiate and manage Voice over IP (VoIP) communications sessions for basic telephone service and for additional real-time communication services, such as instant messaging, conferencing, presence detection, and multimedia. This section provides planning information for implementing *SIP trunks*, a type of SIP connection that extends beyond the boundary of your local network.

What is SIP Trunking?

A SIP trunk is an IP connection that establishes a SIP communications link between your organization and an Internet telephony service provider (ITSP) beyond your firewall. Typically, a SIP trunk is used to connect your organization’s central site to an ITSP. In some cases, you may also opt to use SIP trunking to connect your branch site to an ITSP.

SIP Trunks vs. Direct SIP Connections

The term *trunk* is derived from circuit-switched technology. It refers to a dedicated physical line that connects telephone switching equipment. Like their predecessor, time division multiplexing (TDM) trunks, SIP trunks are connections between two separate SIP networks—the Lync Server 2013 enterprise and the ITSP. Unlike circuit-switched trunks, SIP trunks are virtual connections that can be established over any of the supported SIP trunking connection types. For details about the supported connection types, see How Do I Implement SIP Trunking?.

Direct SIP connections, on the other hand, are SIP connections that do not cross the local network boundary (that is, they connect to a public switched telephone network (PSTN) gateway or private branch exchange (PBX) within your internal network). For details about how you can use direct SIP connections with Lync Server 2013, see Direct SIP Connections.

In This Section

- Overview of SIP Trunking
- How Do I Implement SIP Trunking?
- Components and Topologies for SIP Trunking
- Branch Site SIP Trunking
- SIP Trunk Deployment Checklist

1.3.10.5.1.1 Overview of SIP Trunking

Overview of SIP Trunking

Planning for Enterprise Voice > Planning for PSTN Connectivity > SIP Trunking >

Topic Last Modified: *2012-10-05*

Deploying SIP trunking can be a big step toward simplifying your organization’s telecommunications and preparing for up-to-date enhancements to real-time communications. One of the primary advantages of SIP trunking is that you can consolidate your organization’s connections to the public switched telephone network (PSTN) at a central site, as opposed to its predecessor, time division multiplexing (TDM) trunking, which typically requires a separate trunk from each branch site.

SIP Trunking in Lync Server

The Lync Server 2013 SIP trunking capabilities enable the following:

- An enterprise user, whether inside or outside the corporate firewall, can make a local call or a long-distance call that is specified by an E.164-compliant number that is terminated on the PSTN as a service of the corresponding service provider.
- Any PSTN subscriber can contact an enterprise user inside or outside the corporate firewall by dialing a Direct Inward Dialing (DID) number that is associated with that enterprise user.

Cost Savings

The cost savings associated with SIP trunking can be substantial:

- Long distance calls typically cost much less through a SIP trunk.
- You can cut manageability costs and reduce the complexity of deployment.
- Basic rate interface (BRI) and primary rate interface (PRI) fees can be eliminated if you connect a SIP trunk directly to your ITSP at significantly lower cost. In TDM trunking, service providers charge for calls by the minute. The cost of SIP trunking may be based on bandwidth usage, which you can buy in smaller, more economical increments. (The actual cost depends on the service model of the ITSP you choose.)

SIP Trunking vs. Hosting a PSTN Gateway or IP-PBX

Because SIP trunks connect directly to your service provider, you can eliminate your PSTN gateways and their management cost and complexity. Using a SIP trunk can lead to substantial cost savings through reduced maintenance and administration.

Expanded VoIP Services

Voice features are often the primary motivation for deploying SIP trunking, but voice support is just the first step. With SIP trunking, you can extend VoIP capabilities and enable Lync Server 2013 to deliver a richer set of services. For example:

- Enhanced presence detection for devices that are not running Lync Server 2013 can provide better integration with mobile phones, enabling you to see when a user is on a mobile phone call.
- E9-1-1 emergency calling enables the authorities who answer 911 calls to determine the caller's location from his or her telephone number.

Note:
Contact your ITSP for a list of services that they support and can enable for your organization.

1.3.10.5.1.2 How Do I Implement SIP Trunking?

How Do I Implement SIP Trunking?

Planning for Enterprise Voice > Planning for PSTN Connectivity > SIP Trunking >

Topic Last Modified: *2013-03-09*

To implement SIP trunking, you must route the connection through a Mediation Server, which acts as a proxy for communications sessions between Lync Server 2013 clients and the service provider and transcodes media, when necessary.

Each Mediation Server has an internal network interface and an external network interface. The internal interface connects to the Front End Servers. The external interface is commonly called the gateway interface because it has traditionally been used to connect the Mediation Server to a public switched telephone network (PSTN) gateway or an IP-PBX. To implement a SIP trunk, you connect the external interface of the Mediation Server to the external edge component of the ITSP.

Note:
The external edge component of the ITSP could be a Session Border Controller (SBC), a router, or a gateway.

For details about Mediation Servers, see Mediation Server Component.

Centralized vs. Distributed SIP Trunking

Centralized SIP trunking routes all Voice over Internet Protocol (VoIP) traffic, including branch site traffic, through your central site. The centralized deployment model is simple, cost-effective, and is generally the recommended approach for implementing SIP trunks with Lync Server 2013.

Distributed SIP trunking is a deployment model in which you implement a local SIP trunk at one or more branch sites. VoIP traffic is then routed from the branch site directly to a service provider without going through the central site.

Distributed SIP trunking is required only in the following cases:

- The branch site requires survivable phone connectivity (for example, if the WAN goes down). This requirement should be analyzed for each branch site; some of your branches may require redundancy and failover, whereas others may not.
- Resiliency is required between two central sites. You need to make sure that a

SIP trunk terminates at each central site. For example, if you have Dublin and Tukwila central sites and both use only one site's SIP trunk, if the trunk goes down, the other site's users cannot make PSTN calls.
- The branch site and central site are in different countries/regions. For compatibility and legal reasons, you need at least one SIP trunk per country/ region. For example, in the European Union, communications cannot leave a country/region without terminating locally at a centralized point.

Depending on the geographical location of sites and how much traffic you anticipate within your enterprise, you may not want to route all users through the central SIP trunk, or you may opt to route some users through a SIP trunk at their branch site. To analyze your needs, answer the following questions:
- How big is each site (that is, how many users are enabled for Enterprise Voice)?
- Which direct inward dialing (DID) numbers at each site get the most phone calls?

The decision whether to deploy centralized or distributed SIP trunking requires a cost-benefit analysis. In some cases, it may be advantageous to opt for the distributed deployment model even if it is not required. In a completely centralized deployment, all branch site traffic is routed over WAN links. Instead of paying for the bandwidth required for WAN linking, you may want to use distributed SIP trunking. For example, you may want to deploy a Standard Edition server at a branch site with federation to the central site, or you may want to deploy a Survivable Branch Appliance or a Survivable Branch Server with a small gateway.

Note:

For details about distributed SIP trunking, see Branch Site SIP Trunking.

Supported SIP Trunking Connection Types

Lync Server supports the following connection types for SIP trunking:
- Multiprotocol Label Switching (MPLS) is a private network that directs and carries data from one network node to the next. The bandwidth in an MPLS network is shared with other subscribers, and each data packet is assigned a label to distinguish one subscriber's data from another's. This connection type does not require a virtual private network (VPN). A potential drawback is that excessive IP traffic can interfere with VoIP operation unless VoIP traffic is given priority.
- A private connection with no other traffic—for example, a leased fiber-optic connection or T1 line—is typically the most reliable and secure connection type. This connection type provides the highest call-carrying capacity, but it is typically the most expensive. VPN is not required. Private connections are appropriate for organizations with high call volumes or stringent security and availability requirements.
- The Internet is the least expensive connection type, but it is also the least reliable. Internet connection is the only Lync Server SIP trunking connection type that requires VPN.

Selecting a Connection Type

The most appropriate SIP trunking connection type for your enterprise depends on your needs and your budget.
- For a mid-size or larger enterprise, an MPLS network usually provides the greatest value. It can provide the necessary bandwidth at a cheaper rate than a specialized private network.
- Large enterprises may require a private fiber-optic, T1, T3 or higher connection (E1, E3 or higher in the European Union).
- For a small enterprise or branch site with low call volume, SIP trunking through the Internet may be the best choice. This connection type is not recommended

for mid-size or larger sites.

Bandwidth Requirements

The amount of bandwidth your implementation requires depends on call capacity (the number of concurrent calls you must be able to support). You need to consider bandwidth availability, so that you can take full advantage of the peak capacity that you have paid for. Use the following formula to calculate SIP trunk peak bandwidth requirement:

SIP Trunk Peak Bandwidth = Max Simultaneous Calls x (64 kbps + header size)

Note:
Header size is 20 bytes maximum.

Codec Support

Lync Server 2013 supports only the following codecs:

- G.711 a-law (used primarily outside North America)
- G.711 µ-law (used in North America)

Internet Telephony Service Provider

How you implement the service provider side of a SIP trunk connection varies from one ITSP to another. For deployment information, contact your service provider. For a list of certified SIP trunking service providers, see Microsoft Unified Communications Open Interoperability Program website.

For details about Microsoft certified SIP trunking providers, contact your Microsoft representative.

Important:
You must use a Microsoft certified service provider to ensure that your ITSP supports all of the functionality that traverses the SIP trunk (for example, setting up and managing sessions and supporting all of the extended VoIP services). Microsoft technical support does not extend to configurations that use noncertified providers. If you currently use an Internet service provider that is not certified for SIP trunking, you can opt to continue using that provider as your ISP and use a provider certified by Microsoft for SIP trunking.

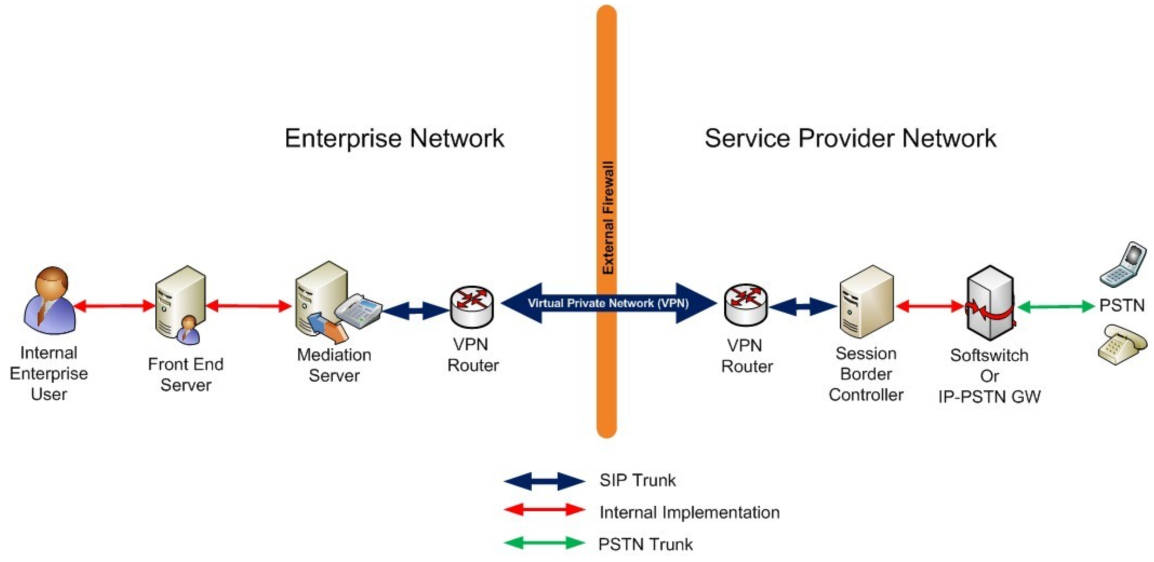
1.3.10.5.1.3 Components and Topologies for SIP Trunking

Components and Topologies for SIP Trunking

Planning for Enterprise Voice > Planning for PSTN Connectivity > SIP Trunking >

Topic Last Modified: *2012-09-21*

The following figure depicts the SIP trunking topology in Lync Server.



As shown in the diagram, an IP virtual private network (VPN) is used for connectivity between the enterprise network and the public switched telephone network (PSTN) service provider. The purpose of this private network is to provide IP connectivity, enhance security, and (optionally) obtain Quality of Service (QoS) guarantees. Because of the nature of a VPN, you do not need to use Transport Layer Security (TLS) for SIP signaling traffic or secure real-time transport protocol (SRTP) for the media traffic. Connections between the enterprise and the service provider therefore consist of plain TCP connections for SIP and plain real-time transport protocol (RTP) (over UDP) for media tunneled through an IP VPN. Ensure that all firewalls between the VPN routers have ports open to allow the VPN routers to communicate, and that the IP addresses on the external edges of the VPN routers are publicly routable.

Important:

Contact your service provider to determine whether it provides support for high availability, including failover. If so, you will need to determine the procedures for setting it up. For example, do you need to configure only one IP address and one SIP trunk on each Mediation Server, or do you need to configure multiple SIP trunks on each Mediation Server?
If you have multiple central sites, also ask whether the service provider has the ability to enable connections to and from another central site.

Note:

For SIP trunking, we strongly recommend that you deploy stand-alone Mediation Servers. For details, see Deploying Mediation Servers and Defining Peers in the Deployment documentation.

Securing the Mediation Server for SIP Trunking

For security purposes, you should set up a virtual LAN (VLAN) for each connection between the two VPN routers. The actual process for setting up a VLAN varies from one router manufacturer to another. For details, contact your router vendor.

We recommend that you follow these guidelines:

- Set up a virtual LAN (VLAN) between the Mediation Server and the VPN router in the perimeter network (also known as DMZ, demilitarized zone, and screened subnet).
- Do not allow broadcast or multicast packets to be transferred from the router

to the VLAN.
- Block any routing rules that route traffic from the router to anywhere but the Mediation Server.

If you use a VPN server, we recommend that you follow these guidelines:

- Set up a VLAN between the VPN server and the Mediation Server.
- Do not allow broadcast or multicast packets to be transmitted from the VPN server to the VLAN.
- Block any routing rule that routes VPN server traffic to anywhere but the Mediation Server.
- Encrypt data on the VPN by using generic routing encapsulation (GRE).

1.3.10.5.1.4 Branch Site SIP Trunking

Branch Site SIP Trunking

Planning for Enterprise Voice > Planning for PSTN Connectivity > SIP Trunking >

Topic Last Modified: *2012-09-21*

In some cases, you may need to implement distributed SIP trunking at selected branch sites. To determine whether a SIP trunk is needed for a branch site, review the information in How Do I Implement SIP Trunking?.

For details about the supported topology options for deploying SIP trunks in branch sites, see Branch-Site Resiliency Solutions.

Example Branch Site SIP Trunk Requirements Analysis

When you decide to deploy a branch site SIP trunk, you need to perform a site-specific cost analysis. For example, an enterprise that has a central site in Redmond, Washington, and a branch site in New York, should do an analysis to determine whether to implement a SIP trunk from the New York site to a local service provider.

To determine whether a distributed SIP trunk in New York is cost-effective, identify which Direct Inward Dialing (DID) numbers will use the SIP trunk, and analyze the number of calls New York makes to areas other than Redmond (425). You can have DID termination for the branch site at the central site. For example, the Redmond central site can host DID numbers for the New York branch site. If the cost of implementing a distributed SIP trunk is less than the cost of those calls, consider implementing a SIP trunk at the New York branch site.

Other Branch Site SIP Trunk Requirements

The choice between a deploying a SIP trunk instead of a gateway is based on the difference between the public switched telephone network (PSTN) long distance toll charges of each option. If you deploy a branch site SIP trunk, you also need to determine your resiliency and bandwidth requirements. If the link between your branch site and central site is resilient and has sufficient bandwidth, you can deploy a SIP trunk or a gateway. You do not need to deploy a Survivable Branch Appliance at the branch site. If the link between your branch site and central site is not resilient, deploy a Survivable Branch Appliance, or deploy a Survivable Branch Server with either a gateway or SIP trunk at the branch site.

1.3.10.5.1.5 SIP Trunk Deployment Checklist

SIP Trunk Deployment Checklist

Planning for Enterprise Voice > Planning for PSTN Connectivity > SIP Trunking >

Topic Last Modified: *2012-09-21*

Before you can deploy a SIP trunk, you and your service provider must exchange some basic connection information about your respective SIP trunk endpoints.

Get the following information for each ITSP gateway that you will connect to:

- IP address
- Fully qualified domain name (FQDN)

Note:

The service provider may ask you to connect to more than one ITSP gateway. In that case, you must configure a connection between each ITSP gateway and each Mediation Server in your pool.

The information you give to your service provider depends on your SIP trunk connection type:

- For Multiprotocol Label Switching (MPLS) or private network connections, give the ITSP the publicly routable IP Address of the router in your perimeter network (also known as DMZ, demilitarized zone, and screened subnet). Verify that the gateway or Session Border Controller (SBC) at the ITSP can reach this address. Also give the ITSP the FQDN of your Mediation Server.
- For virtual private network (VPN) connections, give the ITSP the IP address of your VPN server.

Certificate Considerations

To determine whether you need a certificate for SIP trunking, check with your ITSP about protocol support:

1. If your ITSP supports Transmission Control Protocol (TCP) only, you do not need a certificate.
2. If your ITSP supports Transport Layer Security (TLS), the ITSP must provide you with a certificate.

Note:

SIP works in conjunction with real-time transport protocol (RTP) or secure real-time transport protocol (SRTP), the protocols that manage the actual voice data in Voice over Internet Protocol (VoIP) calls.

Deployment Process

To implement the Lync Server side of the SIP trunk connection, follow these steps:

1. Using the Lync Server Topology Builder, create and configure the SIP domain topology. For details, see Define and Configure a Topology in Topology Builder in the Deployment documentation.
2. Using the Lync Server Control Panel, configure voice routing for the new SIP domain. For details, see Configuring Trunks in the Deployment documentation.
3. Test connectivity by using the **Test-CsPstnOutboundCall** cmdlet. For details, see the Lync Server Management Shell documentation or Help for Lync Server Management Shell.

1.3.10.5.2 Direct SIP Connections

Direct SIP Connections

Planning > Planning for Enterprise Voice > Planning for PSTN Connectivity >

Topic Last Modified: *2012-08-13*

You can use *direct SIP connections* to connect Lync Server to either of the following:

- An IP-PBX (for details, see Direct SIP Deployment Options).
- A PSTN gateway (for details, see PSTN Gateway Deployment Options).

To implement a direct SIP connection, you follow essentially the same deployment steps as you would to implement a SIP trunk. In both cases, you implement the connection by using the external interface of a Mediation Server. The only difference is that you connect SIP trunks to an external entity, such as an ITSP gateway, and you connect direct SIP connections to an internal entity within your local network, such as an IP-PBX or a public switched telephone network (PSTN) gateway.

In This Section

- Direct SIP Deployment Options
- PSTN Gateway Deployment Options

1.3.10.5.2.1 Direct SIP Deployment Options

Direct SIP Deployment Options

Planning for Enterprise Voice > Planning for PSTN Connectivity > Direct SIP Connections >

Topic Last Modified: *2012-09-21*

This topic provides example topologies for deploying direct SIP connections.

Lync Server Stand-Alone

If your organization uses one of the deployments described in this section, you can use Lync Server 2013 as the sole telephony solution for part or all of an organization. This section describes the following deployments in detail:

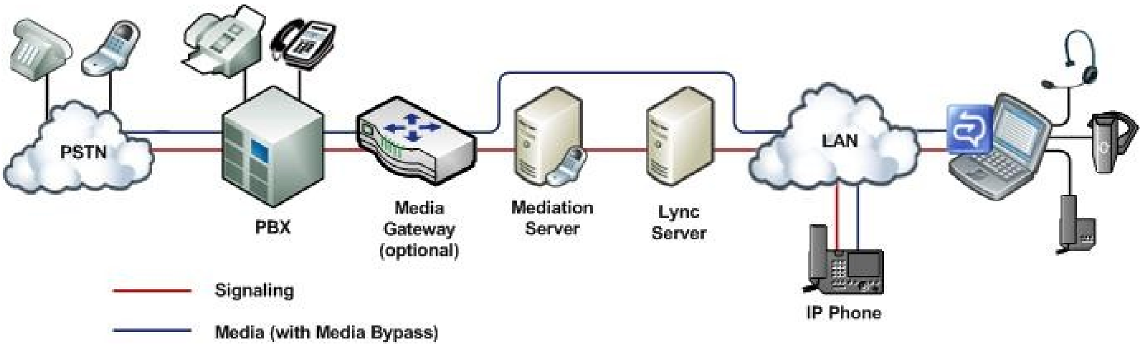
- **Incremental deployment:** This option assumes that you have an existing private branch exchange (PBX) infrastructure and you intend to introduce Enterprise Voice incrementally to smaller groups or teams within your organization.
- **Lync Server VoIP-only deployment:** this option assumes that you are considering deploying Enterprise Voice at a site that does not have a traditional telephony infrastructure.

Incremental Deployment

In incremental deployment, Lync Server 2013 is the sole telephony solution for individual teams or departments, while the rest of the users in an organization continue to use a PBX. This incremental deployment strategy provides one way to introduce IP telephony into your enterprise through controlled pilot programs. Workgroups whose communication needs are best served by Microsoft Unified Communications are moved to Enterprise Voice, while other users remain on the existing PBX. Additional workgroups can be migrated to Enterprise Voice, as needed.

The incremental option is recommended if you have clearly defined user groups that have communication requirements in common and that lend themselves to centralized management. This option is also effective if you have teams or departments that are spread over wide geographic areas, where the savings in long-distance charges can be significant. In fact, this option is useful for creating virtual teams whose members may be scattered across the globe. You can create, modify, or disband such teams in rapid response to shifting business requirements.

The following figure shows the generic topology for deployment of Enterprise Voice behind a PBX. This is the recommended topology for incremental deployment.



Note:
If you are connecting your Lync Server deployment to a certified Direct SIP partner, a public switched telephone network (PSTN) gateway between the Mediation Server and the PBX is not required. For a list of certified Direct SIP partners, see the Microsoft Unified Communications Open Interoperability Program website at http://go.microsoft.com/fwlink/p/?linkId=203309.

Note:
The media path shown in this figure has media bypass enabled (the recommended configuration). If you opt to disable media bypass, the media path is routed through the Mediation Server.

In this topology, selected departments or workgroups are enabled for Enterprise Voice. A PSTN gateway links the Voice over Internet Protocol (VoIP)-enabled workgroup to the PBX. Users who are enabled for Enterprise Voice, including remote workers, communicate across the IP network. Calls by Enterprise Voice users to the PSTN and to coworkers who are not enabled for Enterprise Voice are routed to the appropriate PSTN gateway. Calls from colleagues who are still on the PBX system, or from callers on the PSTN, are routed to the PSTN gateway, which forwards the calls to Lync Server for routing.

There are two recommended configurations for connecting Enterprise Voice to an existing PBX infrastructure for interoperability: Enterprise Voice behind the PBX and Enterprise Voice in front of the PBX.

Enterprise Voice Behind the PBX
When Enterprise Voice is deployed behind the PBX, all calls from the PSTN arrive at the PBX, which routes calls to Enterprise Voice users to a PSTN gateway, and calls to PBX users to the PBX.

Enterprise Voice in Front of the PBX
When Enterprise Voice is deployed in front of the PBX, all calls arrive at the PSTN gateway, which routes calls for Enterprise Voice users to Lync Server and calls for PBX users to the PBX. Calls to the PSTN from both Enterprise Voice and PBX users are routed over the IP network to the most cost-efficient PSTN gateway. The following table shows the advantages and disadvantages of this configuration.

Advantages and Disadvantages of Deploying Enterprise Voice in Front of PBX

Advantages	Disadvantages

PBX still serves users not enabled for Enterprise Voice.	Existing gateways may not support the features or capacity that you want.
PBX handles all earlier devices.	Requires a trunk from gateway to the PBX and from the gateway to the Mediation Server. You may need more trunks from the service provider.
Enterprise Voice users keep the same phone numbers.	

Lync Server VoIP-Only Deployment

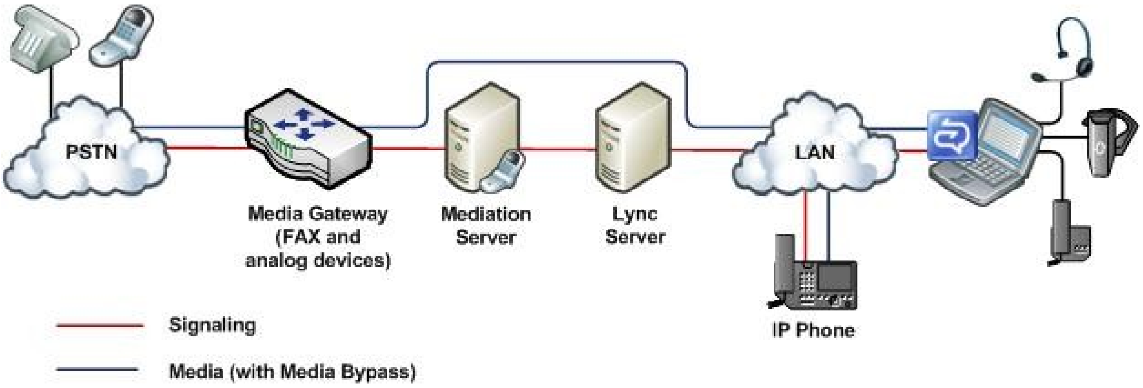
Enterprise Voice provides new businesses, and also new office sites for existing businesses, with the opportunity to implement a full-featured VoIP solution without having to worry about PBX integration or incurring the substantial deployment and maintenance costs of an IP-PBX infrastructure. This solution supports both on-site and remote workers.

In this deployment, all calls are routed over the IP network. Calls to the PSTN are routed to the appropriate PSTN gateway. Lync 2013 or Lync Phone Edition serves as a softphone. Remote call control is unavailable and unnecessary because there are no PBX phones for users to control. Voice mail and auto-attendant services are available through the optional deployment of Exchange Unified Messaging (UM).

Note:

In addition to the network infrastructure that is required to support Lync Server 2013, a VoIP-only deployment can use a small, qualified gateway to support fax machines and analog devices.

The following figure shows a typical topology for a VoIP-only deployment.


PSTN
Media Gateway (FAX and analog devices)
Mediation Server
Lync Server
LAN
IP Phone
Signaling
Media (with Media Bypass)

Note:

The media path shown in this figure has media bypass enabled (the recommended configuration). If you opt to disable media bypass, the media path is routed through the Mediation Server.

1.3.10.5.2.2 PSTN Gateway Deployment Options

PSTN Gateway Deployment Options

Planning for Enterprise Voice > Planning for PSTN Connectivity > Direct SIP Connections >

Topic Last Modified: *2012-09-21*

PSTN Gateways

Public switched telephone network (PSTN) gateways are third-party hardware components that translate signaling and media between the Enterprise Voice infrastructure and the PSTN, either directly or through connection to SIP trunks. In either topology, the gateway terminates the PSTN. The gateway is isolated in its own subnet and is connected to the enterprise network through the Mediation Server.

An enterprise with multiple sites would typically deploy one or more gateways at each site. Branch sites can connect to the PSTN either through a gateway, or through a Survivable Branch Appliance, which combines gateway and servers in a single box. If branch sites use a gateway, both a Registrar and Mediation Server are required on site, unless the WAN link is resilient. One or more Mediation Servers, which are collocated on Front End Servers, can route calls for the one or more gateways at each site. We recommend that the Registrar, Mediation Server, and gateway required on site are deployed as a Survivable Branch Appliance.

Determining the number, size, and location of PSTN gateways is perhaps the most important and expensive decision you must make when planning your Enterprise Voice infrastructure.

Here are the main questions to consider. Keep in mind that the answers to these questions are all interdependent

- How many PSTN gateways are needed? The answer depends on the number of users, the anticipated number of simultaneous calls (traffic load), and the number of sites (each site needs one).
- What size should the gateways be? The answer depends on the number of users at the site and on the traffic load.
- Where should the gateways be located? The answer depends in part on the topology and in part on the geographic distribution of your organization.

You should also consider your gateway topology options (for details, see Gateway Topologies later in this topic).

M:N Trunk Support

The Mediation Servers can route calls through multiple gateways, Session Border Controllers (SBCs) provided by Internet telephony service providers, or a combination of the two. Additionally, multiple Mediation Servers in the pool can interact with multiple gateways. The logical route defined between a Mediation Server and gateway is called a *trunk*. When an internal user places a PSTN call, outbound routing logic on the Front End pool chooses which trunk to route over out of all possible combinations that may be available for routing that particular call. With DNS load balancing, if a call fails to reach a gateway due to an issue with a particular Mediation Server in the pool, the call will be retried to an alternate Mediation Server in the pool.

For details about planning for multiple gateways, see M:N Trunk.

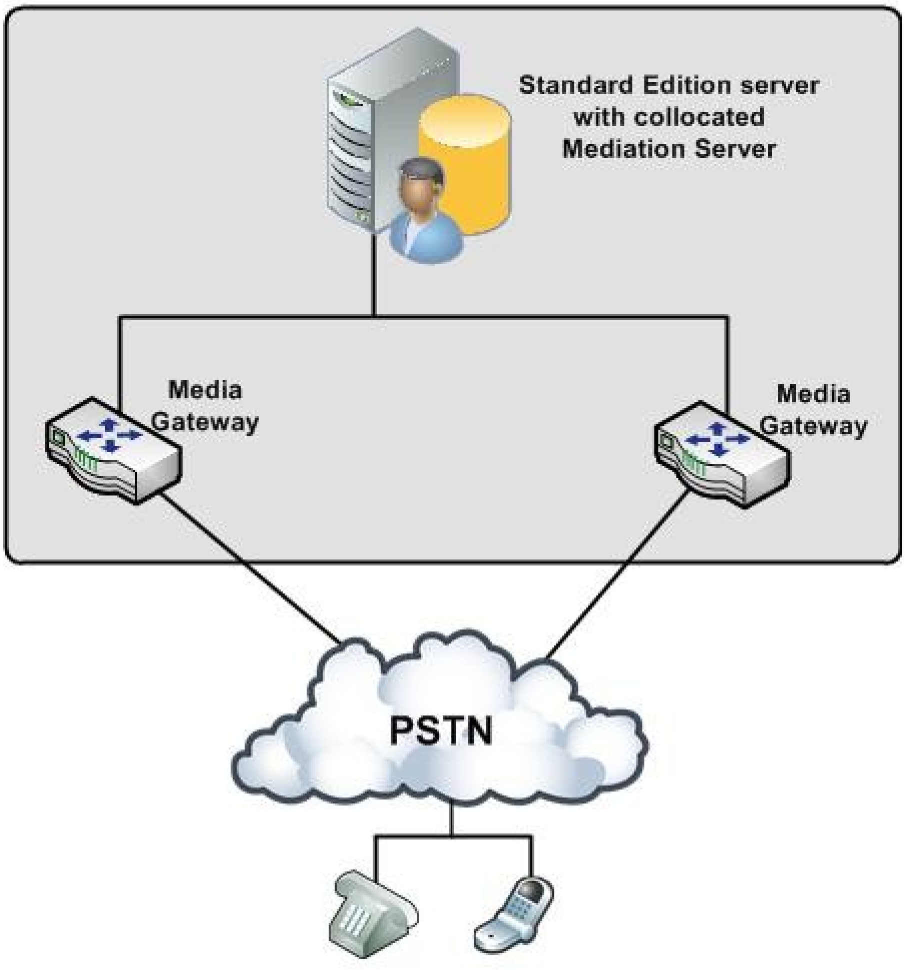
For details about other outbound routing enhancements, see Voice Routes.

Gateway Topologies

When you consider the fundamental questions of gateway deployment, follow these steps:

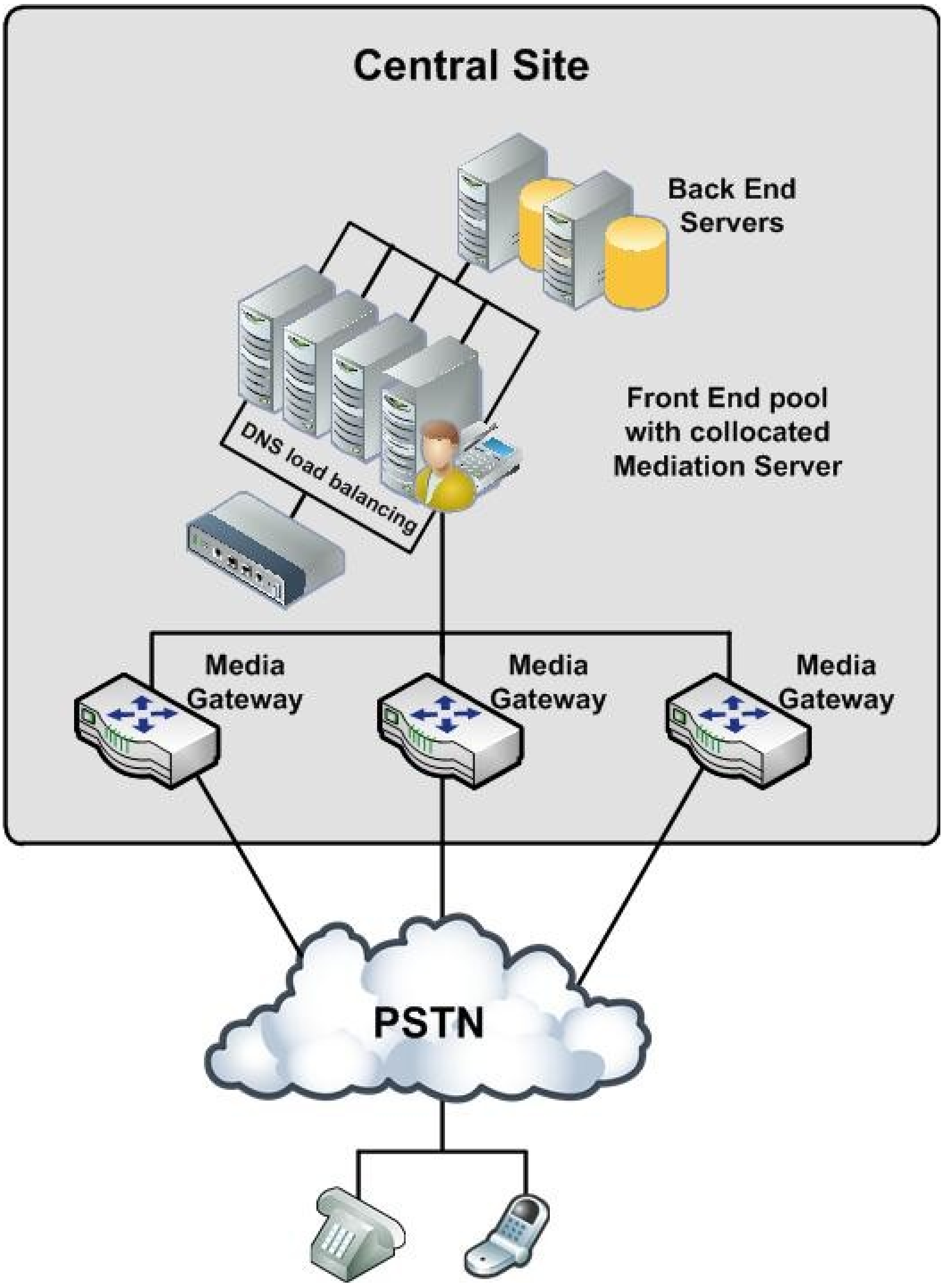
1. Count the sites at which you want to provide PSTN connectivity by using Enterprise Voice.
2. Estimate the traffic at each site (number of users and average number of calls per hour per user).
3. Deploy one or more gateways at each site to handle the anticipated traffic.

The resulting distributed gateway topology is shown in the following figure.



With this topology, calls among workers at each site and between sites are all routed over your intranet. Calls to the PSTN are routed over the enterprise IP network to the gateways that are closest to the location of the destination numbers.But what if your organization supports dozens or hundreds or even thousands of sites spread across one or more continents, as many financial institutions and other large enterprises do? In such cases, deploying a separate gateway at each site is not practical.

To address this issue, many large companies prefer to deploy one or a few large telephony central sites, as shown in the following figure.



In this topology, several large gateways sufficient to accommodate the anticipated user load are deployed at each central site. All calls to users in the enterprise are forwarded by the company's telephone service provider to a central site. Routing logic at the central site determines whether the call should be routed over the intranet or to the PSTN.

Gateway Location

Gateway location may also determine the types of gateways that you choose and how they are configured. There are dozens of PSTN protocols, none of which is a worldwide standard. If all your gateways are located in a single country/region, this is not an issue, but if you locate gateways in several countries/regions, each must be configured according to the PSTN standards of that country/region. Moreover, gateways that are certified for operation in, for example, Canada, may not be certified in India, Brazil, or the European Union.

Gateway Size and Number

The PSTN gateways that most organizations will consider deploying range in size from 2 to as many as 960 ports. (There are even larger gateways, but these are used mainly by telephone service providers.) When estimating the number of ports your organization requires, use the following guidelines:

- Organizations with light telephony usage (one PSTN call per user per hour) should allocate one port for every 15 users. For example, if you have 20 users, you will require a gateway with two ports.
- Organizations with moderate telephony usage (two PSTN calls per user per hour) should allocate one port for every 10 users. For example, if you have 100 users, you will require a total of 10 ports allocated among one or more gateways.
- Organizations with heavy telephony usage (three or more PSTN calls per user per hour) should allocate one port for every five users. For example, if you have 47,000 users, you will require a total of 9,400 ports allocated among at least 10 large gateways.
- Additional ports can be acquired as the number of users or amount of traffic in your organization increases.

For any given number of users you must support, you have the choice of deploying fewer, larger gateways, or smaller ones. As a rule, a minimum of two gateways for an organization is recommended to maintain availability if one gateway fails.

Each PSTN gateway that you deploy must have at least one corresponding Mediation Server.

1.3.10.5.3 M:N Trunk

M:N Trunk

Planning for Enterprise Voice > Components Required for Enterprise Voice > Mediation Server Component >

Topic Last Modified: *2012-10-01*

Lync Server 2013 supports greater flexibility in the definition of a trunk for call routing purposes from previous releases. A trunk is a logical association between a Mediation Server and listening port number with a gateway and a listening port number. This implies several things: A Mediation Server can have multiple trunks to the same gateway; a Mediation Server can have multiple trunks to different gateways; conversely a gateway can have multiple trunks to different Mediation Servers.

A root trunk is still required to be created when a gateway is added to the Lync topology using Topology Builder. The number of gateways that a given Mediation Server can handle depends on the processing capacity of the server during peak busy hours. If you deploy a Mediation Server on hardware that exceeds the minimum hardware requirements for Lync Server 2013, as described in Supported Hardware in the Supportability documentation, then the estimate of how many active non-bypass calls a stand-alone Mediation Server can handle is approximately 1000 calls. When deployed on hardware meeting these specifications, the Mediation Server is expected to perform transcoding, but still route calls for multiple gateways even if the gateways do not support media bypass.

When defining a call route, you specify the trunks associated with that route, but you do not specify which Mediation Servers are associated with that route. Instead, you use Topology Builder to associate trunks with Mediation Servers. In other words, routing determines which trunk to use for a call, and, subsequently, the Mediation Server associated with that trunk is sent the signaling for that call.

The Mediation Server can be deployed as a pool; this pool can be collocated with a Front End pool, or it can be deployed as a stand-alone pool. When a Mediation Server is collocated with a Front End pool, the pool size can be at most 12 (the limit of the Registrar pool size). Taken together, these new capabilities increase the reliability and deployment flexibility for Mediation Servers, but they require associated capabilities in the following peer entities:

- **PSTN gateway.** A Lync Server 2013 qualified gateway must implement DNS load balancing, which enables a qualified public switched telephone network (PSTN) gateway to act as a load balancer for one pool of Mediation Servers, and thereby to load-balance calls across the pool.
- **Session Border Controller.** For a SIP trunk, the peer entity is a Session Border Controller (SBC) at an Internet telephony service provider. In the direction from the Mediation Server pool to the SBC, the SBC can receive connections from any Mediation Server in the pool. In the direction from the SBC to the pool, traffic can be sent to any Mediation Server in the pool. One method of achieving this is through DNS load balancing, if supported by the service provider and SBC. An alternative is to give the service provider the IP addresses of all Mediation Servers in the pool, and the service provider will provision these in their SBC as a separate SIP trunk for each Mediation Server. The service provider will then handle the load balancing for its own servers. Not all service providers or SBCs may support these capabilities. Furthermore, the service provider may charge extra for this capability. Typically, each SIP trunk to the SBC incurs a monthly fee.
- **IP-PBX.** In the direction from the Mediation Server pool to the IP-PBX SIP termination, the IP-PBX can receive connections from any Mediation Server in the pool. In the direction from the IP-PBX to the pool, traffic can be sent to any Mediation Server in the pool. Because most IP-PBXs do not support DNS load balancing, we recommend that individual direct SIP connections be defined from the IP-PBX to each Mediation Server in the pool. The IP-PBX will then handle its own load balancing by distributing traffic over the trunk group. The assumption is that the trunk group has a consistent set of routing rules at the IP-PBX. Whether a particular IP-PBX supports this trunk group concept and how it intersects with the IP-PBX's own redundancy and clustering architecture needs to be determined before you can decide whether a Mediation Server cluster can interact correctly with an IP-PBX.

A Mediation Server pool must have a uniform view of the peer gateway with which it interacts. This means that all members of the pool access the same definition of the peer gateway from the configuration store and are equally likely to interact with it for outgoing calls. Therefore, there is no way to segment the pool so that some Mediation Servers communicate with only certain gateway peers for outgoing calls. If such segmentation is necessary, a separate pool of Mediation Servers must be used. This would be the case, for example, if the associated capabilities in PSTN gateways, SIP trunks, or IP-PBXs to interact with a pool as detailed earlier in this topic are not present.

A particular PSTN gateway, IP-PBX, or SIP trunk peer can route to multiple Mediation Servers or trunks. The number of gateways that a particular pool of Mediation Servers can control depends on the number of calls that use media bypass. If a large number of calls use media bypass, a Mediation Server in the pool can handle many more calls, because only signaling layer processing is necessary.

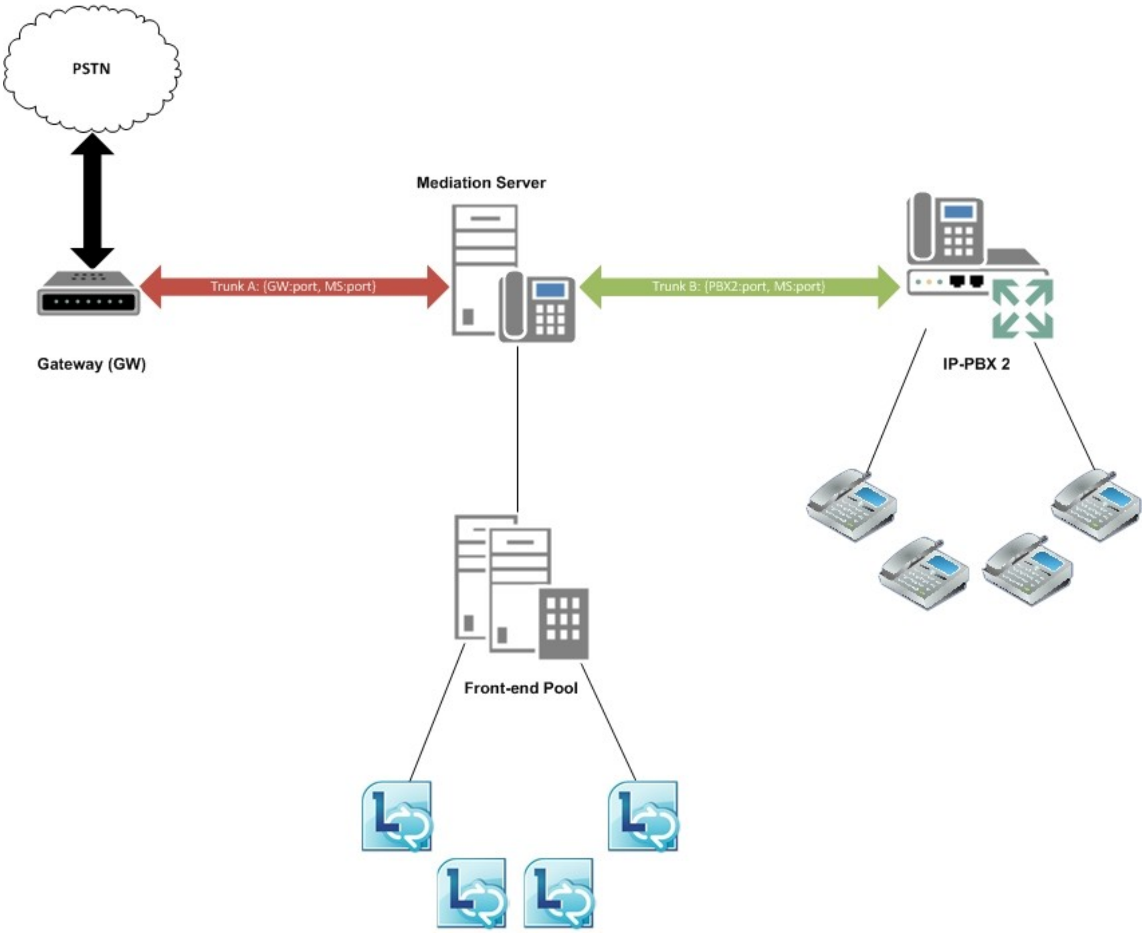
Inter-Trunk Routing

Planning > Planning for Enterprise Voice > Planning for PSTN Connectivity >

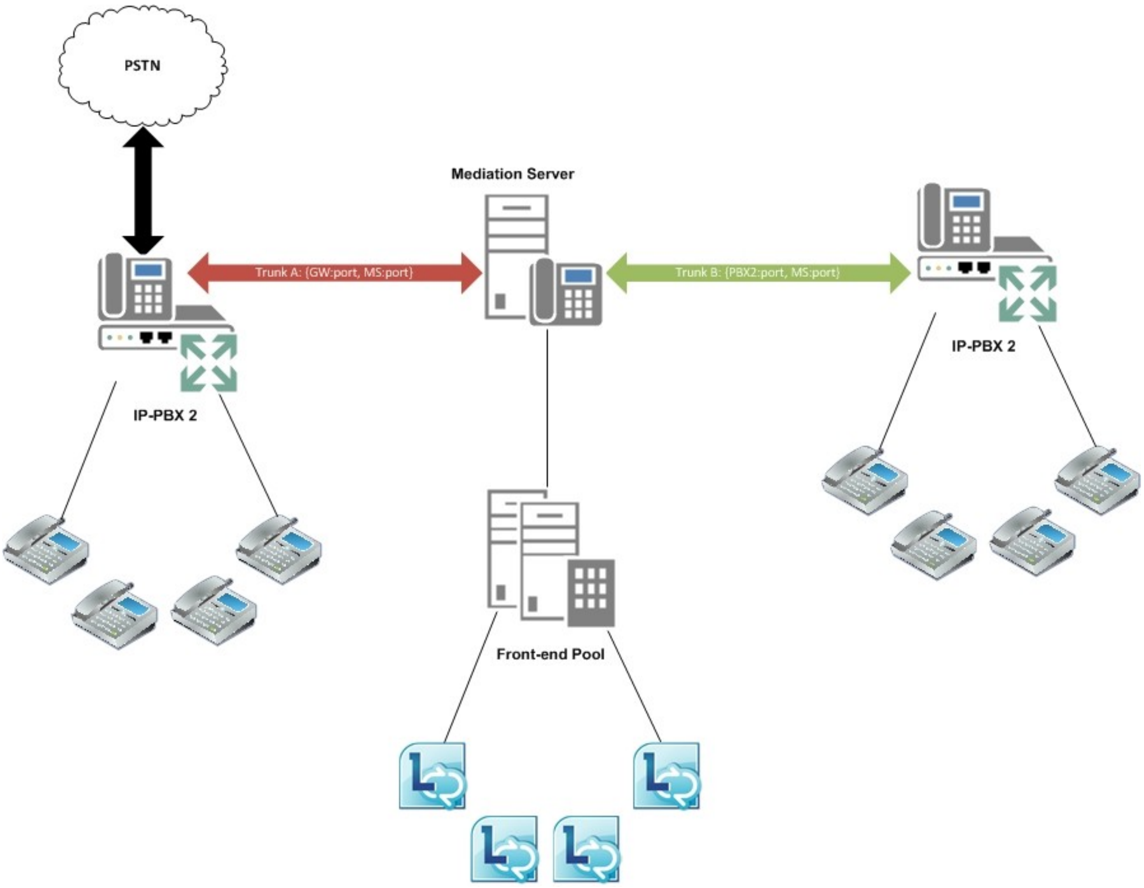
Topic Last Modified: *2012-10-08*

Lync Server 2013 provides basic session management through the support of intertrunk routing. This new capability enables Lync Server to provide call control functionalities to downstream telephony systems. Intertrunk routing can interconnect an IP-PBX to a public switched telephone network (PSTN) gateway so that calls from a private branch exchange (PBX) phone can be routed to the PSTN, and incoming PSTN calls can be routed to a PBX phone. Similarly, Lync Server can interconnect two or more IP-PBX systems so that calls can be placed and received between PBX phones from the different IP-PBX systems.

The following figure illustrates Lync Server 2013 providing interconnectivity between a PSTN gateway and an IP-PBX.



The next figure illustrates Lync Server 2013 connecting two IP-PBX systems.



1.3.10.5.5 Translation Rules

Translation Rules

[Planning](#) > [Planning for Enterprise Voice](#) > [Planning for PSTN Connectivity](#) >

Topic Last Modified: *2012-10-05*

Lync Server 2013 Enterprise Voice requires that all dial strings be normalized to E.164 format for the purpose of performing reverse number lookup (RNL). In Microsoft Lync Server 2010, translation rules are supported only for called numbers. New in Microsoft Lync Server 2013, translation rules are also supported for calling numbers. The *trunk peer* (that is, the associated gateway, private branch exchange (PBX), or SIP trunk) may require that numbers be in a local dialing format. To translate numbers from E.164 format to a local dialing format, you can define one or more translation rules to manipulate the request URI before you route it to the trunk peer. For example, you could write a translation rule to remove +44 from the beginning of a dial string and replace it with 0144.

By performing outbound route translation on the server, you can reduce the configuration requirements on each individual trunk peer in order to translate phone numbers into a local dialing format. When you plan which gateways, and how many gateways, to associate with a specific Mediation Server cluster, it may be useful to group trunk peers with similar local dialing requirements. This can reduce the number of required translation rules and the time it takes to write them.

Important:

Associating one or more translation rules with an Enterprise Voice trunk configuration should be used as an alternative to configuring translation rules on the trunk peer. Do not associate translation rules with an Enterprise Voice trunk configuration if you have configured translation rules on the trunk peer, because the two rules might conflict.

Example Translation Rules

The following examples of translation rules show how you can develop rules on the server to translate numbers from E.164 format to a local format for the trunk peer.

For details about how to implement translation rules, see Defining Translation Rules in the Deployment documentation.

Description	Starting Digits	Length	Digits to Remove	Digits to Add	Matching Pattern	Translation	Example
Conventional long-distance dialing in U.S. (strip out the '+')	+1	Exactly 12	1	0	^\+(1\d{10})$	$1	+14255551010 becomes 14255551010
U.S. international long-distance dialing (strip out '+' and add 011)	+	At least 11	1	011	^\+(\d{9}\d+)$	011$1	+441235551010 becomes 011441235551010

1.3.10.5.6 Planning Outbound Voice Routing

Planning Outbound Voice Routing

See Also

Planning > Planning for Enterprise Voice > Planning for PSTN Connectivity >

Topic Last Modified: *2012-09-21*

Outbound call routing applies to calls that are destined for a public switched telephone network (PSTN) gateway, trunk, or private branch exchange (PBX). When a user places a call, the server normalizes the phone number to E.164 format, if necessary, and attempts to match it to a SIP URI. If the server cannot make the match, it applies outbound call routing logic based on the supplied dial string. You define that logic by configuring the server settings that are described in the following table.

Lync Server Outbound Call Routing Settings

Object	Description
Dial Plan	A dial plan is a named set of normalization rules that translates phone numbers for a

	named location, individual user, or contact object into a single standard (E.164) format for purposes of phone authorization and call routing.
Normalization rule	Normalization rules define how phone numbers expressed in various formats are to be routed for each specified location, user, or contact object. The same dial string may be interpreted and translated differently, depending on the location from which it is dialed and the person or contact object that makes the call. A set of normalization rules associated with a particular location constitutes a dial plan.
Voice policy	A voice policy associates one or more PSTN usage records with one user or a group of users. A voice policy also provides a list of calling features that you can enable or disable.
PSTN usage record	A PSTN usage record specifies a class of call (such as internal, local, or long distance) that can be made by various users, or groups of users, in an organization.
Call Route	A call route associates destination phone numbers with particular trunks and PSTN usage records. A PSTN gateway is considered a trunk.

This section provides guidelines for configuring the following outbound call routing server settings:

- Dial Plans and Normalization Rules
- Voice Policies
- PSTN Usage Records
- Voice Routes

⊟See Also

Concepts

SIP Trunking
Direct SIP Connections

1.3.10.5.6.1 Dial Plans and Normalization Rules

Dial Plans and Normalization Rules

Planning for Enterprise Voice > Planning for PSTN Connectivity > Planning Outbound Voice Routing >

Topic Last Modified: *2012-09-21*

A dial plan is a named set of normalization rules that translates phone numbers for a named location, individual user, or contact object into a single standard (E.164) format for purposes of phone authorization and call routing.

Normalization rules define how phone numbers expressed in various formats are to be routed for each specified location, user, or contact object. The same dial string may be interpreted and translated differently, depending on the location from which it is dialed and the person or contact object making the call.

Dial Plan Scope

A dial plan's *scope* determines the hierarchical level at which the dial plan can be applied. In Lync Server, a user can be assigned a specific per-user dial plan. If a user dial plan is not assigned, the Registrar pool dial plan is applied. If there is no Registrar pool dial plan, the site dial plan is applied. Finally, if there is no other dial plan applicable to the user, the global dial plan is applied.

Clients obtain dial plan scope levels through in-band provisioning settings that are provided when users log on to Lync Server. As the administrator, you can manage and assign dial plan scope levels by using Lync Server Control Panel.

Note:

The service level public switched telephone network (PSTN) gateway dial plan is applied to the incoming calls from a particular gateway.

Dial plan scope levels are defined as follows:

- **User dial plan:** Can be assigned to individual users, groups, or contact objects. Voice applications can look up a per-user dial plan when a call is received with the phone-context set to user-default. For the purpose of assigning a dial plan, a contact object is treated as an individual user.
- **Pool dial plan:** Can be created at the service level for any PSTN gateway or Registrar in your topology. To define a pool dial plan, you must specify the particular service (PSTN gateway or Registrar pool) to which the dial plan applies.
- **Site dial plan:** Can be created for an entire site, except for any users, groups, or contact objects that are assigned a pool dial plan or user dial plan. To define a site dial plan, you must specify the site to which the dial plan applies.
- **Global dial plan:** The default dial plan installed with the product. You can edit the global dial plan, but you cannot delete it. This dial plan applies to all Enterprise Voice users, groups, and contact objects in your deployment, unless you configure and assign a dial plan with a more specific scope.

Planning for Dial Plans

To plan a dial plan, follow these steps:

- List all the locales in which your organization has an office.
  The list must be up-to-date and complete. It will need to be revised as company organization evolves. In a large, multinational company with numerous small branch offices, this can be a time-consuming task.
- Identify valid number patterns for each site.
  The most time-consuming part of planning your dial plans is identifying the valid number patterns for each site. In some cases, you may be able to copy normalization rules that you have written for one dial plan to other dial plans, especially if the corresponding sites are within the same country/region or even continent. In other cases, small changes to numbers in one dial plan may be enough to use them in other dial plans.
- Develop an organization-wide scheme for naming dial plans.
  Adopting a standard naming scheme assures consistency across an organization and makes maintenance and updates easier.
- Decide whether multiple dial plans are required for a single location.
  If your organization maintains a single dial plan across multiple locations, you may still need to create a separate dial plan for Enterprise Voice users who are migrating from a private branch exchange (PBX) and who need to have their existing extensions retained.

- Decide whether per-user dial plans are required. For example, if you have users at a branch site who are registered with the central site or if you have users who are registered on a Survivable Branch Appliance, you can consider special dialing scenarios for such users using per-user dial plans and normalization rules. For details, see Branch-Site Resiliency Requirements.
- Determine dial plan scope (as previously described in this topic).

To create a dial plan, you specify values in the following fields, as required, by using Lync Server Control Panel or Lync Server Management Shell.

Name and Simple Name

For user dial plans, you should specify a descriptive name that identifies the users, groups, or contact objects to which the dial plan will be assigned. For site dial plans, the Name field is prepopulated with the site name and cannot be changed. For pool dial plans, the Name field is prepopulated with the PSTN gateway or Front End pool fully qualified domain name (FQDN) and cannot be changed.

The dial plan *Simple Name* is prepopulated with a string that is derived from the dial plan name. The Simple Name field is editable, which enables you to create a more descriptive naming convention for your dial plans. The *Simple Name* value cannot be empty and must be unique. A best practice is to develop a naming convention for your entire organization and then use this convention consistently across all sites and users.

Description

We recommend that you type the common, recognizable name of the geographic location to which the corresponding dial plan applies. For example, if the dial plan name is London.Contoso.com, the recommended description would be London.

Dial-in Conferencing Region

If you are deploying dial-in conferencing, you will need to specify a dial-in conferencing region to associate dial-in conferencing access numbers with a dial plan.

External Access Prefix

You can specify an external access prefix of up to four characters (#, *, and 0-9) if users need to dial one or more additional leading digits (for example, 9) to get an external line.

Note:

If you specify an external access prefix, you do not need to create an additional normalization rule to accommodate the prefix.

Normalization Rules

Normalization rules define how phone numbers expressed in various formats are to be routed for the named location. The same number string may be interpreted and translated differently, depending on the locale from which it is dialed. Normalization rules are necessary for call routing because users can, and do, use various formats when entering phone numbers in their Contacts lists.

Normalizing user-supplied phone numbers provides a consistent format that facilitates the following tasks:

- Match a dialed number to the intended recipient's SIP-URI.
- Apply dialing authorization rules to the calling party.

The following number fields are among those that your normalization rules may need to account for:

- Dial plan
- Country code
- Area code
- Length of extension

- Site prefix

Creating Normalization Rules

Normalization rules use .NET Framework regular expressions to specify numeric match patterns that the server uses to translate dial strings to E.164 format for the purpose of performing reverse number lookup. You create normalization rules in the Lync Server Control Panel either by entering the expressions manually, or by entering the starting digits and the length of the dial strings to be matched and letting the Lync Server Control Panel generate the corresponding regular expression for you. Either way, when you finish, you can enter a test number to verify that the normalization rule works as expected.

For details about using .NET Framework regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.

Sample Normalization Rules

The following table shows sample normalization rules that are written as .NET Framework regular expressions. The samples are examples only and are not meant to be a prescriptive reference for creating your own normalization rules.

Table 1.Normalization Rules Using .NET Framework Regular Expressions

Rule name	Description	Number pattern	Translation	Example
4digitExtension	Translates 4-digit extensions	^(\d{4})$	+1425555$1	0100 is translated to +14255550100
5digitExtension	Translates 5-digit extensions	^5(\d{4})$	+1425555$1	50100 is translated to +14255550100
7digitcallingRedmond	Translates 7-digit numbers to Redmond local numbers	^(\d{7})$	+1425$1	5550100 is translated to +14255550100
7digitcallingDallas	Translates 7-digit numbers to Dallas local numbers	^(\d{7})$	+1972$1	5550100 is translated to +19725550100
10digitcallingUS	Translates 10-digit numbers in the United States	^(\d{10})$	+1$1	2065550100 is translated to +12065550100
LDCallingUS	Translates numbers with long distance prefixes in the United States	^1(\d{10})$	+$1	12145550100 is translated to +2145550100
IntlCallingUS	Translates numbers with international prefixes in the United States	^011(\d*)$	+$1	01191445550100 is translated to +91445550100
RedmondOperator	Translates 0 to Redmond Operator	^0$	+14255550100	0 is translated to +14255550100

RedmondSitePrefix	Translates numbers with on-net prefix (6) and Redmond site code (222)	^6222(\d{4})$	+1425555$1	62220100 is translated to +14255550100
NYSitePrefix	Translates numbers with on-net prefix (6) and NY site code (333)	^6333(\d{4})$	+1202555$1	63330100 is translated to +12025550100
DallasSitePrefix	Translates numbers with on-net prefix (6) and Dallas site code (444)	^6444(\d{4})$	+1972555$1	64440100 is translated to +19725550100

The following table illustrates a sample dial plan for Redmond, Washington, United States, based on the normalization rules shown in the previous table.

Table 2. Redmond Dial Plan Based on Normalization Rules Shown in Table 1

Redmond.forestFQDN
5digitExtension
7digitcallingRedmond
10digitcallingUS
IntlCallingUS
RedmondSitePrefix
NYSitePrefix
DallasSitePrefix
RedmondOperator

Note:

The normalization rules names shown in the preceding table do not include spaces, but this is a matter of choice. The first name in the table, for example, could have been written "5 digit extension" or "5-digit Extension" and still be valid.

1.3.10.5.6.2 Voice Policies

Voice Policies

Planning for Enterprise Voice > Planning for PSTN Connectivity > Planning Outbound Voice Routing >

Topic Last Modified: *2012-09-21*

Lync Server *voice policies* define the following for each user, site, or organization that is assigned the policy:

- A set of calling features that can be enabled or disabled to determine the Enterprise Voice functionality available to users.
- A set of public switched telephone network (PSTN) usage records that define

what types of calls are authorized.

Planning for Voice Policies

The following steps will help you plan the voice policies that you will need for your Enterprise Voice deployment:

- Determine how you will configure your global voice policy (the default voice policy that is installed with the product). This policy will apply to all Enterprise Voice users who are not explicitly assigned a site-level or per-user policy.
- Identify any site-level voice policies that you might need.
- Identify any per-user voice policies that you might need.
- Decide which call features to enable for each voice policy.
- Determine what PSTN usage records to configure for each voice policy.

Voice Policy Scope

Voice policy scope determines the hierarchical level at which the policy can be applied. In Lync Server, you can configure voice policies with the following scope levels (listed from the most specific to the most general).

- **User voice policy** can be assigned to individual users, groups, or contact objects. This is the lowest level policy. User voice policies can be deployed to enable features for certain users or groups at a site, but not for others in the same site. For example, you may want to disable long distance dialing for some employees. For the purpose of assigning a voice policy, a contact object is treated as an individual user.

  Note:

  We recommend that you deploy a user voice policy for branch site Enterprise Voice users who are registered with the central site deployment, or users who are registered on a Survivable Branch Appliance.

- **Site voice policy** applies to an entire site, except for any users, groups, or contact objects that are assigned a user voice policy. To define a site voice policy, you must specify the site to which the policy applies. If a user voice policy is not assigned, the site voice policy is used.
- **Global voice policy** is the default voice policy that is installed with the product. You can edit the global voice policy to meet the specific needs of your organization, but you cannot rename or delete it. This voice policy applies to all Enterprise Voice users, groups, and contact objects in your deployment unless you configure and assign a voice policy with more specific scope. If you want to disable this policy entirely, be sure that all sites and users have custom policies assigned to them.

Call Features

You can enable or disable the following call features for each voice policy:

- **Call forwarding** enables users to forward calls to other phones and client devices. Enabled by default.
- **Delegation** enables users to specify other users to send and receive calls on their behalf. Enabled by default.
- **Call transfer** enables users to transfer calls to other users. Enabled by default.
- **Call park** enables users to park calls and then pick up the call from a different phone or client. Disabled by default.
- **Simultaneous ringing** enables incoming calls to ring on an additional phone (for example, a mobile phone) or other endpoint devices. Enabled by default.
- **Team call** enables users on a defined team to answer calls for other members of the team. Enabled by default.
- **PSTN reroute** enables calls made by users who are assigned this policy to other enterprise users to be rerouted on the public switched telephone network (PSTN) if the WAN is congested or unavailable. Enabled by default.

- **Bandwidth policy override** enables administrators to override call admission control policy decisions for a particular user. Disabled by default.
- **Malicious call tracing** enables users to report malicious calls by using the Lync client, and then flags such calls in the call detail records. Disabled by default.
- **Voicemail escape** prevents calls from being immediately routed to the user's mobile phone voicemail system when simultaneous ringing is configured and the phone is turned off, out of battery, or out of range, and is based on a timer value. This setting enables and disables the timer and sets the value of the timer. It can be configured only by using the Lync Server Management Shell. Disabled by default.
- **Call forwarding and simultaneous ringing PSTN usages** enables administrators to specify the same PSTN usage as the voice policy for call forwarding and simultaneous ringing, restrict call forwarding and simultaneous ringing to internal Lync users only, or specify a custom PSTN usage that is different from the voice policy's PSTN usage. The default is to use the same PSTN usage as the voice policy for call forwarding and simultaneous ringing.

PSTN Usage Records

Each voice policy should have one or more associated PSTN usage records. PSTN usages can be associated with a voice policy for the purpose of simultaneous ringing and call forwarding only. For details about planning PSTN usage records, see PSTN Usage Records.

Note:

PSTN usage order is critical because in matching users to routes, the outbound routing functionality compares PSTN usages from top to bottom. If the first usage matches the call route, that route is used. If not, the outbound routing functionality looks at the next PSTN usage on the list and continues until a match is found. In effect, the subsequent PSTN usages provide backup if the first one on the list is unavailable.

1.3.10.5.6.3 PSTN Usage Records

PSTN Usage Records

Planning for Enterprise Voice > Planning for PSTN Connectivity > Planning Outbound Voice Routing >

Topic Last Modified: *2012-09-23*

Planning PSTN usage records consists mainly of listing all the call permissions that are currently in force in your organization, from the CEO to temporary workers, consultants, and contingent staff. This process also provides an opportunity to reexamine existing call permissions and revise them. You can create PSTN usage records only for those call permissions that apply to your anticipated Enterprise Voice users, but a better long-range solution might be to create PSTN usage records for all call permissions, regardless of whether some may not currently apply to the group of users to be enabled for Enterprise Voice. If call permissions change or new users with different call permissions are added, you will have already created the required PSTN usage records.

The following table shows a typical PSTN usage table.

PSTN Usage Records

Phone attribute	Description
Local	Local calls
Long-Distance	Long distance calls
International	International calls
Delhi	Delhi full-time employees

Redmond	Redmond full-time employees
RedmondTemps	Redmond temporary employees
Zurich	Zurich full-time employees

By themselves, PSTN usage records do not do anything. For them to work, you must associate them with the following:

- Voice policies, which are assigned to users.
- Routes, which are assigned to phone numbers.

For details about voice policies and routes, see Voice Policies and Voice Routes. For details about how to create and configure them, see Configuring Voice Routes for Outbound Calls.

1.3.10.5.6.4 Voice Routes

Voice Routes

Planning for Enterprise Voice > Planning for PSTN Connectivity > Planning Outbound Voice Routing >

Topic Last Modified: *2012-10-22*

Call routes specify how Lync Server handles outbound calls placed by Enterprise Voice users. When a user dials a number, the Front End Server normalizes the dial string to E.164 format, if necessary, and attempts to match it to a SIP URI. If the server cannot make the match, it applies outgoing call routing logic based on the number. The final step in defining that logic is to create a separate named call route for each set of destination phone numbers that are listed in each dial plan.

Before you define outbound call routes, you should complete the following steps:

- Deploy one or more trunks.
- Create dial plans as needed for sites, individuals, and Contact objects.
- Create public switched telephone network (PSTN) usage records.

Additionally, to enable outbound call routing, you must create and assign one or more voice policies. You can do this either before or after you define outbound call routes.

For each route, you must specify:

- A name by which the route can be easily identified.
- An optional description in cases where the name alone may not be sufficient to describe the route.
- The regular expression matching pattern that identifies the destination phone numbers to which the route is applied, along with exceptions to which the matching pattern is not to be applied.
- One or more trunks that you want to assign to the route.
- The PSTN usage records that users must have in order to call numbers matching the destination phone number regular expression.

You can specify call routes in the Lync Server Control Panel. These call routes populate the server routing table, which Lync Server uses to route calls that are destined for the PSTN.

M:N Trunk Support

Lync Server provides flexibility in how calls are routed to the PSTN. A voice route specifies a set of trunks to the PSTN that can be used for a particular voice call. A trunk associates a Mediation Server and a port number with a PSTN gateway and listening port number. This logical association enables a Mediation Server to be associated with multiple gateways and have multiple connections to the same gateway. When defining a call route, you specify the trunks associated with that route, but you do not specify which Mediation Servers are associated with the route. To create trunks by defining the relationships between Mediation Servers and PSTN gateways, IP-PBXs, and Session Border Controllers (SBCs), use the Topology Builder.

Least-Cost Routing

The ability to specify the trunks to which various numbers are routed enables you to determine which routes incur the lowest costs and implement them accordingly. The general rule in selecting trunks is to choose the trunk with the closest gateway to the location of the destination number in order to minimize long-distance charges. For example, if you are in New York and calling a number in Rome, you would carry the call over the IP network to the trunk with the gateway in your Rome office, thereby incurring a charge only for a local call.

For an example of how least-cost routing might be used, consider the following: Fabrikam decides to enable German users to dial U.S. numbers by using the U.S. trunk. Fabrikam also wants to configure the system so that all calls from U.S. Lync Server users to Germany and adjacent countries/regions terminate on the trunk with the gateway in Germany. This routing will save money, because a call from Germany to Austria, for example, is less expensive than a call from the U.S. to Austria.

Translating Outbound Dial Strings

Lync Server 2013, like its immediate predecessors, requires all dial strings to be normalized to E.164 format for the purpose of performing reverse number lookup (RNL). For trunks with gateways or private branch exchanges (PBXs) that require numbers translated in local dialing formats, Lync Server 2013 enables you to create one or more rules that assist in manipulating the called number (i.e. Request URI) prior to routing it to the trunk. For example, you could write a rule to remove +44 from the head of a dial string and replace it with 0144.

With Lync Server 2013, it is possible to create one or more rules that assist in manipulating the calling number prior to routing it to the trunk.

In planning your trunks that associate gateways:port pairs with Mediation Server:port pairs, it may be useful to group trunks with similar local dialing requirements, and therefore reduce the number of required translation rules and the time it takes to write them.

Configuring Caller ID

Lync Server provides a way to manipulate the caller ID for outbound calls. For example, if an organization wants to mask employees' direct-dial extensions and replace them with the generic corporate or departmental number, an administrator can do that by using Lync Server Control Panel to suppress the caller ID and replace it with a specified alternative caller ID. In planning your routing logic, consider which individuals, groups, sites you'll want this option for—perhaps, even, for all employees.

Note:

For calls that are rerouted over the PSTN, the generic caller ID will be presented instead of the original caller ID. This can cause the call to bypass Do Not Disturb or privacy settings that the callee may have configured.

Additional Routing Logic

In creating outbound call routes, you should be aware of the following factors that can affect routing logic:

- Where a call is established over a federated boundary, the domain portion of the URI is used to route the call over to the enterprise that is responsible for applying the outbound routing logic.
- If the domain portion of the request URI does not contain a supported domain for the enterprise, the outbound routing component on the server does not process the call.
- If a user is not enabled for Enterprise Voice, the server applies other routing logic, as appropriate.
- If a call is routed to a gateway that is fully occupied (all trunk lines are busy), the gateway rejects the call and the outbound routing logic redirects the call to the next-least-cost route. Give this careful consideration, because a gateway sized for a small office overseas (for example, Zurich) may actually carry a significant amount of nonlocal traffic for international calls to Switzerland. If the gateway is not correctly sized for this additional traffic, calls to Switzerland may be routed by way of a gateway in Germany, resulting in larger toll charges.

1.3.10.6 Planning for Exchange Unified Messaging Integration

Planning for Exchange Unified Messaging Integration

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-10-13*

Lync Server 2013 supports integration with Exchange Unified Messaging (UM) for combining voice messaging and email messaging into a single messaging infrastructure. In Microsoft Exchange Server 2007 Service Pack 1 (SP1) and Microsoft Exchange Server 2010, Exchange Unified Messaging (UM) is one of several Exchange server roles that you can install and configure.

In Microsoft Exchange Server 2013, Exchange UM runs as a service on an Exchange Mailbox server. For Lync Server 2013 Enterprise Voice deployments, Unified Messaging combines voice messaging and email messaging into a single store that is available from a telephone (Outlook Voice Access) or a computer. Unified Messaging and Lync Server 2013 work together to provide call answering, Outlook Voice Access, and auto-attendant services to users of Enterprise Voice.

For more information about the architecture changes in Microsoft Exchange Server 2013, see “Voice Architecture Changes” in the Microsoft Exchange Server 2013 documentation at http://go.microsoft.com/fwlink/p/?LinkId=266730.

For these features to be supported in an on-premises Exchange UM deployment, you must be running one of the following:

- Microsoft Exchange Server 2007 Service Pack 1 (SP1) or latest service pack
- Microsoft Exchange Server 2010 or latest service pack
- Microsoft Exchange Server 2013
- Features of Integrated Unified Messaging and Lync Server 2013
- Components and Topologies for On-Premises Unified Messaging
- Guidelines for Integrating On-Premises Unified Messaging and Lync Server 2013
- Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013

Features of Integrated Unified Messaging and Lync Server 2013

Planning > Planning for Enterprise Voice > Planning for Exchange Unified Messaging Integration >

Topic Last Modified: *2012-10-01*

Lync Server 2013, Enterprise Voice uses the Exchange Unified Messaging (UM) infrastructure to provide call answering, call notification, voice access (including voice mail), and auto-attendant services.

Call Answering

Call answering is the receiving of voice messages on behalf of users whose calls are not answered or are busy. It includes playing a personal greeting, recording a message, and submitting the message to be queued for delivery to the user's mailbox, which is stored on the Exchange mailbox server.

If a caller leaves a message, the message is routed to the user's Inbox. If a caller chooses not to leave a message, a missed call notification is stored in the user's mailbox. Users can then access their Inbox by using the Microsoft Outlook messaging and collaboration client, Outlook Web Access, the Exchange ActiveSync technology, or Outlook Voice Access. The subject and priority of calls can be displayed in a way similar to that of email.

Outlook Voice Access

Outlook Voice Access enables an Enterprise Voice user to access not just voice mail, but also the Exchange inbox, including email, calendar, and contacts from a telephony interface. The subscriber access number is assigned by an Exchange UM administrator.

Auto Attendant

Auto attendant is an Exchange UM feature that can be used to configure a phone number that outside users can dial to reach company representatives. In particular, it provides a series of voice prompts that assist an external caller in navigating a menu system. The list of available options is configured on the Exchange UM server by the Exchange UM administrator.

Fax Services

Exchange UM includes fax features, which enable users to receive incoming faxes in their Exchange mailboxes. For details, see "Unified Messaging" in the Microsoft Exchange Server documentation at http://go.microsoft.com/fwlink/p/?linkId=135652.

Note:

Fax services provided by the Exchange UM server are not available in Lync Server deployments that are integrated with Microsoft Exchange Server 2010, Exchange 2010 with the latest service pack, or Exchange 2013.

Components and Topologies for On-Premises Unified Messaging

Server Software and Infrastructure Support > Voice Support > Exchange Unified Messaging (UM) Support >

Topic Last Modified: *2012-09-25*

This topic describes the Microsoft Exchange Server 2013 components required to provide Exchange Unified Messaging (UM) features to Lync Server 2013 deployment. It also describes the supported topologies for on-premises Exchange UM integration.

Exchange Server Components

To provide the Exchange UM features and services described in Features of Integrated Unified Messaging and Lync Server 2013 to Enterprise Voice users in your organization, you must deploy an Microsoft Exchange Mailbox server and Client Access server, which hosts user mailboxes and provides a single storage location for email and voice mail. Exchange UM runs as a service on Exchange Mailbox and Client Access servers.

For details about Exchange UM components in Microsoft Exchange Server 2007 and Microsoft Exchange Server 2010, see Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail in the Deployment documentation.

Supported Topologies

You can deploy Lync Server 2013 and Exchange Unified Messaging (UM) in the same forest or multiple forests. If the deployment spans multiple forests, you must perform the Exchange integration steps for each Exchange UM forest. Furthermore, you must configure each Microsoft Exchange forest to trust the Lync Server 2013 forest and the Lync Server 2013 forest to trust each Exchange UM forest. In addition to this forest trust, the Exchange UM settings for all users must be set on the user objects in the Lync Server 2013 forest.

Lync Server 2013 supports the following topologies for Exchange UM integration:

- Single forest
- Single domain (that is, a single forest with a single domain). Lync Server 2013, Microsoft Exchange, and users all reside in the same domain.
- Multiple domain (that is, a root domain with one or more child domains). Lync Server 2013, and Microsoft Exchange servers are deployed in different domains from the domain where you create users. Exchange UM servers can be deployed in different domains from the Lync Server 2013 pool they support.
- Multiple forest (that is, resource forest). Lync Server 2013 is deployed in a single forest, and then users are distributed across multiple forests. The users' Exchange UM attributes must be replicated over to the Lync Server 2013 forest.

Note:

Exchange can be deployed in multiple forests. Each Exchange organization can provide Exchange UM to its users, or Exchange UM can be deployed in the same forest as Lync Server 2013.

Guidelines for Integrating On-Premises Unified Messaging and Lync Server 2013

See Also

Planning > Planning for Enterprise Voice > Planning for Exchange Unified Messaging Integration >

Topic Last Modified: *2012-09-25*

The following are guidelines and best practices to consider when you deploy Enterprise Voice:

◆**Important:**
Exchange Unified Messaging (UM) supports IPv6 only if you are also using UCMA 4.

- Deploy a Lync Server 2013 Standard Edition server or a Front End pool. For details about installation, see Deploying Lync Server 2013 in the Deployment documentation.
- Work with Exchange administrators to confirm which tasks each of you will perform to assure a smooth and successful integration.
- Deploy the Exchange Mailbox server roles in each Exchange Unified Messaging (UM) forest where you want to enable users for Exchange UM. For details about installing Exchange server roles, see the Microsoft Exchange Server 2013 documentation.

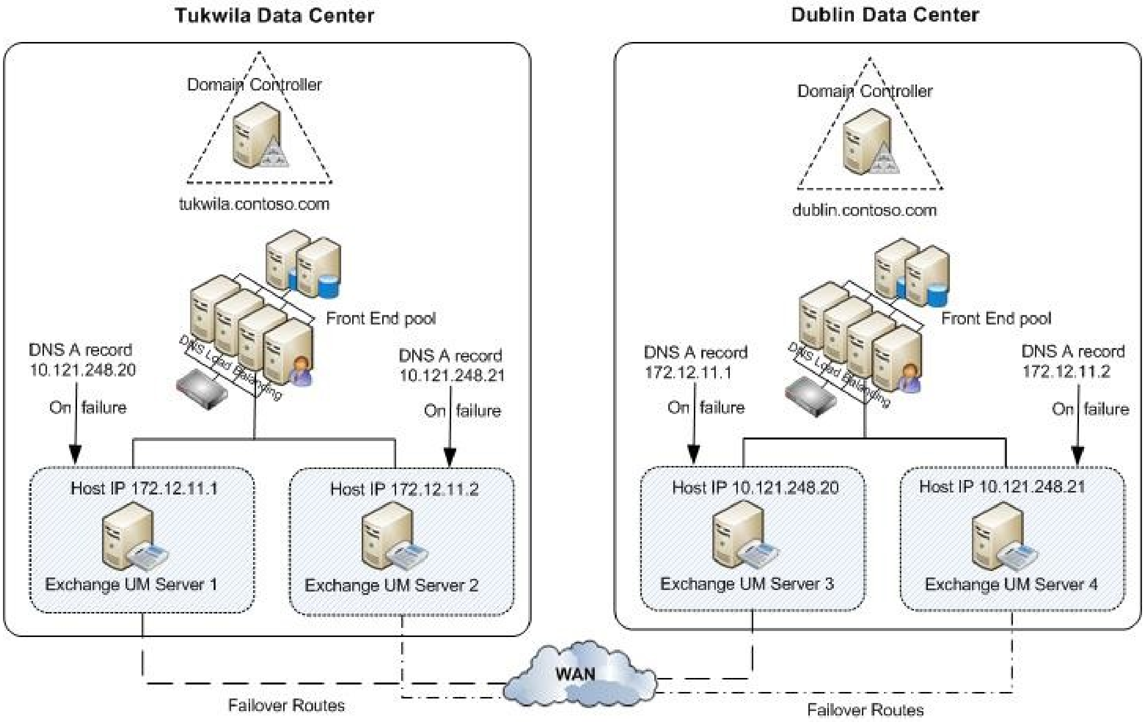
◆**Important:**
When Exchange Unified Messaging (UM) is installed, it is configured to use a self-signed certificate. The self-signed certificate, however, does not enable Lync Server 2013 and Exchange UM to trust each other, which is why it is necessary to request a separate certificate from a certification authority that both servers trust.

- If Lync Server 2013 and Exchange UM are installed in different forests, configure each Exchange forest to trust the Lync Server 2013 forest and the Lync Server 2013 forest to trust each Exchange forest. Also, set the users' Exchange UM settings on the user objects in the Lync Server 2013 forest, typically by using a script or a cross-forest tool, such as Identity Lifecycle Manager (ILM).
- If necessary, install the Exchange Management Console to manage your Unified Messaging servers.
- Obtain valid phone numbers for Outlook Voice Access and auto attendant.
- If you are using a version of Exchange UM earlier than Microsoft Exchange Server 2010 Service Pack 1 (SP1), coordinate names for Exchange UM SIP URI dial plans and Enterprise Voice dial plans.

Deploying Redundant Exchange UM Servers

◆**Important:**
We recommend that you deploy a minimum of two servers on which Exchange UM services is running for each Exchange UM SIP URI dial plan that you configure for your organization. In addition to providing expanded capacity, deploying redundant servers provides high availability. In the event of an server failure, Lync Server 2013 can be configured to fail over to another server.

The following example configurations provide Exchange UM resiliency.

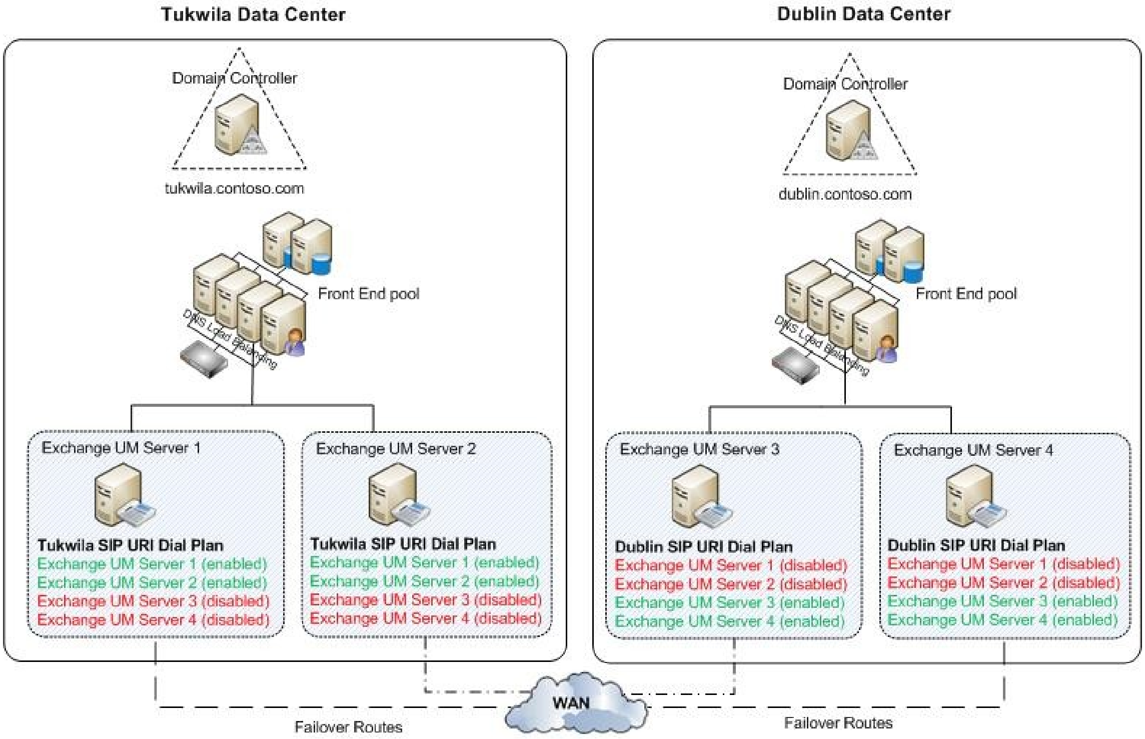


In Example 1, Exchange UM servers 1 and 2 are enabled in the Tukwila data center, and Exchange UM servers 3 and 4 are enabled in the Dublin data center. In the event of an Exchange UM outage in Tukwila, the Domain Name System (DNS) A records for servers 1 and 2 should be configured to point to servers 3 and 4, respectively. In the event of an Exchange UM outage in Dublin, the DNS A records for servers 3 and 4 should be configured to point to servers 1 and 2, respectively.

Note:

For Example 1, you should also assign one of following certificate on each Exchange UM server:

- Use a certificate with a wildcard in the Subject Alternative Name (SAN).
- Put the fully qualified domain name (FQDN) of each of the four Exchange UM servers in the SAN.


Tukwila Data Center
Domain Controller
tukwila.contoso.com
Front End pool
DNS Load Balancing
Exchange UM Server 1
Tukwila SIP URI Dial Plan
Exchange UM Server 1 (enabled)
Exchange UM Server 2 (enabled)
Exchange UM Server 3 (disabled)
Exchange UM Server 4 (disabled)
Exchange UM Server 2
Tukwila SIP URI Dial Plan
Exchange UM Server 1 (enabled)
Exchange UM Server 2 (enabled)
Exchange UM Server 3 (disabled)
Exchange UM Server 4 (disabled)
Dublin Data Center
Domain Controller
dublin.contoso.com
Front End pool
DNS Load Balancing
Exchange UM Server 3
Dublin SIP URI Dial Plan
Exchange UM Server 1 (disabled)
Exchange UM Server 2 (disabled)
Exchange UM Server 3 (enabled)
Exchange UM Server 4 (enabled)
Exchange UM Server 4
Dublin SIP URI Dial Plan
Exchange UM Server 1 (disabled)
Exchange UM Server 2 (disabled)
Exchange UM Server 3 (enabled)
Exchange UM Server 4 (enabled)
WAN
Failover Routes
Failover Routes

In Example 2, under ordinary operating conditions Exchange UM servers 1 and 2 are enabled in the Tukwila data center, and Exchange UM servers 3 and 4 are enabled in the Dublin data center. All four servers are included in the Tukwila users' SIP URI dial plan; however, servers 3 and 4 are disabled. In the event of an Exchange UM outage in Tukwila, for example, Exchange UM servers 1 and 2 should be disabled and Exchange UM servers 3 and 4 should be enabled so the Tukwila Exchange UM traffic will be routed to the servers in Dublin.

For details about how to enable or disable Unified Messaging on Exchange 2013, see “Integrate Exchange 2013 UM with Lync Server” at http://go.microsoft.com/fwlink/p/?LinkId=265372.

For details about how to enable or disable Unified Messaging on Microsoft Exchange Server 2010, see:

- "Enable Unified Messaging on Exchange 2010" at http://go.microsoft.com/fwlink/p/?LinkId=204418.
- "Disable Unified Messaging on Exchange 2010" at http://go.microsoft.com/fwlink/p/?LinkId=204416.

See Also

Concepts

Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013

1.3.10.6.4 Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013

Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013

Planning > Planning for Enterprise Voice > Planning for Exchange Unified Messaging Integration >

Topic Last Modified: *2012-12-17*

If you want to integrate Exchange Unified Messaging (UM) with Lync Server 2013, you must perform the tasks described in this topic. Also be sure that you review the planning and deployment best practices described in Guidelines for Integrating On-Premises Unified Messaging and Lync Server 2013. This topic assumes that you have deployed Lync Server 2013 with a collocated Mediation Server and that you have enabled users for Lync Server 2013, but not necessarily that you have performed all deployment and configuration steps to enable Enterprise Voice, as described in Deploying Enterprise Voice in the Deployment documentation.

Unified Messaging Integration Process

◆**Important:**
It is important that you coordinate with your organization's Exchange administrators to confirm the tasks that each of you will perform to help ensure a smooth, successful integration.

Phase	**Steps**	**Required groups and roles**	**Deployment documentation**
Deploy one of the following: - Microsoft Exchange Server 2007 Service Pack 1 (SP2) or latest service pack - Microsoft Exchange Server 2010 or latest service pack - Microsoft Exchange Server 2013	If you are using Microsoft Exchange Server 2013, install the following Exchange Server roles in either the same forest or a different forest as Lync Server 2013: - Client Access - Mailbox If Microsoft Exchange Server 2013 and Exchange Unified Messaging (UM) are installed in different forests, configure each Exchange forest to trust the Lync Server 2013 forest. If you are using Exchange 2010, install the following Exchange Server roles in either the same forest or a different forest as Lync Server 2013: - Unified Messaging - Hub Transport - Client Access - Mailbox If Lync Server 2013 and Exchange Unified	Enterprise administrators (if this is the first Exchange Server in the organization) -OR- Exchange Organization administrator (if this is not the first Exchange Server in the organization)	See the appropriate documentation for your version of Exchange Server: - Exchange Server 2007 deployment documentation at http://go.microsoft.com/fwlink/p/?LinkId=268694. - Exchange Server 2010 or latest service pack deployment documentation at http://go.microsoft.com/fwlink/p/?LinkId=268695. - Microsoft Exchange Server 2013 Planning and Deployment at http://go.microsoft.com/fwlink/p/?LinkId=266569.

	Messaging (UM) are installed in different forests, configure each Exchange forest to trust the Lync Server 2013 forest.		
Install certificates.	Download and install certificates for each Exchange UM server from a trusted root certificate authority (CA). The certificates are required for mutual Transport Level Security (MTLS) between the servers running Exchange UM and Lync Server 2013.	Administrators	Configure Certificates on the Server Running Microsoft Exchange Server Unified Messaging
Create and configure a new Exchange UM SIP dial plan.	On the Exchange UM server, create a SIP dial plan based on your organization’s specific deployment requirements.	Exchange Organization administrator	For Exchange 2007 SP1 or latest service pack, see "How to Create a Unified Messaging SIP URI Dial Plan" at http://go.microsoft.com/fwlink/p/?linkId=268632. For Exchange 2010 or latest service pack, see "Create a UM Dial Plan" at http://go.microsoft.com/fwlink/p/?linkId=268674. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.
Configure security settings for the Exchange UM SIP dial plan.	To encrypt Enterprise Voice traffic, configure the security settings on the Exchange UM SIP dial plan as **SIP Secured** or **Secured**. This is an especially important step if you have deployed or plan to deploy Lync Phone Edition devices in your environment. For Lync Phone Edition devices to function in an environment with Exchange UM integration, Lync Server encryption settings must	Exchange Organization administrator	Configure Unified Messaging on Microsoft Exchange For Exchange 2007 SP1 or latest service pack, see also: "How to Configure Security on a Unified Messaging Dial Plan" at http://go.microsoft.com/fwlink/p/?LinkId=268696. For Exchange 2010 or latest service pack, see also:

	align with the Exchange UM dial plan security settings. For details, refer to the Deployment documentation.		"Configure VoIP Security on a UM Dial Plan" http://go.microsoft.com/fwlink/p/?LinkId=268697. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.
Add Unified Messaging servers to the Exchange UM SIP dial plan.	To enable a newly installed Unified Messaging server to answer and process incoming calls, you must add the Unified Messaging server to a UM dial plan. In this case, add the server to the Exchange UM SIP dial plan.	Administrators Exchange Server administrators	For Exchange 2007 SP1 or latest service pack, see "How to Add Unified Messaging Server to a Dial Plan" at http://go.microsoft.com/fwlink/p/?linkId=268681. For Exchange 2010 or latest service pack, see "View or Configure the Properties of a UM Server" at http://go.microsoft.com/fwlink/p/?linkId=268682. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.
Configure mailboxes with SIP addresses.	Assign SIP addresses to the mailboxes of Enterprise Voice users who will be using Exchange UM features.	Lync Server 2013 administrator Exchange Recipient administrator	For Exchange 2007 SP1 or latest service pack, see "How to Add, Remove, or Modify a SIP Address for a UM-Enabled User" at http://go.microsoft.com/fwlink/p/?LinkId=268698. For Exchange 2010 or latest service pack, see "Modify a SIP Address for a UM-Enabled User" at http://go.microsoft.com/fwlink/p/?LinkId=268699. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.
Run the exchucutil.ps1	On the server running Exchange UM services,	Exchange Organization	Configure Unified

script.	open the Exchange Management Shell and run the exchucutil.ps1 script, which does the following: • Grants Lync Server 2013 permission to read Exchange UM Active Directory Domain Services (AD DS) objects, specifically, the SIP dial plans created in the previous task. • Creates a Unified Messaging IP gateway object in Active Directory for each Lync Server 2013 Enterprise Edition pool or Standard Edition server that hosts users who are enabled for Enterprise Voice. • Creates an Exchange UM hunt group for each gateway. The hunt group pilot identifier will be the name of the dial plan that is associated with the corresponding gateway. These need to be mapped 1:1 if there is more than one dial plan.	administrator Exchange Recipient administrator	Messaging on Microsoft Exchange

Configure Lync Server 2013 dial plans.	If you are integrating with Exchange 2007 SP1 or latest service pack, or Exchange 2010, create a new Enterprise Voice dial plan with a name that matches the Exchange UM dial plan fully qualified domain name (FQDN). **Note:** You will need to do this for each UM Dial plan. If you are integrating with Exchange 2010 SP1, ensure that suitable global/site-level or pool-level Enterprise Voice dial plans have been configured. **Note:** If you are integrating with Exchange 2010 SP1, the Lync Server dial plan and Exchange UM SIP dial plan names do not need to match.	RTCUniversalServerAdmins	Configuring Dial Plans
Run the Exchange UM Integration tool.	On the Lync Server 2013, run **ocsumutil.exe**, which: • Creates Subscriber Access and Auto Attendant contact objects. • Validates that there is an Enterprise Voice dial plan with a name that matches the Exchange UM dial plan FQDN. If you are running Exchange 2010 SP1 or later, the dial plan names do not need to match, and you can ignore the	RTCUniversalServerAdmins *and* RTCUniversalUserAdmins **Important:** To run ocsumutil.exe successfully, the user must belong to both of these groups. **Note:** To create Contact objects, the user who runs ocsumutil.exe must have the correct permission to the Active Directory	Configure Lync Server 2013 to Work with Unified Messaging on Microsoft Exchange Server

	tool's warning about this. This tool works by scanning the Active Directory for Exchange UM settings and allowing the Lync Server 2013 administrator to view, create, and edit contact objects.	organizational unit (OU) where the new contact objects are stored. This permission can be granted by running the **Grant-CsOUPermission** cmdlet. For details, see the Lync Server Management Shell documentation.	
If necessary, perform other Enterprise Voice configuration steps.	If you have not already configured Enterprise Voice settings on your servers or users, do one or more of the following: • Deploy and configure Public switched telephone network (PSTN) gateways and Mediation Servers • Define voice policies, PSTN usage records, and outbound call routes. • Enable users for Enterprise Voice. • Optionally, configure specific users with dial plans. Other configuration steps may be required depending on the Enterprise Voice features that you enable.	RTCUniversalServerAdmins RTCUniversalUserAdmins	See topics in the following sections: • Configuring Voice Policies, PSTN Usage Records, and Voice Routes • Deploying Enterprise Voice

Enable Enterprise Voice users for Exchange UM.	On the Exchange UM server, ensure that a Unified Messaging mailbox policy has been created and that each user has a unique extension number assignment, and then enable the user for Unified Messaging.	Exchange Recipient administrato r	For Exchange 2007 SP1 or latest service pack, see "How to Enable a User for Unified Messaging" at http://go.microsoft.com/fwlink/p/?LinkId=268700. For Exchange 2010 or latest service pack, see "Enable a User for Unified Messaging" at http://go.microsoft.com/fwlink/p/?LinkId=268701. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.

1.3.10.7 Hosted Exchange Unified Messaging Integration

Hosted Exchange Unified Messaging Integration

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-09-20*

In addition to the support that previous Lync Server 2013 releases have provided for integration with *on-premises* deployments of Exchange Unified Messaging (UM), Lync Server 2013 introduces support for integration with *hosted* Exchange UM. Hosted Exchange UM enables Lync Server 2013 to provide voice messaging to your users if you transfer some or all of them to a hosted Exchange service provider such as Microsoft Exchange Online.

Lync Server 2013 Enterprise Voice uses the Exchange UM infrastructure to provide call answering, call notification, voice access (including voice mail), and auto attendant services. For details, see Features of Integrated Unified Messaging and Lync Server 2013.

- Hosted Exchange UM Architecture and Routing
- Hosted Voice Mail Policies
- Hosted Exchange User Management
- Hosted Exchange Contact Object Management
- Deployment Process for Integrating Hosted Exchange UM with Lync Server 2013

1.3.10.7.1 Hosted Exchange UM Architecture and Routing

Hosted Exchange UM Architecture and Routing

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-03-26*

This section provides an overview of the architecture for on-premises and hosted

Exchange UM integration, including supported modes, shared SIP space, and routing considerations.

- Hosted Exchange UM Integration Architecture
- Hosted Exchange UM Routing

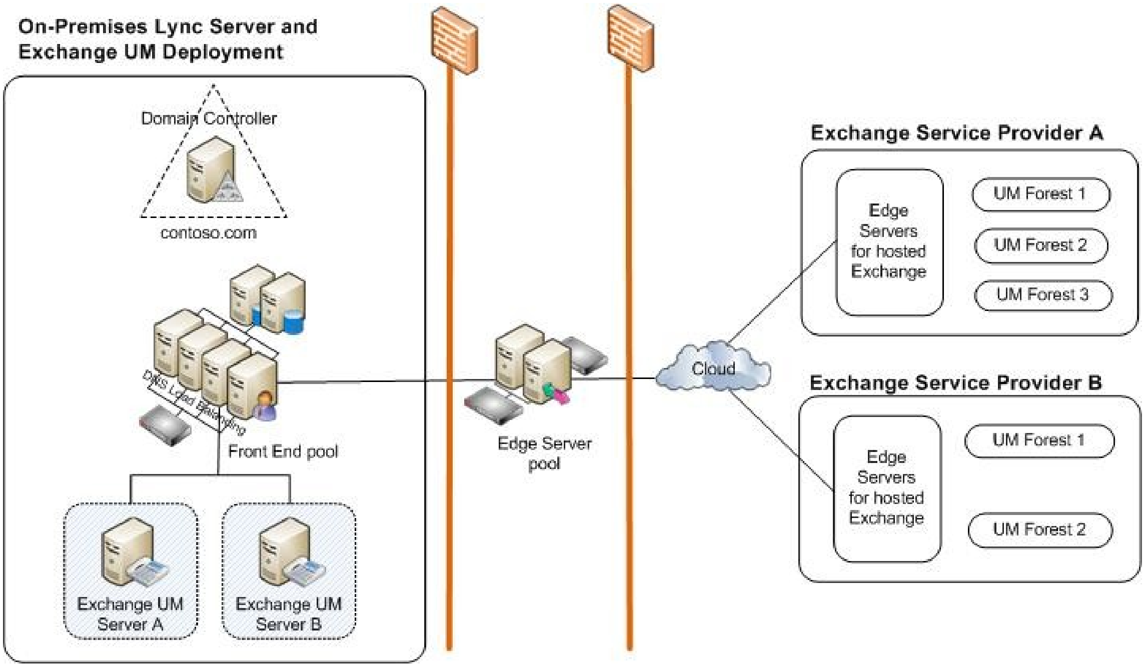
1.3.10.7.1.1 Hosted Exchange UM Integration Architecture

Hosted Exchange UM Integration Architecture

Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration > Hosted Exchange UM Architecture and Routing >

Topic Last Modified: *2012-09-25*

The Lync Server 2013 ExUM Routing application supports integration with an on-premises Exchange Unified Messaging (UM) deployment, with Exchange UM hosted by a service provider, or with a combination of the two. The following diagram shows all three possibilities.



The following modes are supported:

- **On-premises deployment:** Lync Server 2013 and Exchange UM are both deployed on local servers within your enterprise.
- **Cross-premises deployment:** Lync Server 2013 is deployed on local servers within your enterprise and Exchange UM is hosted in an online service provider’s facility, such as a Microsoft Exchange Online data center.
- **Mixed deployment:** Your Lync Server 2013 deployment has some user mailboxes homed on local Exchange servers within your enterprise and some mailboxes homed in a hosted Exchange service data center.

> **Note:**
> The mixed deployment can be used as a transitional solution during evaluation and phased migration of users to hosted Exchange UM, or a permanent solution if you opt to keep some users’ Exchange UM services on-

premises after transferring others.

Shared SIP Address Space

To integrate Lync Server 2013 with an on-premises Exchange UM deployment, you grant Lync Server 2013 permission to read Exchange UM Active Directory Domain Services objects. This approach does not work for integration with hosted Exchange UM, however, because Lync Server 2013 and Exchange UM are installed in separate forests with no trust between them.

To integrate Lync Server 2013 with hosted Exchange UM, you must configure a *shared SIP address space*. In this configuration, the same SIP domain address space is available to both Lync Server 2013 and the hosted Exchange UM service provider.

Note:

Use of the shared SIP address space is similar to the approach used in a cross-premises Lync Server 2013 environment, in which some users are homed in the on-premises deployment and some are homed in a hosted deployment (such as Lync Online). The SIP domain is split between them. When you integrate Lync Server 2013 with hosted Exchange UM, ensure that you include the Exchange UM service provider in the shared SIP address space.

To configure the shared SIP address space for integrating with an Exchange UM service provider, you need to configure your Edge Server as follows:

1. Configure the Edge Server for federation by running the **Set-CsAccessEdgeConfiguration** cmdlet to set the following parameters:
   - **UseDnsSrvRouting** specifies that Edge Servers will rely on DNS SRV records when sending and receiving federation requests.
   - **AllowFederatedUsers** specifies whether internal users are allowed to communicate with users from federated domains. This property also determines whether internal users can communicate with users in a split domain scenario.
   - **EnablePartnerDiscovery** specifies whether Lync Server 2013 will use DNS records to try to discover partner domains that are not listed in the Active Directory allowed domains list. If False, Lync Server 2013 will federate only with domains that are found on the allowed domains list. This parameter is required if you use DNS service routing. In most deployments, the value is set to false to avoid opening up federation to all partners.
2. Replicate the Central Management store to the Edge Server and verify the replication. For details, see Export Your Topology and Copy It to External Media for Edge Installation in the Deployment documentation.
3. Configure a *hosting provider* on the Edge Server by running the **New-CsHostingProvider** cmdlet to set the following parameters:
   - **Identity** specifies a unique string value identifier for the hosting provider that you are creating, for example, **Hosted Exchange UM**.
   - **Enabled** indicates whether the network connection between your domain and the hosting provider is enabled. Must be set to **True**.
   - **EnabledSharedAddressSpace** indicates whether the hosting provider will be used in a shared SIP address space scenario. Must be set to **True**.
   - **HostsOCSUsers** indicates whether the hosting provider is used to host Lync Server 2013 accounts. Must be set to **False**.
   - **ProxyFQDN** specifies the fully qualified domain name (FQDN) for the proxy server used by the hosting provider, for example, **proxyserver.fabrikam.com**. Contact your hosting provider for this information. This value cannot be modified. If the hosting provider changes its proxy server, you will need to delete and then recreate the entry for that provider.
   - **IsLocal** indicates whether the proxy server used by the hosting provider is contained within your Lync Server 2013 topology. Must be set to **False**.

1.3.10.7.1.2 Hosted Exchange UM Routing

Hosted Exchange UM Routing

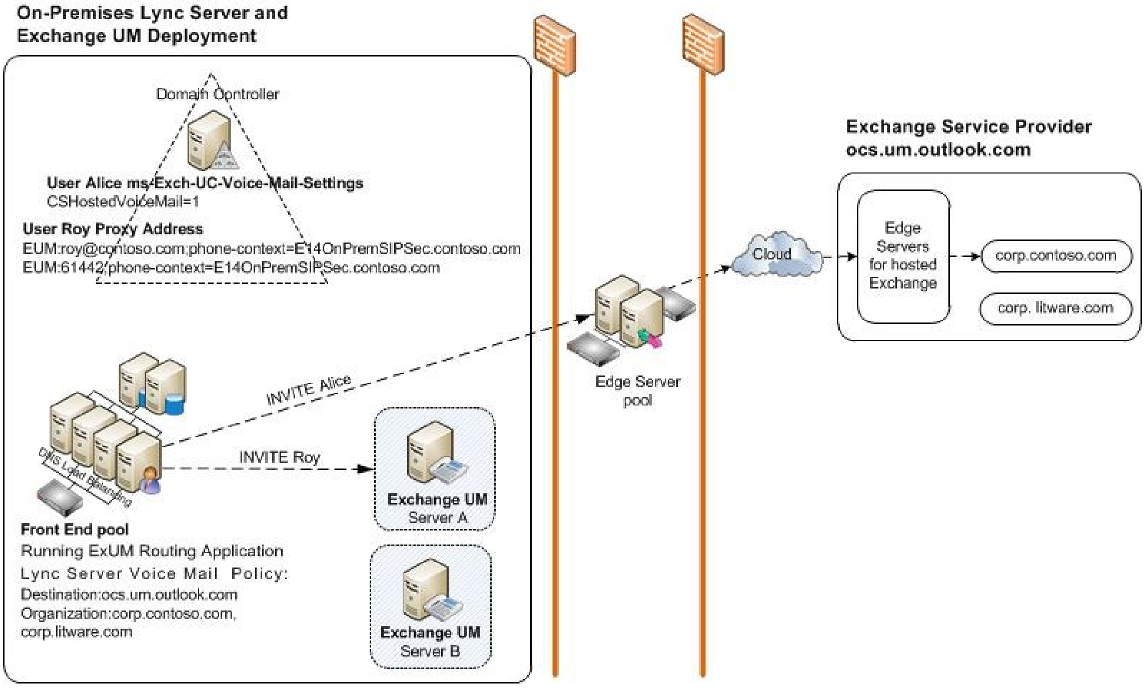
Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration > Hosted Exchange UM Architecture and Routing >

Topic Last Modified: *2012-10-01*

The Exchange UM Routing application runs on the Front End Server to route calls, either to an on-premises Microsoft Exchange Server Unified Messaging (UM) deployment or to hosted Exchange UM service.

The ExUM Routing Application

The Lync Server 2013 Exchange UM Routing application uses information from user account settings and from hosted voice mail policy parameters to determine how to route calls for hosted voice messaging, as shown in the following diagram.


On-Premises Lync Server and
Exchange UM Deployment
Domain Controller
User Alice ms-Exch-UC-Voice-Mail-Settings
CSHostedVoiceMail=1
User Roy Proxy Address
EUM:roy@contoso.com;phone-context=E14OnPremSIPSec.contoso.com
EUM:61442;phone-context=E14OnPremSIPSec.contoso.com
INVITE Alice
INVITE Roy
DNS Load Balancing
Front End pool
Running ExUM Routing Application
Lync Server Voice Mail Policy:
Destination:ocs.um.outlook.com
Organization:corp.contoso.com,
corp.litware.com
Exchange UM
Server A
Exchange UM
Server B
Edge Server
pool
Cloud
Exchange Service Provider
ocs.um.outlook.com
Edge
Servers
for hosted
Exchange
corp.contoso.com
corp. litware.com

Exchange UM routing can be configured to route calls to users who are enabled for on-premises Exchange UM, to users who are enabled for hosted Exchange UM, or to a combination of the two.

For example, suppose that Roy’s mailbox and Exchange UM service are homed in an on-premises Exchange deployment.

- The proxy address information from Roy’s user account provides the information that the ExUM Routing application uses to route his calls to an on-premises Exchange UM server.

Alice’s mailbox and Exchange UM service are located at a hosted Exchange service provider’s data center. Routing for her Exchange UM calls is configured as follows:

- The values set in the msExchUCVoiceMailSettings attribute of Alice’s user account tell the ExUM Routing application to check for routing details in a hosted voice mail policy.

Note:
The value of the msExchUCVoiceMailSettings attribute can be set by either the Exchange service provider or the Lync Server 2013 administrator. In the example shown in the preceding diagram, the value (CsHostedVoiceMail=1) was set by the Lync Server 2013 administrator to enable hosted voice mail for Alice. For details about this attribute, see Hosted Exchange User Management.

- The hosted voice mail policy that is assigned to Alice's user account provides routing details:
  - Destination is the hosted Exchange UM service provider (ls.ExUm.<*hostedExchangeServer*>.com in this example).
  - Organizations are identified by the tenant IDs, which are the routing FQDNs for SIP messages for Exchange Server tenants that are located on ls.ExUm.<*hostedExchangeServer*>.com (corp.contoso.com and corp.litwareinc.com in this example).

  Note:
  The FQDN for Exchange Online is exap.um.outlook.com.

  For details, see Hosted Voice Mail Policies.

Note:
If both the msExchUCVoiceMailSettings attribute and the UM proxy address settings are present in a user account, the msExchUCVoiceMailSettings attribute takes precedence.

1.3.10.7.2 Hosted Voice Mail Policies

Hosted Voice Mail Policies

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-10-01*

A *hosted voice mail policy* provides information to the Lync Server 2013 ExUM Routing application about where to route calls for users whose mailboxes are located on a hosted Exchange service.

Note:
Hosted voice mail policies are required only for Lync Server 2013 integration with hosted Exchange UM. They are not needed for integration with on-premises Exchange UM.

Hosted Voice Mail Policy Scope

Hosted voice mail policy scope determines the hierarchical level at which the policy applies. You can configure hosted voice mail policies with the following scope levels:

- The *global* policy can potentially affect all users in the Lync Server 2013 deployment. If a user is enabled for hosted Exchange UM access and has not been assigned a per-user policy, and if a site policy has not been assigned to the user's site, the global policy applies. The global policy is installed with Lync Server 2013. You can modify it to meet your needs, but you cannot rename or delete it.
- A *site* policy can affect all users that are homed on the site for which the policy is defined. If a user is configured for hosted Exchange UM access and has not been assigned a per-user policy, the site policy applies.
- A *per-user* policy can affect only individual users or groups. To enforce a per-user policy, you must explicitly assign the policy to individual users, groups, and contact objects.

Note:

In most cases, only one hosted voice mail policy is required. You can often modify the global policy to meet all your needs. If you deploy multiple hosted voice mail policies, all such policies have per-user scope.

Hosted Voice Mail Policy Attributes

A voice mail policy defines two attributes that the Lync Server 2013 ExUM Routing application inserts in the request URI of an INVITE message that is sent to the hosted Exchange UM implementation:

- **Destination:** The fully qualified domain name (FQDN) of the hosted Exchange UM service. This value is used by the on-premises Lync Server Edge Server for routing purposes.

  Note:

  The FQDN for Exchange Online is exap.um.outlook.com.

- **Organization:** The FQDN of the tenant on the hosted Exchange UM service that homes your Lync Server 2013 users' mailboxes. A voice mail policy can contain multiple organizations. If more than one organization is included in the policy, this attribute must be a comma-separated list of the Exchange Server tenants that home your Lync Server 2013 user mailboxes.

Note:

The tenant administrator of your hosted Exchange UM service will provide the necessary values for your Destination and Organization attribute settings. To configure your policy, you must run the New-CsHostedVoicemailPolicy cmdlet or use the Set-CsHostedVoicemailPolicy cmdlet to modify one that exists (for example, the global policy).

For details about managing hosted voice mail policies, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsHostedVoicemailPolicy
- Set-CsHostedVoicemailPolicy
- Get-CsHostedVoicemailPolicy

Per-User Voice Mail Policy Assignment

If your hosted voice mail policy is defined with per-user scope, you must explicitly assign it. You can run the Grant-CsHostedVoicemailPolicy cmdlet to assign the policy to individual users or groups.

For details about assigning or removing a per-user hosted voice mail policy, see the Lync Server Management Shell documentation for the following cmdlets:

- Grant-CsHostedVoicemailPolicy
- Remove-CsHostedVoicemailPolicy

1.3.10.7.3 Hosted Exchange User Management

Hosted Exchange User Management

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-10-18*

To provide voice mail services for Lync Server 2013 users whose mailboxes are located on a hosted Exchange service, you must enable their user accounts for hosted voice mail.

Note:

Before a Lync Server 2013 user can be enabled for hosted voice mail, a hosted voice mail policy that applies to the corresponding user account must be deployed. The policy can be global, site, or per-user in scope, as long as it applies to the user whom you want to enable. For details, see Hosted Voice Mail Policies.

The msExchUCVoiceMailSettings Attribute

Lync Server 2013 introduces a new user attribute named **msExchUCVoiceMailSettings**, which is created as part of the Lync Server 2013 Active Directory schema preparation. This multivalued attribute holds voice mail settings that are shared by Lync Server 2013 and the hosted Exchange service.

The hosted Exchange service may in some cases set the value of the msExchUCVoiceMailSettings attribute in the process of enabling Exchange UM, or during the process of transferring mailboxes to a hosted Exchange Server. If this attribute is not set by Exchange, the Lync Server 2013 administrator must set it by running the Set-CsUser cmdlet, as described earlier in this topic.

The attribute's key/value pairs and their authors are shown in the following table.

The msExchUCVoiceMailSettings Attribute Key/Value Pairs

Value	Author	Meaning
ExchangeHostedVoiceMail=1	Exchange	User has been enabled for hosted UM access by Exchange Server. The Exchange UM Routing application will check the user's hosted voice mail policy for routing details.
ExchangeHostedVoiceMail=0	Exchange	User has been disabled for hosted UM access by Exchange Server.
CsHostedVoiceMail=1	Lync Server	User has been enabled for hosted UM access by Lync Server 2013. The Lync Server 2013 ExUM Routing application will check the user's hosted voice mail policy for routing details.
CsHostedVoiceMail=0	Lync Server	User has been disabled for hosted UM access by Lync Server 2013.

Note:

If the attribute already has values other than one of the Lync Server 2013 key/value pairs (CSHostedVoiceMail=0 or CSHostedVoiceMail=1), a warning will indicate that the attribute may be managed by a different application. For example, a warning is displayed if the key/value pair ExchangeHostedVoiceMail=0 or ExchangeHostedVoiceMail=1 is already present. In that case, you can change the value by editing it the Active Directory, or run the following cmdlet to set the value to null:

```
Set-CsUser –identity user –HostedVoicemail $null
```

Enabling Users for Hosted Voice Mail

To enable a user's voice mail calls to be routed to hosted Exchange UM, you must run the Set-CsUser cmdlet to set the value of the *HostedVoiceMail* parameter. This parameter also signals Lync Server 2013 to light up the “call voice mail” indicator.

- The following example enables Pilar Ackerman’s user account for hosted voice mail:

  ```
  Set-CsUser -Identity "Pilar Ackerman" -HostedVoiceMail $True
  ```

  The cmdlet verifies that a hosted voice mail policy (global, site-level or per-user) applies to this user. If no policy applies, the cmdlet fails.
- The following example disables Pilar Ackerman’s user account for hosted voice mail:

  ```
  Set-CsUser -Identity "Pilar Ackerman" -HostedVoiceMail $False
  ```

  The cmdlet verifies that no hosted voice mail policy (global, site-level or per-user) applies to this user. If a policy does apply, the cmdlet fails.

For details about using the Set-CsUser cmdlet, see the Lync Server Management Shell documentation.

1.3.10.7.4 Hosted Exchange Contact Object Management

Hosted Exchange Contact Object Management

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-09-25*

You need to configure a Contact object for each auto-attendant number and subscriber access number in your cross-premises deployment.

For integration with hosted Exchange UM, ocsumutil.exe cannot be used to manage Contact objects, because it depends on Active Directory Exchange UM settings. In a cross-premises deployment, Lync Server 2013 and hosted Exchange UM are installed in separate forests with no trust between them. For security reasons, Lync Server 2013 administrators have no direct access to Exchange UM Active Directory settings. As a result, Lync Server 2013 provides a different model for managing Contact objects in a *shared SIP address space* that is accessible to both Lync Server 2013 and the hosted Exchange UM service.

Hosted Contact Object Workflow

The following are the general steps for working with your hosted Exchange tenant administrator to manage contact objects:

1. The Exchange administrator requests phone numbers for the Exchange UM subscriber access and auto-attendant Contact objects.
2. The Lync Server 2013 administrator creates a Contact object for each phone number and assigns a hosted voice mail policy to each Contact object.
3. The Lync Server 2013 administrator provides the phone numbers to the Exchange administrator.
4. The Exchange administrator assigns the phone numbers to appropriate Exchange UM dial plans for auto attendants and subscriber access.

Note:

There is no need to configure any Lync Server 2013 dial plan settings on the Contact objects as there is with on-premises deployments.

Configuring Hosted Contact Objects

Note:

Before Lync Server 2013 Contact objects can be enabled for hosted Exchange UM, a hosted voice mail policy that applies to them must be deployed. The policy can be of global, site-level, or per-user scope, as long as it applies to the contact object you want to enable. For details, see Hosted Voice Mail Policies.

To configure hosted auto-attendant and subscriber access Contact objects in a cross-premises deployment, you must use the following cmdlets:

- **New-CsExUmContact** creates a new Contact object for hosted UM.
- **Set-CsExUmContact** modifies an existing Contact object for hosted Exchange UM.

The following example creates an auto-attendant Contact object:

```
New-CsExUmContact -SipAddress sip:exumaa1@fabrikam.com -RegistrarPool RedmondPool
```

This example creates a new Exchange UM Contact object with the SIP address sip:exumaa1@fabrikam.com. The name of the pool where the Lync Server 2013 Registrar service is running is RedmondPool.litwareinc.com. The Active Directory organizational unit where this information will be stored is OU=ExUmContacts,DC=litwareinc,DC=com. The phone number of the Contact object is 2065554567. The optional -AutoAttendant $True parameter specifies that this object is an auto-attendant Contact object. Setting the -AutoAttendant parameter to False (the default) specifies a subscriber access Contact object.

For details about the New-CsExUmContact and Set-CsExUmContact cmdlets, see the Lync Server Management Shell documentation.

1.3.10.7.5 Deployment Process for Integrating Hosted Exchange UM with Lync Server 2013

Deployment Process for Integrating Hosted Exchange UM with Lync Server 2013

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-09-25*

Effective planning for integrating Lync Server 2013 with hosted Exchange Unified Messaging (UM) requires that you take into account the following:

- Prerequisites for integrating Lync Server 2013 with hosted Exchange UM
- Steps required during the integration process

Deployment Prerequisites for Integrating with Hosted Exchange UM

Before you can begin the integration process, you must already have deployed Lync Server 2013 (at a minimum, a Front End pool or a Standard Edition server), an Edge Server, and Lync 2013 or Lync 2010 clients.

Integration Process

The following table provides an overview of the hosted Exchange UM integration process. For details about deployment steps, see Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM in the Deployment documentation.

Phase	Steps	Rights and permissions	Deployment documentation
Configure the Edge Server.	1. Configure the Edge Server for federation. 2. Manually replicate data to the Edge Server. 3. Configure the hosting provider on the Edge Server.	RTCUniversalServerAdmins	Configure the Edge Server for Integration with Hosted Exchange UM
Configure hosted voice mail policy.	1. Either modify the global hosted voice mail policy or create a new hosted voice mail policy with Site or Per-User scope. 2. For policies with Per-User scope, assign the policy to users or groups.	RTCUniversalServerAdmins	Manage Hosted Voice Mail Policies
Enable users for hosted voice mail.	- Configure user accounts for users whose mailboxes are on a hosted Exchange service.	RTCUniversalUserAdmins	Enable Users for Hosted Voice Mail
Configure hosted contact objects.	1. Create auto-attendant Contact objects for hosted Exchange UM. 2. Create Subscriber Access contact objects for hosted Exchange UM.	RTCUniversalUserAdmins **Note:** To create, modify or remove contact objects, the user who runs the New-CsExUmContact, Set-CsExUmContact or Remove-CsExUmContact cmdlet must have the correct permission to the Active Directory organizational unit where the new contact objects are stored. This permission can be granted by running the Grant-CsOUPermission cmdlet. For details, see the Lync Server Management Shell documentation.	Create Contact Objects for Hosted Exchange UM

1.3.10.8 Planning for Call Admission Control

Planning for Call Admission Control

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-09-21*

For unified communications (UC) applications that are IP-based, such as telephony, video, and application sharing, the available bandwidth of enterprise networks is not generally considered to be a limiting factor within LAN environments. However, on WAN links that interconnect sites, network bandwidth can be limited. When an influx of network traffic oversubscribes a WAN link, current mechanisms such as queuing, buffering, and packet dropping are used to resolve the congestion. The extra traffic is typically delayed until the network congestion eases or, if necessary, the traffic is dropped. For conventional data traffic in such situations, the receiving client can recover. For real-time traffic such as unified communications, network congestion cannot be resolved in this manner, because the unified communications traffic is sensitive to both latency and packet loss. Congestion on the WAN can result in a poor Quality of Experience (QoE) for users. For real-time traffic in congested conditions, it is better to deny calls than to provide connections with poor quality.

Call admission control (CAC) determines whether there is sufficient network bandwidth to establish a real-time session of acceptable quality. In Lync Server 2013, CAC controls real-time traffic only for audio and video, but it does not affect data traffic. If the default WAN path does not have the required bandwidth, CAC can attempt to route the call through an Internet path or the public switched telephone network (PSTN). CAC is available only in Lync Server.

This section describes the call admission control functionality and explains how to plan for CAC.

Note:

Lync Server has three advanced Enterprise Voice features: call admission control (CAC), emergency services (E9-1-1), and media bypass. For an overview of planning information that is common to all three of these features, see Network Settings for the Advanced Enterprise Voice Features.

- Overview of Call Admission Control
- Defining Your Organization's Requirements for Call Admission Control
- Example: Gathering Your Organization's Requirements for Call Admission Control
- Components and Topologies for CAC
- Best Practices for Call Admission Control
- Deployment Checklist for Call Admission Control

1.3.10.8.1 Overview of Call Admission Control

Overview of Call Admission Control

Planning > Planning for Enterprise Voice > Planning for Call Admission Control >

Topic Last Modified: *2012-09-22*

Real-time communications are sensitive to the latency and packet loss that can occur on congested networks. Call admission control (CAC) determines, based on available network bandwidth, whether to allow real-time communications sessions such as voice or video calls to be established. The CAC design in Lync Server 2013 offers four main attributes:

- It is simple to deploy and manage without requiring additional equipment, such as specially configured routers.
- It addresses critical unified communications use cases, such as roaming users and multiple points of presence. CAC policies are enforced according to where the endpoint is located, not where the user is homed.
- In addition to voice calls, it can be applied to other traffic, such as video calls and audio/video conferencing sessions.
- Provides the flexibility to enable representation of various kinds of network topologies. For examples, see Components and Topologies for CAC.

If a new voice or video session exceeds the bandwidth limits that you have set on a WAN link, the session is either blocked or (for phone calls only) rerouted to the PSTN.

CAC controls real-time traffic for voice and video only. It does not control data traffic.

Administrators define CAC policies, which are enforced by the Bandwidth Policy Service that is installed with every Front End pool. CAC settings are automatically propagated to all Lync Server Front End Servers in your network.

For calls that fail because of CAC policies, the order of precedence for rerouting the call is as follows:

1. Internet
2. PSTN
3. Voice mail

Call detail recording (CDR) captures information about calls that are rerouted to the PSTN or to voice mail. CDR does not capture information about calls that are rerouted to the Internet, because the Internet is treated as an alternate path rather than a secondary option.

Note:
Voice mail deposits will not be denied because of bandwidth constraints.

The Bandwidth Policy Service generates two types of log files in comma separated values (CSV) format. The **check failures** log file captures information when bandwidth requests are denied. The **link utilization** log file captures a snapshot of the network topology and the WAN link bandwidth utilization. Both of these log files can assist you in fine-tuning your CAC policies based on utilization.

Call Admission Control Considerations

The administrator selects to install the Bandwidth Policy Service on the first pool configured in the central site. Since there is a single central site per network region, there is only one Bandwidth Policy Service per network region, which manages bandwidth policy for that region, its associated sites and the links to those sites. The Bandwidth Policy Service runs as part of the Front End Servers, and therefore high availability is built-in within that pool. The Bandwidth Policy Service running on each Front End Server synchronizes every 15 seconds. If the Front End pool fails, CAC policies are no longer enforced for that site until the Front End pool and consequently the Bandwidth Policy Service becomes operational again. This implies that all calls will go through for the duration the Bandwidth Policy Service is out of service. Therefore there is the possibility of bandwidth oversubscription of your links during this period

The Bandwidth Policy Service provides high availability within a Front End pool; however, it does not provide redundancy across Front End pools. The Bandwidth Policy Service cannot failover from one Front End pool to another. Once service to the Front End pool is restored, the Bandwidth Policy Service is resumed and can enforce bandwidth policy checks again.

Network Considerations

Although bandwidth restriction for audio and video is enforced by the Bandwidth Policy Service in Lync Server 2013, this restriction is not enforced at the network router (layer 2 and 3). Lync Server 2010 CAC cannot prevent a data application, for example, from consuming the entire network bandwidth on a WAN link, including the bandwidth that is reserved for audio and video by your CAC policy. To protect the necessary bandwidth on your network, you can deploy a Quality of Service (QoS) protocol such as Differentiated Services (DiffServ). Therefore, a best practice is to coordinate the CAC bandwidth policies you define with any QoS settings that you might deploy.

Media and Signaling Paths over VPN

If your enterprise supports media through VPN, ensure that either both the media stream and the signaling stream go through the VPN or both are routed through the internet. By default, the media and signaling streams go through the VPN tunnel.

Call Admission Control of Outside Users

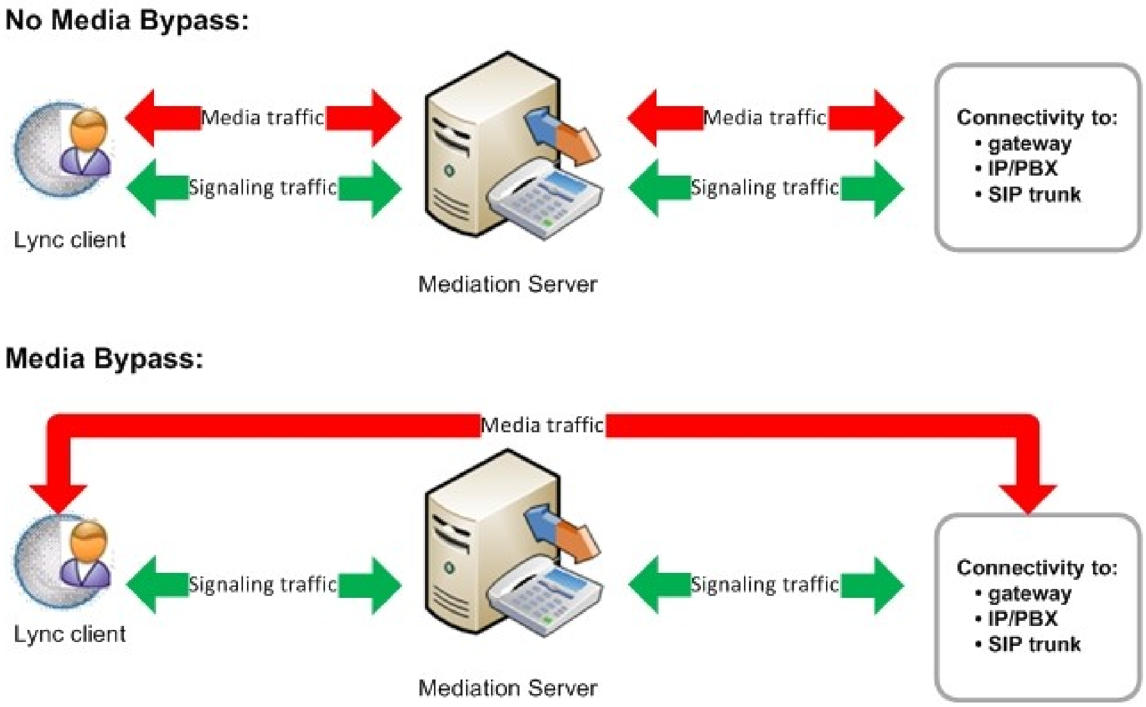
Call admission control is not enforced for remote users where the network traffic flows through the Internet. Because the media traffic is traversing the Internet, which is not managed by Lync Server, CAC cannot be applied. CAC checks will be performed, however, on the portion of the call that flows through the enterprise network.

Call Admission Control of PSTN Connections

Call admission control is enforceable on the Mediation Server regardless of whether it is connected to an IP/PBX, a PSTN gateway, or a SIP trunk. Because the Mediation Server is a back-to-back user agent (B2BUA), it terminates media. It has two connection sides: a side that is connected to Lync Server and a gateway side, which is connected to PSTN gateways, IP/PBXs, or SIP trunks. For details about PSTN connections, see Planning for PSTN Connectivity.

CAC can be enforced on both sides of the Mediation Server unless media bypass is enabled. If media bypass is enabled, the media traffic doesn’t traverse the Mediation Server but instead flows directly between the Lync client and the gateway. In this case, CAC is not needed. For details, see Planning for Media Bypass.

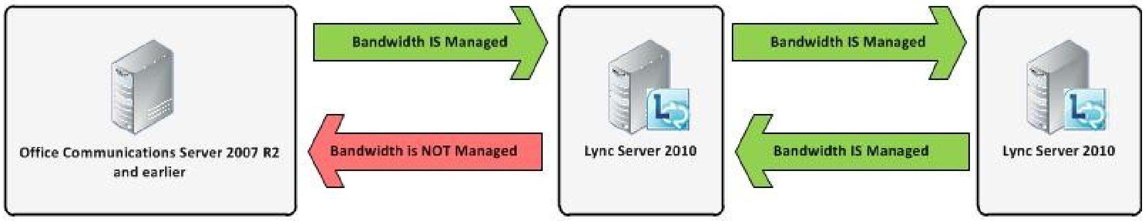
The following figure illustrates how CAC is enforced on PSTN connections with and without media bypass enabled.



Compatibility of Call Admission Control with Earlier Versions of Office Communications Server

Call admission control can be enabled only on endpoints that are enabled for Lync Server 2010 and later.

Call admission control cannot be enabled on endpoints running Office Communicator 2007 R2 or earlier.



1.3.10.8.1.1 Infrastructure Requirements for Call Admission Control

Infrastructure Requirements for Call Admission Control

Planning for Enterprise Voice > Planning for Call Admission Control > Overview of Call Admission Control >

Topic Last Modified: *2012-08-21*

No additional infrastructure requirements, such as special network routers, are necessary. Deploying Lync Server 2013 will automatically install the Bandwidth Policy Service used to enforce call admission control (CAC) policies. Call admission control works only with clients running Lync.

1.3.10.8.2 Defining Your Organization's Requirements for Call Admission Control

Defining Your Organization's Requirements for Call Admission Control

Planning > Planning for Enterprise Voice > Planning for Call Admission Control >

Topic Last Modified: *2012-09-21*

Planning for call admission control (CAC) requires detailed information about your enterprise network topology. To help plan your call admission control policies, follow these steps.

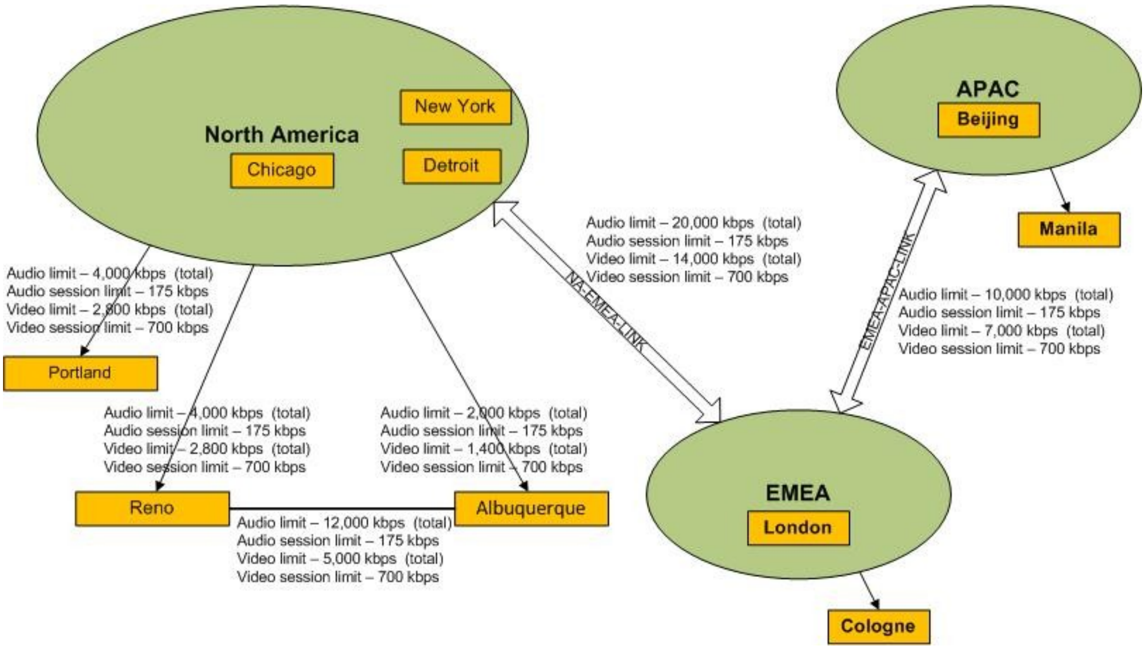
1. Identify the hubs/backbones (called *network regions*) within your enterprise network.
2. Identify the offices or locations (called *network sites*) within each network region.
3. Determine the network route between every pair of network regions.
4. Determine the bandwidth limits for each WAN link.

   Note:

   Bandwidth limits refer to how much of the bandwidth on a WAN link is allocated to Enterprise Voice and audio/video traffic. When a WAN link is described as "bandwidth-constrained," the WAN link has a bandwidth limit that is lower than the expected peak traffic over the link.

5. Identify the IP subnets that are assigned to each network site.

To explain these concepts, we'll use the example network topology shown in the following figure.


North America
New York
Chicago
Detroit
APAC
Beijing
Manila
Audio limit – 20,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 14,000 kbps (total)
Video session limit – 700 kbps
NA-EMEA-LINK
EMEA-APAC-LINK
Audio limit – 10,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 7,000 kbps (total)
Video session limit – 700 kbps
Audio limit – 4,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 2,800 kbps (total)
Video session limit – 700 kbps
Portland
Audio limit – 4,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 2,800 kbps (total)
Video session limit – 700 kbps
Audio limit – 2,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 1,400 kbps (total)
Video session limit – 700 kbps
Reno
Albuquerque
Audio limit – 12,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 5,000 kbps (total)
Video session limit – 700 kbps
EMEA
London
Cologne

Note:

All network sites are associated with a network region. For example, Portland, Reno, and Albuquerque are included in the North America region. In this figure, only WAN links that have CAC policies applied are shown, with bandwidth limits. The network sites of Chicago, New York, and Detroit are shown inside the North America region oval because they are not bandwidth-constrained, and therefore do not require CAC policies.

The components of this example topology are explained in the following sections. For details about how this topology was planned, including the bandwidth limits, see Example: Gathering Your Organization's Requirements for Call Admission Control.

Identify Network Regions

A network region represents a network backbone or a network hub.

A network backbone or hub is a part of computer network infrastructure that interconnects different parts of the network, providing a path for the exchange of information between different LANs or subnets. A backbone can tie together diverse networks from a small location to a wide geographic area. The backbone's capacity is typically greater than that of the networks that connect to it.

Our example topology has three network regions: North America, EMEA, and APAC. A network region contains a collection of network sites (see the definition of network sites later in this topic). Work with your network operations team to identify your network regions.

Associating a Central Site with each Network Region

CAC requires that a Lync Server central site is defined for each network region. The central site is selected with the best network connectivity and highest bandwidth to all the other sites within that network region. The preceding example of network topology shows three network regions, each with a central site that manages CAC decisions. From the preceding example, the appropriate association is shown in the following table.

Note:
Central sites do not necessarily correspond to network sites. In the examples in this documentation, some central sites—Chicago, London, and Beijing—share the same name as the network sites. However, even if a central site and network site share the same name, the central site is an element of the Lync Server topology, whereas the network site is a part of the overall network in which the Lync Server topology resides.

Network regions, central sites, and network sites

Network Region	Central Site	Network Sites
North America	Chicago	Chicago New York Detroit Portland Reno Albuquerque
EMEA	London	London Cologne
APAC	Beijing	Beijing Manila

Identify Network Sites

A network site represents a location where your organization has a physical venue—for example, offices, a set of buildings, or a campus. A physical venue with a LAN and has WAN connectivity to other sites is considered a network site. Start by inventorying all of your organization's offices. In our example topology, the North America network region consists of the following network sites: New York, Chicago, Detroit, Portland, Reno, and Albuquerque.

You must associate every network site with a network region. Depending on whether the network site has a constrained WAN link, a bandwidth policy is associated with the network site. For details about CAC policies and the bandwidth that you allocate by using them, see "Define Bandwidth Policies" later in this topic. To configure CAC, you associate network sites with network regions, and then you create bandwidth-allocating policies to apply to the bandwidth-constrained connections between a given site or region and the WAN connections between the sites and regions.

Identify Network Links

Network links represent connections to the physical WAN that links different regions and sites. In our example topology, there are two regional network links, five network links between regions and sites, and one network link between two sites.

The two regional links are between North America and EMEA, represented as NA-EMEA-LINK, and between APAC and EMEA, represented as EMEA-APAC-LINK.

The site links are indicated by the lines connecting Portland, Reno, and Albuquerque to the North America region, Manila to the APAC region, and Cologne to the EMEA region. The line between Reno and Albuquerque shows a direct network link between these two sites.

Define Bandwidth Policies

Work with your network operations team to determine how much WAN bandwidth is available for real-time audio and video traffic across the WAN links in your organization. Bandwidth policies are typically applied to WAN links if the bandwidth usage is constrained; that is, if it expected to be more than the bandwidth that can be allocated for audio and video modalities.

CAC *bandwidth policies* define the maximum bandwidth that can be reserved for real-time audio and video modalities. Since CAC does not limit the bandwidth of other traffic, it cannot prevent other data traffic such as a large file transfer, music streaming, from using up all of the network bandwidth.

CAC bandwidth policies can define any or all of the following:

- Maximum total bandwidth allocated for audio.
- Maximum total bandwidth allocated for video.
- Maximum bandwidth allocated for a single audio call (session).
- Maximum bandwidth allocated for a single video call (session).

Note:

All CAC bandwidth values represent the maximum *unidirectional* bandwidth limits.

Note:

The Lync Server 2013 Voice Policy features provide the ability to override bandwidth policy checks for incoming calls to the user (not for outgoing calls that are placed by the user). After the session is established, the bandwidth consumption will be accurately accounted for. This setting should be used sparingly. For details, see Create a Voice Policy and Configure PSTN Usage Records or Modify a Voice Policy and Configure PSTN Usage Records in the Deployment documentation.

To optimize bandwidth utilization on a per-session basis, consider the type of audio and video codecs that will be used. In particular, avoid allocating insufficient bandwidth for a codec that you expect to be used frequently. Conversely, if you want to prevent media from using a codec that requires more bandwidth, you should set the maximum bandwidth per session low enough to discourage such use. For audio, not every codec is available for every scenario. For example:

- Peer-to-peer audio calls between Lync endpoints will use either RTAudio (8kHz) or RTAudio (16kHz) when you factor in the bandwidth and prioritization of codecs.
- Conference calls between Lync endpoints and the A/V Conferencing service will use either G.722 or Siren.
- Calls to the public switched telephone network (PSTN) either to or from Lync endpoints will use either G.711 or RTAudio (8kHz).

Use the following table to help optimize the maximum per-session bandwidth settings.

Bandwidth utilization by codecs

Codec	Bandwidth requirement with no forward error correction (FEC)	Bandwidth requirement with forward error correction (FEC)
RTAudio (8kHz)	49.8 kbps	61.6 kbps
RTAudio (16kHz)	67 kbps	96 kbps

Siren	57.6 kbps	73.6 kbps
G.711	102 kbps	166 kbps
G.722	105.6 kbps	169.6 kbps
RTVideo (CIF 15 fps)	260 kbps	Not applicable
RTVideo (VGA 30 fps)	610 kbps	Not applicable

Note:
Bandwidth requirements take into account overhead for the following: Ethernet II, IP, User Datagram Protocol (UDP), RTP (real-time transport protocol), and SRTP (secure real-time transport protocol). They also include 10 kbps for RTCP overhead.

The G.722.1 and Siren codecs are similar, but they offer different bit rates.

G.722, the default codec for Lync Server conferencing, is completely different from the G.722.1 and Siren codecs.

The Siren codec is used in Lync Server in the following situations:

- If the bandwidth policy is set too low for G.722 to be used.
- If a Communications Server 2007 or Communications Server 2007 R2 client connects to a Lync Server conferencing service (because those clients do not support the G.722 codec).

Bandwidth utilization by scenario

Scenario	Bandwidth requirement optimized for quantity (kbps)	Bandwidth requirement for Balanced mode (kbps)	Bandwidth requirement optimized for quality (kbps)
Peer-to-peer audio calls	45 kbps	62 kbps	91 kbps
Conference calls	53 kbps	101 kbps	165 kbps
PSTN calls (between Lync 2013 and PSTN gateway, with media bypass)	97 kbps	97 kbps	161 kbps
PSTN calls (between Lync 2013 and Mediation Server, without media bypass)	45 kbps	97 kbps	161 kbps
PSTN calls (between Mediation Server and PSTN gateway, without media bypass)	97 kbps	97 kbps	161 kbps

Identify IP Subnets

For each network site, you will need to work with your network administrator to determine what IP subnets are assigned to each network site. If your network administrator has already organized the IP subnets into network regions and network sites, then your work is significantly simplified.

In our example, the New York site in the North America region is assigned the following IP subnets: 172.29.80.0/23, 157.57.216.0/25, 172.29.91.0/23, 172.29.81.0/24. Suppose Bob, who typically works in Detroit, travels to the New York office for training. When he turns on his computer and connects to the network, his computer will get an IP address in one of the four ranges reserved for New York, for example 172.29.80.103.

⚠**Warning:**

The IP subnets specified during network configuration on the server must match the format provided by client computers in order to be properly used for media bypass. A Lync client takes its local IP address and masks the IP address with the associated subnet mask. When determining the bypass ID associated with each client, the Registrar will compare the list of IP subnets associated with each network site against the subnet provided by the client for an exact match. For this reason, it is important that subnets entered during network configuration on the server are actual subnets instead of virtual subnets. (If you deploy call admission control, but not media bypass, call admission control will function properly even if you configure virtual subnets.)
For example, if a client signs in on a computer with an IP address of 172.29.81.57 with an IP subnet mask of 255.255.255.0, Lync 2013 will request the bypass ID associated with subnet 172.29.81.0. If the subnet is defined as 172.29.0.0/16, although the client belongs to the virtual subnet, the Registrar will not consider this a match because the Registrar is specifically looking for subnet 172.29.81.0. Therefore, it is important that the administrator enters subnets exactly as provided by Lync clients (which are provisioned with subnets during network configuration either statically or by DHCP.)

1.3.10.8.3 Example: Gathering Your Organization's Requirements for Call Admission Control

Example: Gathering Your Organization's Requirements for Call Admission Control

Planning > Planning for Enterprise Voice > Planning for Call Admission Control >

Topic Last Modified: *2012-09-21*

This example shows you how to plan for and implement call admission control (CAC). At a high level, this consists of the following activities:

1. Identify all of your network hubs and backbones (known as *network regions*).
2. Identify the Lync Server central site that will manage CAC for each network region.
3. Identify and define the *network sites* that are connected to each network region.
4. For each network site whose connection to the WAN is bandwidth-constrained, describe the bandwidth capacity of the WAN connection and the bandwidth limits that to the network administrator has set for Lync Server media traffic, if applicable. You do not need to include sites whose connection to the WAN is not bandwidth-constrained.
5. Associate each subnet in your network with a network site.
6. Map the links between the network regions. For each link, describe its bandwidth capacity and any limits that the network administrator has placed on Lync Server media traffic.
7. Define a route between every pair of network regions.

Gather the Required Information

To prepare for call admission control, gather the information described in the following steps:

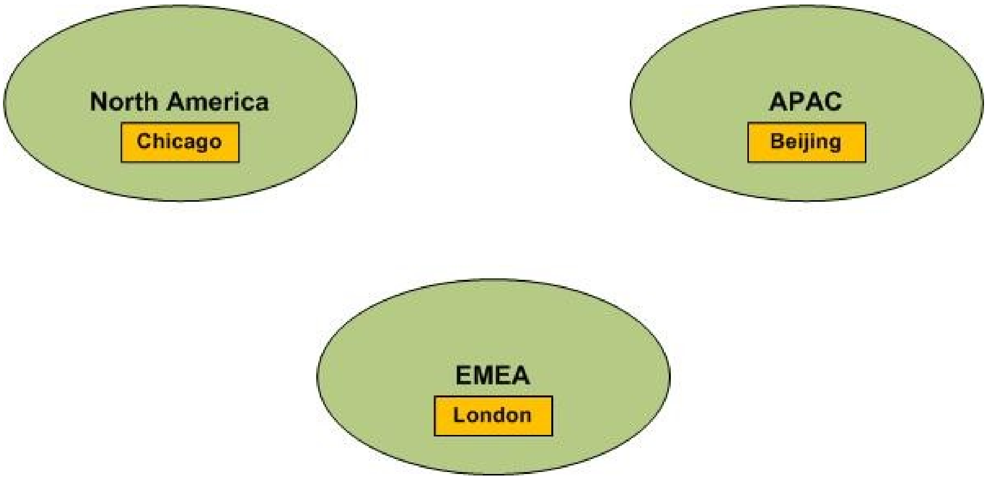
1. Identify your network regions. A network region represents a network

backbone or a network hub.

A network backbone or a network hub is a part of computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnets. A backbone can tie together diverse networks, from a small location to a wide geographic area. The backbone's capacity is typically greater than that of the networks connected to it.

Our example topology has three network regions: North America, EMEA, and APAC. A network region contains a collection of network sites. Work with your network administrator to define the network regions for your enterprise.

2. Identify each network region’s associated central site. A central site contains at least one Front End Server and is the Lync Server deployment that will manage CAC for all media traffic that passes through the network region’s WAN connection.



Note:

A Multiprotocol Label Switching (MPLS) network should be represented as a network region in which each geographic location has a corresponding network site. For details, see the “Call Admission Control on an MPLS Network” topic in the Planning documentation.

In the preceding example network topology, there are three network regions, each with a Lync Server central site that manages CAC. The appropriate central site for a network region is chosen by the geographic vicinity. Because media traffic will be heaviest within network regions, the ownership by geographic vicinity makes it self-contained and will continue to be functional even if other central sites become unavailable.

In this example, a Lync Server deployment named Chicago is the central site for the North America region.

All Lync users in North America are homed on servers in the Chicago deployment. The following table shows central sites for all three network regions.

Network Regions and their Associated Central Sites

Network Region	Central Site
North America	Chicago
EMEA	London
APAC	Beijing

Note:

Depending on your Lync Server topology, the same central site can be assigned to multiple network regions.

3. For each network region, identify all of the network sites (offices or locations) whose WAN connections are not bandwidth-constrained. Because these sites are not bandwidth constrained, you do not need to apply CAC bandwidth policies to them.
   In the example shown in the following table, three network sites do not have bandwidth-constrained WAN links: New York, Chicago, and Detroit.

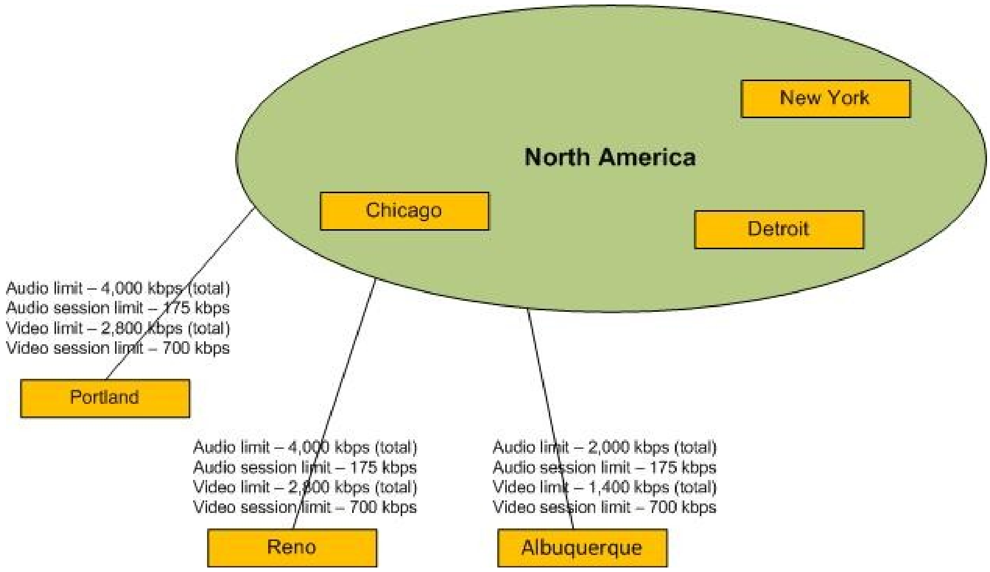
Network Sites not Constrained by WAN Bandwidth

Network Site	Network Region
New York	North America
Chicago	North America
Detroit	North America

4. For each network region, identify all of the network sites that connect to the network region through bandwidth-constrained WAN links.
   To help ensure audio and video quality, we recommend that these bandwidth-constrained network sites have their WANs monitored and CAC bandwidth policies that limit media (voice or video) traffic flow to and from the network region.
   In the example shown in the following table, there are three network sites that are constrained by WAN bandwidth: Portland, Reno and Albuquerque.

Network Sites Constrained by WAN Bandwidth

Network Site	Network Region
Albuquerque	North America
Reno	North America
Portland	North America


New York
North America
Chicago
Detroit
Audio limit – 4,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 2,800 kbps (total)
Video session limit – 700 kbps
Portland
Audio limit – 4,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 2,800 kbps (total)
Video session limit – 700 kbps
Reno
Audio limit – 2,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 1,400 kbps (total)
Video session limit – 700 kbps
Albuquerque

5. For each bandwidth-constrained WAN link, determine the following:
   - Overall bandwidth limit that you want to set for all concurrent audio sessions. If a new audio session will cause this limit to be exceeded, Lync Server does not allow the session to start.
   - Bandwidth limit that you want to set for each individual audio session. The default CAC bandwidth limit is 175 kbps, but it can be modified by the administrator.
   - Overall bandwidth limit that you want to set for all concurrent video sessions. If a new video session will cause this limit to be exceeded, Lync Server does not allow the session to start.

- Bandwidth limit that you want to set for each individual video session. The default CAC bandwidth limit is 700 kbps, but it can be modified by the administrator.

Network Sites with WAN Bandwidth Constraint Information (Bandwidth in kbps)

Network Site	Network Region	BW Limit	Audio Limit	Audio Session Limit	Video Limit	Video Session Limit
Albuquerque	North America	5,000	2,000	175	1,400	700
Reno	North America	10,000	4,000	175	2,800	700
Portland	North America	5,000	4,000	175	2,800	700
New York	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)
Chicago	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)
Detroit	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)

6. For every subnet in your network, specify its associated network site.

Important:

Every subnet in your network must be associated with a network site, even if the network site is not bandwidth constrained. This is because call admission control uses subnet information to determine at which network site an endpoint is located. When the locations of both parties in the session are determined, call admission control can determine if there is sufficient bandwidth to establish a call. When a session is established over a link that has no bandwidth limits, an alert is generated.

If you deploy Audio/Video Edge Servers, the public IP addresses of each Edge Server must be associated with the network site where the Edge Server is deployed. Each public IP address of the A/V Edge Server must be added to your network configuration settings as a subnet with a subnet mask of 32. For example, if you deploy A/V Edge Servers in Chicago, then for each external IP address of those servers create a subnet with a subnet mask of 32 and associate network site Chicago with those subnets. For details about public IP addresses, see Determine External A/V Firewall and Port Requirements in the Planning documentation.

Note:

A Key Health Indicator (KHI) alert is raised, specifying a list of IP addresses that are present in your network but are either not associated with a subnet, or the subnet that includes the IP addresses is not associated with a network site. This alert will not be raised more than once within an 8 hour period. The relevant alert information and an example are as follows:

Source: CS Bandwidth Policy Service (Core)
Event number: 36034
Level: 2
Description: The subnets for the following IP Addresses: <List of IP Addresses> are either not configured or the subnets are not associated to a network site.
Cause: The subnets for the corresponding IP addresses are missing from the network configuration settings or the subnets are not associated to a network site.
Resolution: Add subnets corresponding to the preceding list of IP addresses

into the network configuration settings and associate every subnet to a network site.
For example, if the IP address list in the alert specifies 10.121.248.226 and 10.121.249.20, either these IP addresses are not associated with a subnet, or the subnet that they are associated with does not belong to a network site. If 10.121.248.0/24 and 10.121.249.0/24 are the corresponding subnets for these addresses, you can resolve this issue as follows:

- Be sure that IP address 10.121.248.226 is associated with the 10.121.248.0/24 subnet and IP address 10.121.249.20 is associated with the 10.121.249.0/24 subnet.
- Be sure that the 10.121.248.0/24 and 10.121.249.0/24 subnets are each associated with a network site.

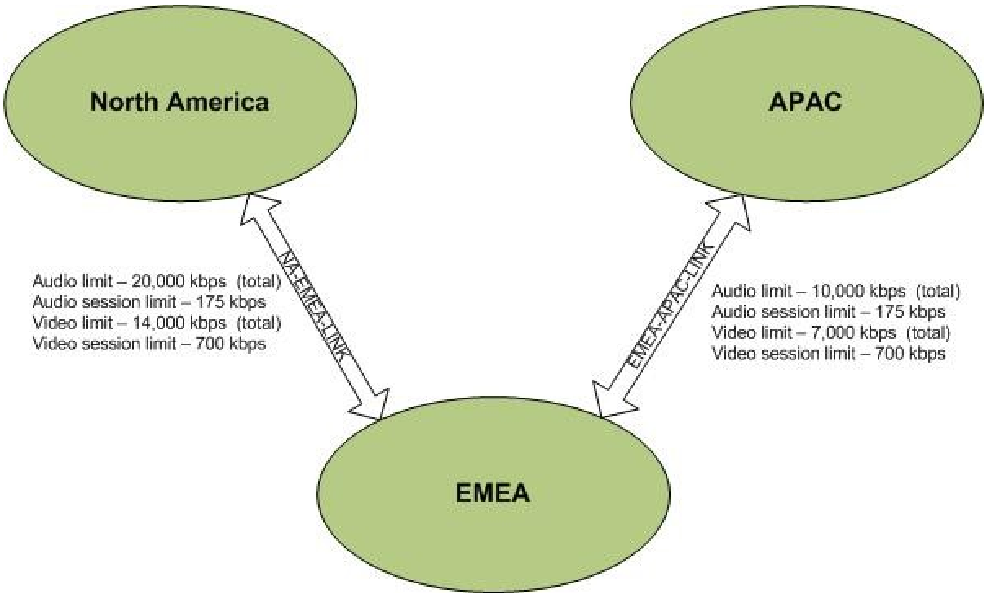
Network Sites and Associated Subnets (Bandwidth in kbps)

Network Site	Network Region	BW Limit	Audio Limit	Audio Session Limit	Video Limit	Video Session Limit	Subnets
Albuquerque	North America	5,000	2,000	175	1,400	700	172.29.79.0/23, 157.57.215.0/25, 172.29.90.0/23, 172.29.80.0/24
Reno	North America	10,000	4,000	175	2,800	700	157.57.210.0/23, 172.28.151.128/25
Portland	North America	5,000	4,000	175	2,800	700	172.29.77.0/24 10.71.108.0/24, 157.57.208.0/23
New York	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)	172.29.80.0/23, 157.57.216.0/25, 172.29.91.0/23, 172.29.81.0/24
Chicago	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)	157.57.211.0/23, 172.28.152.128/25
Detroit	North America	(no limit)	(no limit)	(no limit)	(no limit)	(no limit)	172.29.78.0/24 10.71.109.0/24, 157.57.209.0/23

1. In Lync Server call admission control, the connections between network regions are called *region links*. For each region link, determine the following,

just as you did for the network sites:

- Overall bandwidth limit that you want to set for all concurrent audio sessions. If a new audio session will cause this limit to be exceeded, Lync Server does not allow the session to start.
- Bandwidth limit that you want to set for each individual audio session. The default CAC bandwidth limit is 175 kbps, but it can be modified by the administrator.
- Overall bandwidth limit that you want to set for all concurrent video sessions. If a new video session will cause this limit to be exceeded, Lync Server does not allow the session to start.
- Bandwidth limit that you want to set for each individual video session. The default CAC bandwidth limit is 700 kbps, but it can be modified by the administrator.


North America
APAC
NA-EMEA-LINK
EMEA-APAC-LINK
Audio limit – 20,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 14,000 kbps (total)
Video session limit – 700 kbps
Audio limit – 10,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 7,000 kbps (total)
Video session limit – 700 kbps
EMEA

Region Link Bandwidth Information (Bandwidth in kbps)

Region Link Name	First Region	Second Region	BW Limit	Audio Limit	Audio Session Limit	Video Limit	Video Session Limit
NA-EMEA-LINK	North America	EMEA	50,000	20,000	175	14,000	700
EMEA-APAC-LINK	EMEA	APAC	25,000	10,000	175	7,000	700

2. Define a route between every pair of network regions.

Note:

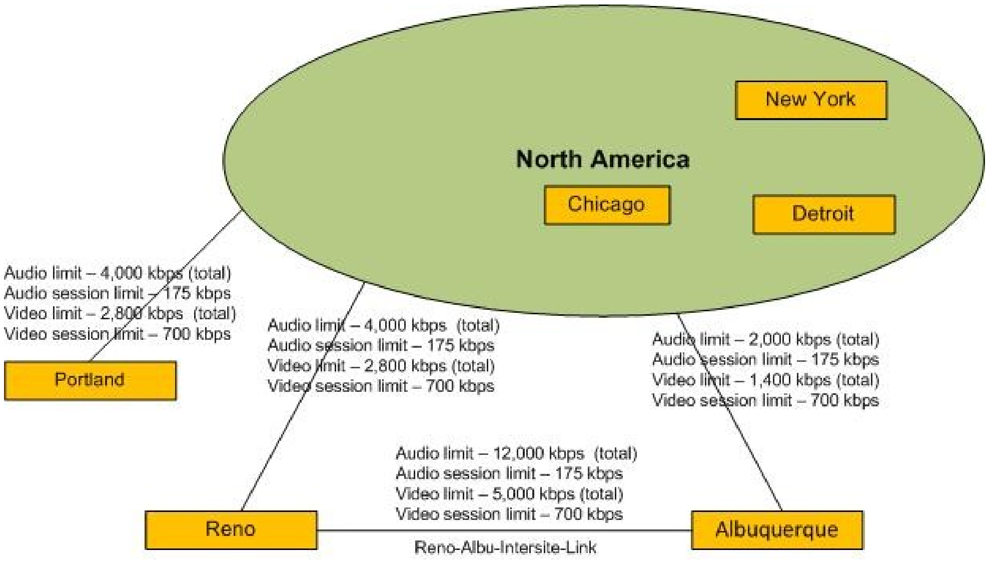
Two links are required for the route between the North America and APAC regions because there is no region link that directly connects them.

Region Routes

Region Route Name	First Region	Second Region	Region Links
NA-EMEA-ROUTE	North America	EMEA	NA-EMEA-LINK
EMEA-APAC-ROUTE	EMEA	APAC	EMEA-APAC-LINK

NA-APAC-ROUTE	North America	APAC	NA-EMEA-LINK, EMEA-APAC-LINK

3. For every pair of network sites that are directly connected by a single link (called an *inter-site* link), determine the following:
   - Overall bandwidth limit that you want to set for all concurrent audio sessions. If a new audio session will cause this limit to be exceeded, Lync Server does not allow the session to start.
   - Bandwidth limit that you want to set for each individual audio session. The default CAC bandwidth limit is 175 kbps, but it can be modified by the administrator.
   - Overall bandwidth limit that you want to set for all concurrent video sessions. If a new video session will cause this limit to be exceeded, Lync Server does not allow the session to start.
   - Bandwidth limit that you want to set for each individual video session. The default CAC bandwidth limit is 700 kbps, but it can be modified by the administrator.


New York
North America
Chicago
Detroit
Audio limit – 4,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 2,800 kbps (total)
Video session limit – 700 kbps
Portland
Audio limit – 4,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 2,800 kbps (total)
Video session limit – 700 kbps
Audio limit – 2,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 1,400 kbps (total)
Video session limit – 700 kbps
Audio limit – 12,000 kbps (total)
Audio session limit – 175 kbps
Video limit – 5,000 kbps (total)
Video session limit – 700 kbps
Reno
Albuquerque
Reno-Albu-Intersite-Link

Bandwidth Information for an Inter-Site Link between Two Network Sites (Bandwidth in kbps)

Inter-Site Link Name	First Site	Second Site	BW Limit	Audio Limit	Audio Session Limit	Video Limit	Video Session Limit
Reno-Albu-Intersite-Link	Reno	Albuquerque	20,000	12,000	175	5,000	700

Next Steps

After you have gathered the required information, you can perform CAC deployment either by using the Lync Server Management Shell or Lync Server Control Panel.

Note:

Although you can perform most network configuration tasks by using Lync Server Control Panel, to create subnets and intersite links, you must use Lync Server Management Shell. For details, see the Lync Server Management Shell documentation for the **New-CsNetworkSubnet** cmdlet and the **New-CsNetworkIntersitePolicy** cmdlet.

1.3.10.8.4 Components and Topologies for CAC

Components and Topologies for CAC

[Planning](#) > [Planning for Enterprise Voice](#) > [Planning for Call Admission Control](#) >

Topic Last Modified: *2012-10-20*

The topics in this section provide information about special considerations for deploying call admission control (CAC) with various types of network topologies.

- [Call Admission Control on an MPLS Network](#)
- [Call Admission Control on a SIP Trunk](#)
- [Call Admission Control with a Third-Party PSTN Gateway or PBX](#)

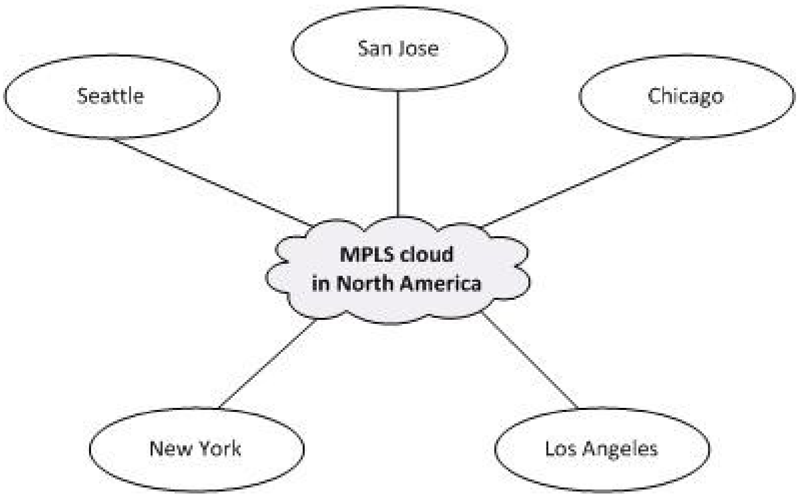
1.3.10.8.4.1 Call Admission Control on an MPLS Network

Call Admission Control on an MPLS Network

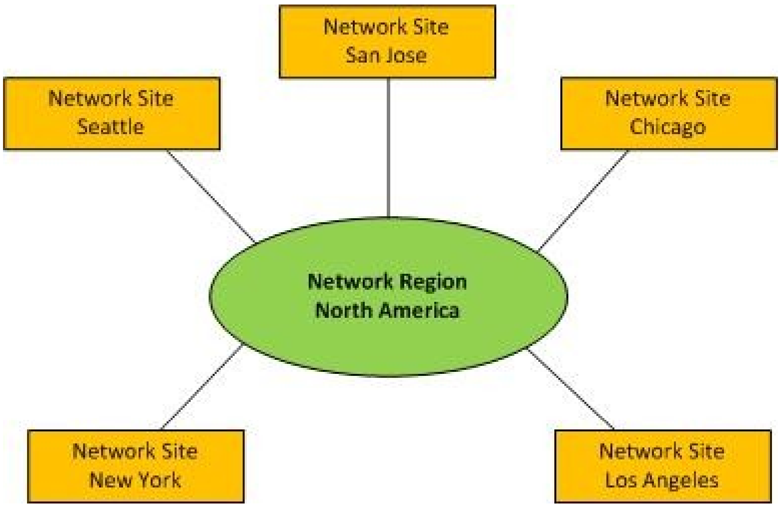
[Planning for Enterprise Voice](#) > [Planning for Call Admission Control](#) > [Components and Topologies for CAC](#) >

Topic Last Modified: *2012-09-22*

In a Multiprotocol Label Switching (MPLS) network, all sites are connected by a full-mesh. That is, all sites are connected directly to the MPLS backbone of the Internet service provider, and each site is provisioned bandwidth to be used across a WAN link to the MPLS cloud. There is no network hub or central site to control IP routing. The following figure shows a simple network based on MPLS technology.



To deploy call admission control (CAC) in an MPLS network, you create a network region to represent the MPLS cloud, and create a network site to represent each MPLS satellite site. The following figure illustrates how the network region and network sites should be configured to represent the example MPLS network in the previous figure. The overall bandwidth limits and bandwidth session limits are then based on the capacity of the WAN link from each network site to the network region that represents the MPLS cloud.



1.3.10.8.4.2 Call Admission Control on a SIP Trunk

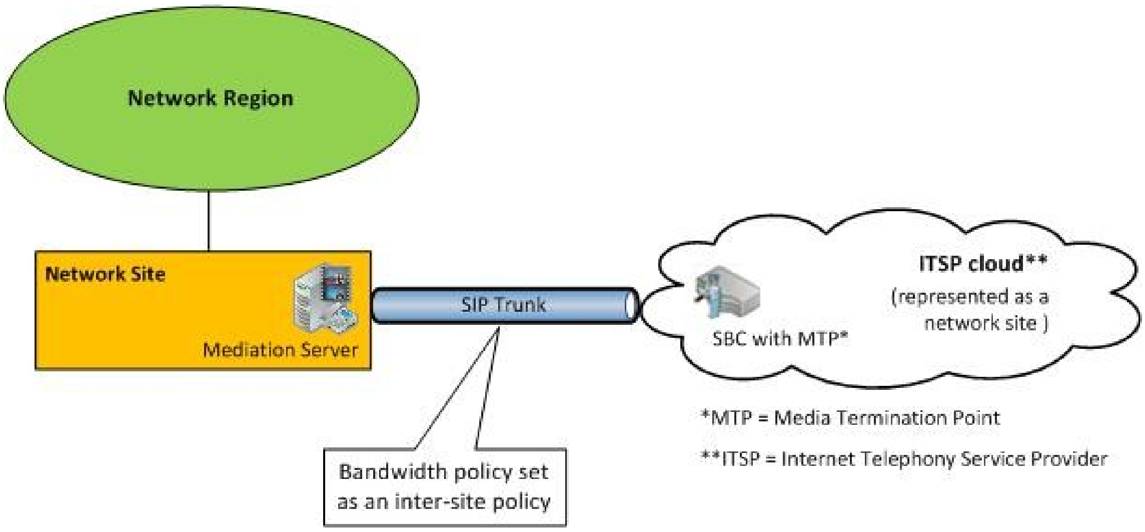
Call Admission Control on a SIP Trunk

Planning for Enterprise Voice > Planning for Call Admission Control > Components and Topologies for CAC >

Topic Last Modified: *2012-09-22*

To deploy call admission control (CAC) on a SIP trunk, you create a network site to represent the Internet telephony service provider (ITSP). To apply bandwidth policy values on the SIP trunk, you create an inter-site policy between the network site in your enterprise and the network site that you create to represent the ITSP.

The following figure shows an example CAC deployment on a SIP trunk.


Network Region
Network Site
Mediation Server
SIP Trunk
SBC with MTP*
ITSP cloud**
(represented as a network site)
*MTP = Media Termination Point
**ITSP = Internet Telephony Service Provider
Bandwidth policy set as an inter-site policy

To configure CAC on a SIP trunk, you will have to perform the following tasks during CAC deployment:

1. Create a network site to represent the ITSP. Associate the network site to an appropriate network region, and allocate bandwidth of zero for audio and video for this network site. For details, see Configure Network Sites for CAC

in the Deployment documentation.

Note:
For the ITSP, this network site configuration is not functional. Bandwidth policy values are actually applied in step 2.

2. Create an inter-site link for the SIP trunk using the relevant parameter values for the site you created in step 1. For example, use the name of the network site in your enterprise as the value of the NetworkSiteID1 parameter, and the ITSP network site as the value of the NetworkSiteID2 parameter. For details, see Create Network Intersite Policies in the Deployment documentation. Also see the Lync Server Management Shell documentation for the New-CsNetworkInterSitePolicy cmdlet.
3. Get the IP address of the Session Border Controller's (SCB) Media Termination Point from your ITSP. Add that IP address with a subnet mask of 32 to the network site that represents the ITSP. For details, see Associate a Subnet with a Network Site.

1.3.10.8.4.3 Call Admission Control w ith a Third-Party PSTN Gatew ay or PBX

Call Admission Control with a Third-Party PSTN Gateway or PBX

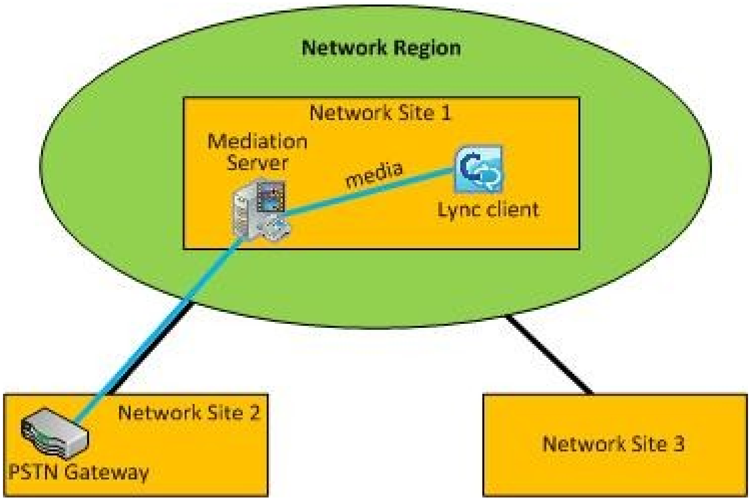
Planning for Enterprise Voice > Planning for Call Admission Control > Components and Topologies for CAC >

Topic Last Modified: *2012-10-20*

This topic describes examples of how call admission control (CAC) can be deployed on the link between the Mediation Server's gateway interface and a third-party public switched telephone network (PSTN) gateway or private branch exchange (PBX).

Case 1: CAC between the Mediation Server and a PSTN gateway

CAC can be deployed on the WAN link from the Mediation Server's gateway interface to a third-party PBX or PSTN gateway.



In this example, CAC is applied between the Mediation Server and a PSTN gateway. If a Lync client user at Network Site 1 places a PSTN call through the PSTN gateway in

Network Site 2, the media flows through the WAN link. Therefore, two CAC checks are performed for each PSTN session:

- Between the Lync client application and the Mediation Server
- Between the Mediation Server and the PSTN gateway

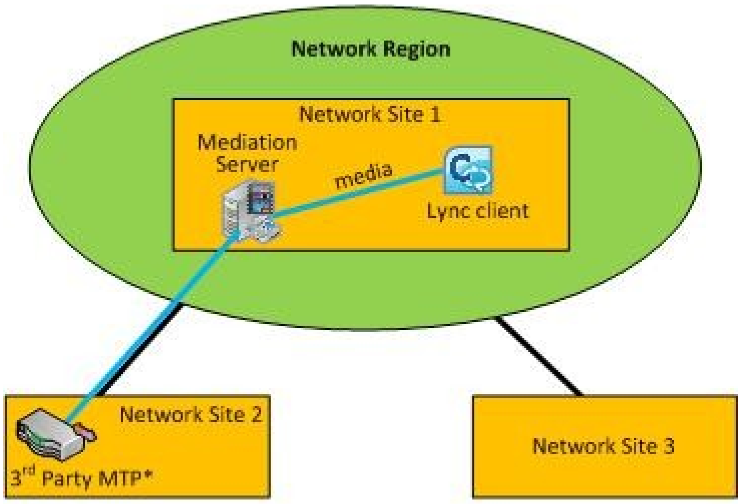
This works for both incoming PSTN calls to a client in Network Site 1, and for outgoing PSTN calls originating from a client application in Network Site 1.

Note:

Make sure that the IP subnet that the PSTN gateway belongs to is configured and associated with Network Site 2.
Make sure that the IP subnet that both interfaces of the Mediation Server belong to is configured and associated with Network Site 1.
For details, see Associate a Subnet with a Network Site.

Case 2: CAC between the Mediation Server and a third-party PBX with Media Termination Point

This configuration is similar to Case 1. In both the cases, the Mediation Server knows what device terminates media at the opposite end of the WAN link, and the IP address of the PSTN gateway or PBX with Media Termination Point (MTP) is configured on the Mediation Server as the next hop.



*MTP = Media Termination Point

In this example, CAC is applied between the Mediation Server and the PBX/MTP. If a Lync client user at the Network Site 1 places a PSTN call through the PBX/MTP located in Network Site 2, the media flows through the WAN link. Therefore, for each PSTN session two CAC checks are performed:

- Between the Lync client application and the Mediation Server
- Between the Mediation Server and the PBX/MTP

This works for both incoming PSTN calls to a client in Network Site 1, and outgoing PSTN calls originating from a client in Network Site 1.

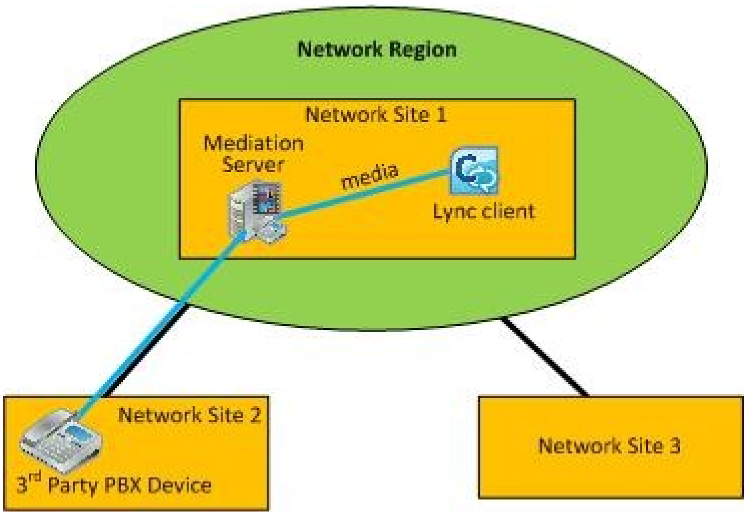
Note:

Make sure that the IP subnet that the MTP belongs to is configured and associated with Network Site 2.

Make sure that the IP subnet that both interfaces of the Mediation Server belong to is configured and associated with Network Site 1.
For details, see Associate a Subnet with a Network Site.

Case 3: CAC between the Mediation Server and a third-party PBX without a Media Termination Point

Case 3 is slightly different from the first two cases. If there is no MTP on the third-party PBX, for an outgoing session request to the third-party PBX the Mediation Server does not know where media will terminate in the PBX boundary. In this case, the media flows directly between the Mediation Server and the third-party endpoint device.



In this example, if a Lync client user at Network Site 1 places a call to a user through the PBX, the Mediation Server is able to perform CAC checks only on the proxy leg (between the Lync client application and Mediation Server). Because the Mediation Server does not have information about the endpoint device while the session is being requested, CAC checks cannot be performed on the WAN link (between the Mediation Server and the third-party endpoint) prior to call establishment. After the session is established, however, the Mediation Server facilitates in accounting for the bandwidth used on the trunk.

For calls that originate from the third-party endpoint, the information about that endpoint device is available at the time of session request and CAC check can be performed on both the sides of the Mediation Server.

Note:

Make sure that the IP subnet that the endpoint devices belong to is configured and associated with Network Site 2.
Make sure that the IP subnet that both interfaces of the Mediation Server belong to is configured and associated with Network Site 1.
For details, see Associate a Subnet with a Network Site.

1.3.10.8.5 Best Practices for Call Admission Control

Best Practices for Call Admission Control

Planning > Planning for Enterprise Voice > Planning for Call Admission Control >

Topic Last Modified: *2012-09-22*

To enhance performance and facilitate deployment, apply the following best practices when you deploy call admission control:

- Ensure that WANs are adequately provisioned for current and anticipated media traffic.

> **Note:**
> We recommend that you factor in a buffer to your bandwidth limits. There are scenarios such as race conditions that affect the total bandwidth used and can result in situations where the bandwidth limit is exceeded. For example, if two calls try to start while media traffic is approaching a bandwidth limit, one of them may be denied because the other managed to start first.

- Monitor network usage and call detail records so that you can choose optimal CAC settings and update CAC settings as network usage changes.
- Use CAC bandwidth policies to complement QoS settings.
- If you want to re-route blocked calls onto the PSTN, verify PSTN functionality and capacity. For details, see Planning Outbound Voice Routing.

> **Note:**
> Capacity refers to the number of ports you need to open to support potential PSTN re-routing.

1.3.10.8.6 Deployment Checklist for Call Admission Control

Deployment Checklist for Call Admission Control

Planning > Planning for Enterprise Voice > Planning for Call Admission Control >

Topic Last Modified: *2012-10-08*

To plan effectively for call admission control (CAC), you need to consider the following:

- Prerequisites for deploying CAC.
- Information required for CAC and configuration decisions that you must make in advance of deployment.

Deployment Prerequisites for Call Admission Control

Before you deploy call admission control, you must already have deployed your Lync Server 2013 internal servers, including either a Front End pool or a Standard Edition server.

Information Requirements for Call Admission Control

The following table summarizes the required information for deploying call admission control.

Information Requirements for Call Admission Control Deployment

Information	Summary of Information Required	Documentation
Lync Server capabilities required by your organization	• Capabilities to be supported by your organization • Capabilities to be enabled for individual users	Defining Your Organization's Requirements for Call Admission Control
Topologies and components to be deployed	• CAC related components are automatically installed as part of Lync Server 2013	Defining Your Organization's Requirements for Call Admission Control
System requirements	• Hardware requirements • Software requirements • Collocation requirements	Determining Your System Requirements
Infrastructure requirements	• No specific infrastructure requirements are necessary for CAC	Infrastructure Requirements for Call Admission Control
Network interface requirements	• Internal and external interface information • Routing information (including information on the NextHop blog at http://go.microsoft.com/fwlink/p/?LinkId=203149, Microsoft Lync Server team's customer response channel)	Deploying External User Access
Deployment strategy	• Deployment sequence • Workgroup or domain • Security • Monitoring and auditing • Hardware considerations	Best Practices for Call Admission Control
Deployment process	• Prerequisites • Information requirements • Process and procedures	Configure Call Admission Control

1.3.10.9 Planning for Emergency Services (E9-1-1)

Planning for Emergency Services (E9-1-1)

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-10-17*

Lync Server 2013 supports Enhanced 9-1-1 (E9-1-1) services within the United States as part of an Enterprise Voice deployment. E9-1-1 is an emergency dispatch feature that associates a 9-1-1 call with an Emergency Response Location (ERL) that consists of civic (that is, street) addresses and other more specific location information, such as floor numbers, for calls from office buildings and other multitenant facilities. By using the provided ERL, a Public Safety Answering Point (PSAP) can immediately dispatch first responders to the caller in distress with reduced risk of inadvertently directing the responder to an incorrect or ambiguous location.

Note:
Lync Server has three advanced Enterprise Voice features: call admission control, emergency services (E9-1-1), and media bypass. For an overview of planning information that is common to all three of these features, see Network Settings for the Advanced Enterprise Voice Features.

- Overview of E9-1-1
- Defining Your Requirements for Emergency Calls
- Deployment Checklist for E9-1-1

1.3.10.9.1 Overview of E9-1-1

Overview of E9-1-1

Planning > Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) >

Topic Last Modified: *2012-10-29*

Microsoft Lync Server 2013 supports Enhanced 9-1-1 (E9-1-1) calling from Lync clients and Lync Phone Edition devices. When you configure Lync Server for E9-1-1, emergency calls placed from Lync 2013 or Lync Phone Edition include Emergency Response Location (ERL) information from the Location Information service database. ERLs consist of civic (that is, street) addresses and other information that helps to identify a more precise location in office buildings and other multitenant facilities. When a user makes an emergency call, Lync Server routes the call audio, along with the location and callback information, through a Mediation Server to an E9-1-1 service provider. The E9-1-1 service provider uses the civic address of the caller to route the call to the Public Safety Answering Point (PSAP) that serves the caller's location, and sends along an Emergency Service Query Key (ESQK) that the PSAP uses to look up the caller's ERL.

Lync Server supports two methods for routing emergency calls to an E9-1-1 service provider:

- A Session Initiation Protocol (SIP) trunk connection to a qualified E9-1-1 service provider
- An Emergency Location Identification Number (ELIN) gateway to a public switched telephone (PSTN)-based E9-1-1 service provider

When you use a SIP trunk E9-1-1 service provider, you add ERLs to the Location Information service database, and then validate the locations against a Master Street Address Guide (MSAG) that is maintained by the E9-1-1 service provider. If an E9-1-1 service provider receives a call that doesn't have location information or has a location that has not been validated against the MSAG, the E9-1-1 service provider routes the call to a national/regional Emergency Call Response Center (ECRC), which is staffed with specially trained personnel who verbally obtain the caller's location, if possible, and manually route the call to the appropriate PSAP. (Some SIP trunk E9-1-1 service providers also provide customers with a PSTN direct inward dialing (DID) number to the ECRC, which provides an alternate means of routing 9-1-1 calls, if the SIP trunk fails for any reason.)

Unlike time division multiplexing (TDM) and IP-based private branch exchange (PBX) phones, which have fixed locations, a Lync endpoint can be very mobile. When you deploy the E9-1-1 feature, Lync Server helps to ensure that no matter where a caller is located, the emergency call can be routed to the PSAP that serves the caller's location. For example, if a user's main office is located in Redmond, Washington, but the user places an emergency call from a computer in a branch office in Wichita, Kansas, the SIP trunk or PSTN-based E9-1-1 service provider will route the call to the PSAP in Wichita, not to the PSAP in Redmond.

When you use an ELIN gateway, you also add ERLs to the Location Information service database, but you include also an ELIN number for each location. The ELIN number becomes the emergency calling number during the emergency call. You must then make sure that your PSTN carrier uploads the ELINs to the Automatic Location Identification (ALI) database.

Note:

Lync-connected analog devices cannot receive location information from the Location Information service or transmit location to the E9-1-1 service provider. If you use the SIP trunk E9-1-1 service provider option and need to support E9-1-1 from analog phones, you have two options:

- **Traditional PS-ALI option** If you have local PSTN gateways at each site where analog phones are deployed and each analog phone has a DID, you can provision the analog device’s location directly with a Private Switch/ Automatic Location Identification (PS-ALI) service provider. In this case, you configure specially-crafted Lync voice policies and assign them to the analog device contact objects so that E9-1-1 calls from those phones route directly through the local gateway to the PSTN provider that services the site (instead of routing the call to an E9-1-1 service provider SIP trunk). When an emergency call is placed, a database at a PS-ALI provider that is associated with the PSTN trunk maps the DID of each analog phone to a physical location and provides this location to the PSAP. These records must be updated with the PS-ALI service provider every time phones are moved to different ERLs.
- **E9-1-1 service provider option** You can register the analog phone DIDs and their corresponding ERLs with the E9-1-1 service provider, if this is supported by the E9-1-1 service provider. If the provider receives a call from Lync Server that doesn’t include PIDF-LO data, the provider can see if there is a database match on the calling party’s DID number. By using the ERL retrieved from its database, the provider can automatically route the emergency call to the correct PSAP, and the PSAP will receive the DID of the analog device and an ESQK record that allows the dispatcher to lookup the caller’s location.

If you use the ELIN gateway option and need to support E9-1-1 from analog phones, you can provision the analog device's location directly with the PS-ALI service provider, as described in the first option above.

From a Lync Server perspective, the E9-1-1 process can be separated into two stages:

- Stage 1: Acquiring a location
- Stage 2: Routing the emergency call to an E9-1-1 service provider

This section describes how these stages work.

If you plan to configure your infrastructure to automatically detect client location, first you need to decide which network elements you will use to map callers to locations. For details about the possible options, see Defining the Network Elements Used to Determine Location.

In This Section

- Acquiring a Location
- Routing E9-1-1 Calls by Using a SIP Trunk
- Routing E9-1-1 Calls by Using an ELIN Gateway

1.3.10.9.1.1 Acquiring a Location

Acquiring a Location

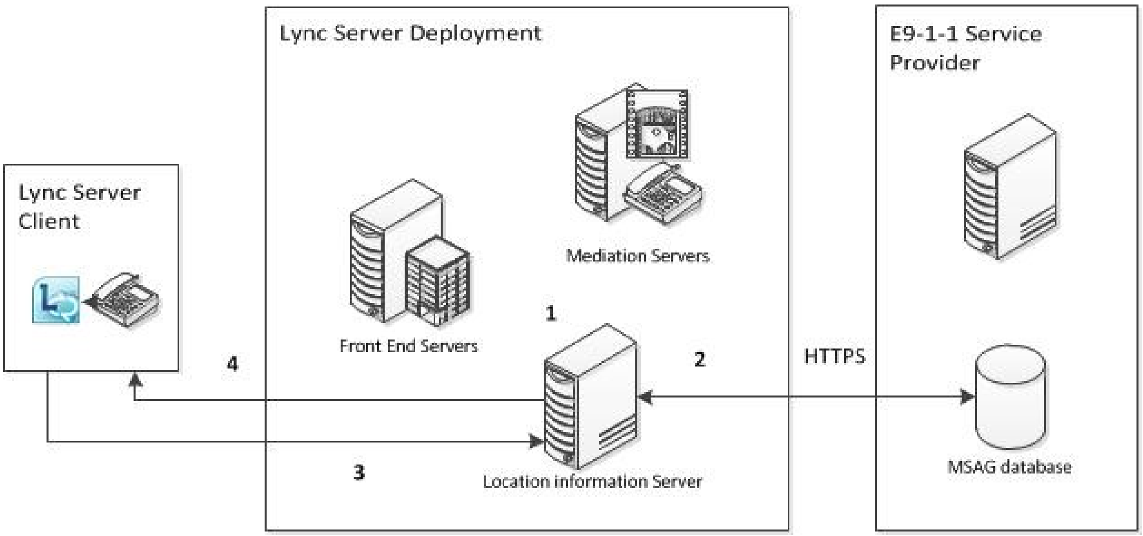
Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Overview of E9-1-1 >

Topic Last Modified: *2012-06-06*

In a Lync Server 2013 E9-1-1 deployment, each internally-connected Lync or Lync Phone Edition client actively acquires its own location. After SIP registration, the client furnishes all the network connectivity information that it knows about itself it in a location request to the Location Information service, which is a web service backed by a replicated SQL Server database. Each central site pool has a Location Information service, which uses the network information to query its records for a matching location. If there is a match, the Location Information service returns a location to the client. If there is not a match, the user may be prompted to enter a location manually (depending on location policy settings). The location data are transmitted back to the client in an Internet Engineering Task Force (IETF) standardized XML format called Presence Information Data Format Location Object (PIDF-LO).

The Lync Server client includes the PIDF-LO data as part of an emergency call, and this data is used by the E9-1-1 service provider to determine the appropriate PSAP and route the call to that PSAP along with the correct ESQK, which allows the PSAP dispatcher to obtain the caller’s location.

The following diagram shows how a Lync Server client acquires a location (except for the third-party client MAC address–based location method):



For a client to acquire a location, the following steps must take place:

1. The administrator populates the Location Information service database with the network wiremap (tables that map various types of network addresses to corresponding Emergency Response Locations (ERLs)).
2. If you use a SIP trunk E9-1-1 service provider, the administrator validates the civic address portions of the ERLs against a Master Street Address Guide (MSAG) database maintained by the E9-1-1 service provider. If you use an ELIN gateway, the administrator ensures that the PSTN carrier uploads the ELINs to the Automatic Location Identification (ALI) database.
3. During registration or whenever a network change occurs, an internally-connected client sends a location request that contains the client's discovered network addresses to the Location Information service.
4. The Location Information service queries its published records for a location, and, if a match is found, returns the ERL to the client in PIDF-LO format.

1.3.10.9.1.2 Routing E9-1-1 Calls by Using a SIP Trunk

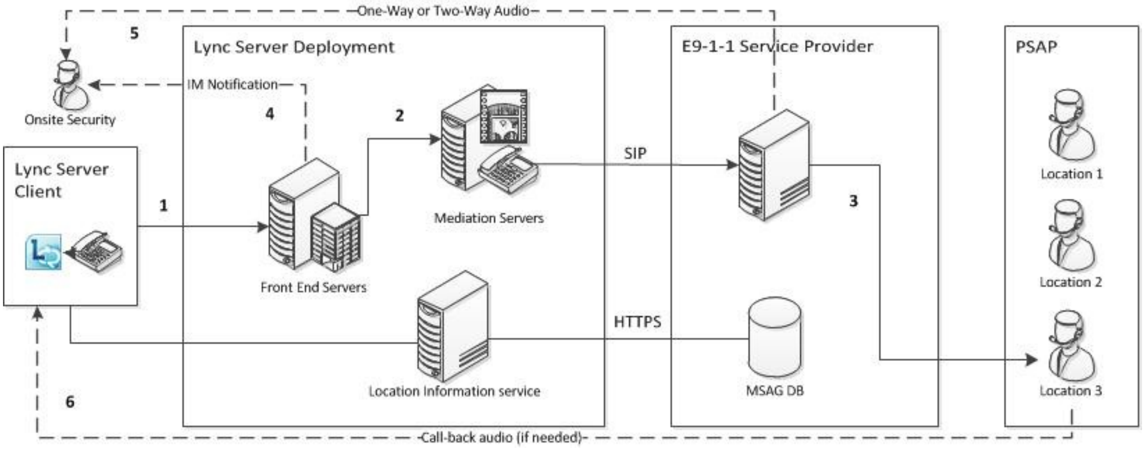
Routing E9-1-1 Calls by Using a SIP Trunk

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Overview of E9-1-1 >

Topic Last Modified: *2012-09-29*

Using a SIP trunk to connect to a qualified E9-1-1 service provider is one way that you can deploy E9-1-1. For details about using an ELIN gateway to connect to a public switched telephone network (PSTN)-based E9-1-1 service provider, see Routing E9-1-1 Calls by Using an ELIN Gateway.

The following diagram shows how an emergency call is routed from Lync Server to the Public Safety Answering Point (PSAP) when you use a SIP trunk and qualified E9-1-1 service provider.



When an emergency call is placed from a compatible Lync Server client:

1. A SIP INVITE that contains the location, the caller's callback number, and the (optional) Notification URL and conference callback number is routed to Lync Server.
2. Lync Server matches the emergency number and routes the call (based on the **PSTN Usage** value that is defined in the applicable location policy) to a Mediation Server, and from there, over a SIP trunk to the E9-1-1 service provider.
3. The E9-1-1 service provider routes the emergency call to the correct PSAP based on the location that is provided with the call. When the client includes a validated Emergency Response Location (ERL) with the emergency call, the provider automatically routes the call to the appropriate PSAP. If the location was manually entered by the user, the Emergency Call Response Center (ECRC) first verbally verifies the accuracy of the location with the caller before routing the emergency call to the PSAP.
4. If you configured the location policy for notifications, one or more of your organization’s security officers are sent a special Lync emergency notification instant message. This message always pops up on the security officers’ screen(s) and contains the caller’s name, phone number, time, and location, enabling security personnel to quickly respond to the emergency caller by using an instant message or voice.
5. If you configured the location policy for conferencing and it is supported by the E9-1-1 service provider, an internal Security Desk is conferenced into the call with either one-way audio or two-way audio.
6. If the call is broken prematurely, the PSAP uses the callback number to contact the caller directly.

Routing E9-1-1 Calls by Using an ELIN Gateway

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Overview of E9-1-1 >

Topic Last Modified: *2013-02-05*

Some partners in the Unified Communications Open Interoperability Program provide qualified Emergency Location Identification Number (ELIN)-capable gateways, which can serve as an alternative to a SIP trunk connection to a qualified E9-1-1 service provider. ELIN gateways support ISDN or Centralized Automatic Message Accounting (CAMA) connectivity to public switched telephone network (PSTN)-based E9-1-1 services. For details about partners who provide ELIN gateways and links to their documentation, see http://go.microsoft.com/fwlink/p/?LinkId=248425.

Like SIP trunk connections to E9-1-1 service providers, ELIN gateways also provide the means of routing an emergency call to the caller's most appropriate Public Safety Answering Point (PSAP), but these gateways use an ELIN as the location identifier. You define ELINs for each Emergency Response Location (ERL) in your organization (for details, see Managing Locations for ELIN Gateways).

When you use an ELIN gateway for emergency calls, you use the same Lync Server E9-1-1 infrastructure that you would use for a SIP trunk connection. That is, the Location Information service database provides the location to the Lync Server client, and the location policy enables the feature and defines the routing. With an ELIN gateway, however, you need to add the ELINs to the Location Information service database and have your PSTN carrier upload them to the Automatic Location Identification (ALI) database.

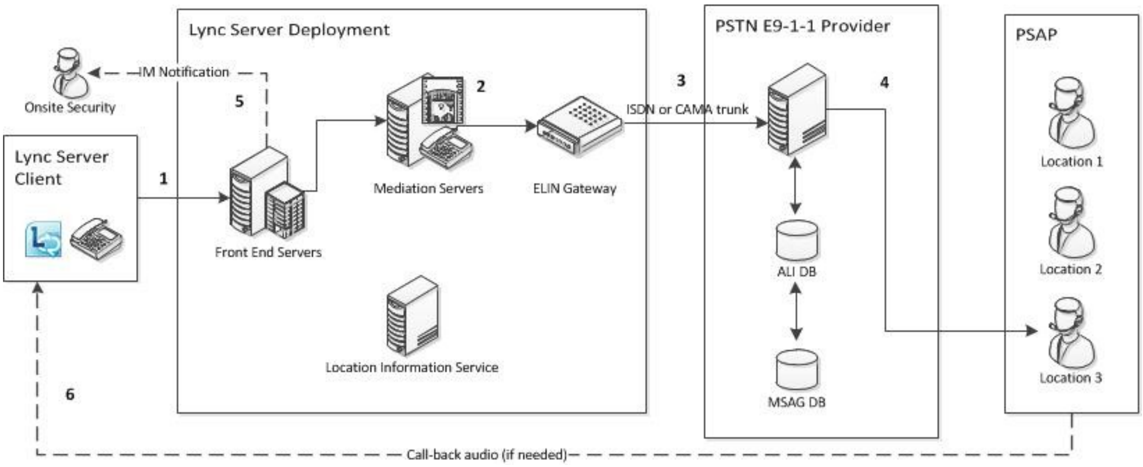
When a Lync client obtains its location from the Location Information service, the location includes the ELIN. During an emergency call, the ELIN is included with the location sent to the ELIN gateway. The ELIN gateway identifies the call as an emergency call and swaps the calling party's number with the ELIN. The ELIN gateway then routes the call to the PSTN with the ELIN as the calling number. The PSTN E9-1-1 provider looks up the ELIN in the ALI database, which is a companion database to the Master Street Address Guide (MSAG) database. The PSTN then sends the call to the most appropriate PSAP based on the ALI lookup, and the PSAP sends first responders to the caller's location based on the ALI lookup. The calling number is cached on the ELIN gateway for a predefined amount of time for callbacks. During a callback, the PSAP reaches the ELIN gateway, which swaps the ELIN for the caller's direct inward dialing (DID) number.

ELIN gateways support emergency calls only from within your organization's network. They do not support emergency calls made from outside your network.

Note:

For details about using a SIP trunk connection for emergency calls, see Routing E9-1-1 Calls by Using a SIP Trunk.

The following diagram shows how an emergency call is routed from Lync Server to the PSAP when you use an ELIN gateway.



1. A SIP INVITE containing the location, the caller's callback number, and the (optional) Notification URL and conference callback number is routed to Lync Server.
2. Lync Server matches the emergency number and then routes the call (based on the **PSTN Usage** value defined in the applicable location policy) to a Mediation Server, and from there to an ELIN gateway.
3. The ELIN gateway routes the call over an ISDN or CAMA trunk to the PSTN.
4. The PSTN identifies the call as an emergency call and routes it to an E9-1-1 selective router in the network. The E9-1-1 selective router looks up the caller's number in the ALI database to obtain the geographical location. The E9-1-1 selective router sends the call to the most appropriate PSAP based on the location information that was retrieved from the ALI database.
5. If you configured the location policy for notifications, one or more of your organization's security officers are sent a special Lync emergency notification instant message. This message always pops up on the security officers' screen(s) and contains the caller's name, phone number, time, and location, enabling security personnel to quickly respond to the emergency caller by using an instant message or voice.
6. If the call is broken prematurely, the PSAP uses the ELIN to contact the caller directly. The ELIN gateway swaps the ELIN for the caller's DID.

1.3.10.9.2 Defining Your Requirements for Emergency Calls

Defining Your Requirements for Emergency Calls

Planning > Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) >

Topic Last Modified: *2012-06-06*

Before you begin a Microsoft Lync Server 2013 E9-1-1 deployment, you should first be able to answer the questions detailed in the following sections. The planning you need to do depends on the type of E9-1-1 solution that you choose to deploy—a SIP trunk E9-1-1 service provider or an Emergency Location Identification Number (ELIN) gateway. The following table identifies the sections in this planning workbook that you'll need to review for each of those solutions.

Planning Steps by Type of E9-1-1 Solution

SIP trunk service provider	ELIN gateway
Defining the Scope of the E9-1-1 Deployment	Defining the Scope of the E9-1-1 Deployment

Defining the Network Elements Used to Determine Location	Defining the Network Elements Used to Determine Location
Enabling Users for E9-1-1	Enabling Users for E9-1-1
Managing Locations for SIP Trunk Service Providers	Managing Locations for ELIN Gateways
Defining the User Experience for Manually Acquiring a Location	Defining the User Experience for Manually Acquiring a Location
Designing the SIP Trunk for E9-1-1	Including the Security Desk
Including the Security Desk	Defining the Location Policy
Choosing an E9-1-1 Service Provider	Assigning Location Policy Scope
Defining the Location Policy	
Assigning Location Policy Scope	

- Defining the Scope of the E9-1-1 Deployment
- Defining the Network Elements Used to Determine Location
- Enabling Users for E9-1-1
- Managing Locations for SIP Trunk Service Providers
- Managing Locations for ELIN Gateways
- Defining the User Experience for Manually Acquiring a Location
- Designing the SIP Trunk for E9-1-1
- Including the Security Desk
- Choosing an E9-1-1 Service Provider
- Defining the Location Policy
- Assigning Location Policy Scope

1.3.10.9.2.1 Defining the Scope of the E9-1-1 Deployment

Defining the Scope of the E9-1-1 Deployment

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-06-06*

Before you configure Microsoft Lync Server 2013 for E9-1-1, you need to plan your E9-1-1 deployment. Some of the questions to consider include:

What are your organization’s policy and legal obligations with regard to E9-1-1?

E9-1-1 legal requirements for PBXs (called Multi-line Telephone Systems, or MLTS, in E9-1-1 parlance) differ from state to state. You should consult with your legal team to understand the obligations that may apply to your deployment of Lync Server in your relevant geographies.

What areas within your enterprise need to be enabled for E9-1-1?

You can enable E9-1-1 for the entire enterprise or for selected locations. For example, you may have varying E9-1-1 requirements for offices in different states, or you may want to exclude sites outside the U.S.

How will you deploy E9-1-1 to branch sites?

Voice resiliency is an important concept to understand when deploying E9-1-1 at a branch site. If you have centralized E-9-1-1 SIP trunks and a WAN outage occurs, clients signing in may not be able to obtain a location from Location Information service or to connect to the emergency services service provider. Lync Server provides several strategies for handling voice resiliency in branch offices, including: having resilient data networks, deploying a SIP trunk at each branch, or pushing emergency calls out to the local gateway during outages. For details, see Planning for Branch-Site Voice Resiliency.

Will you enable E9-1-1 for users working outside the network?

Automatic location acquisition is available only for clients located inside the organization’s network, so your organization needs to decide whether it will support E9-1-1 calls made from Lync clients while off-premises. For example, will you enable users to place emergency calls if they are working from home or from a customer site? If a client is located outside the enterprise network, the client can be configured to prompt the user for a location. However, because these user-provided locations cannot be prevalidated against the Master Street Address Guide (MSAG), the emergency services service provider dispatcher will need to confirm the validity of the location verbally with the caller before routing the call to the Public Safety Answering Point (PSAP).

Note:

Lync clients of users who connect to your organization’s network by using VPN can pick up internal IP address information, but because these addresses cannot be used to identify the user’s actual location, it is essential that VPN subnets are excluded from the Location Information service.

Do you want to provide emergency call routing to sites outside the U.S.?

You may want to provide emergency routing to areas of your company not served by an emergency services service provider (for example, international locations). To do this, create a new site, and then assign voice policies to the sites that refer to a PSTN usage that routes the call through the local PSTN gateway.

1.3.10.9.2.2 Defining the Network Elements Used to Determine Location

Defining the Network Elements Used to Determine Location

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-10-29*

If you are setting up your Lync Server infrastructure to support automatic client location detection, you first need to decide which network elements you are going to use to map callers to locations. In Lync Server 2013, you can associate the following Layer 2 and Layer 3 network elements with locations:

- Wireless access point (WAP) Basic Service Set Identification (BSSID) addresses (Layer 2)
- LLDP switch port (Layer 2)
- LLDP switch chassis IDs (Layer 2)
- IP subnets (Layer 3)
- Client MAC addresses (Layer 2)

The network elements are listed in order of precedence. If a client can be located by using more than one network element, Lync Server uses the order of precedence to determine which mechanism to use.

The following sections provide more details for using each network element.

Important:

When you use network elements to map callers to locations, it is of utmost importance that you keep the Location Information service database up-to-date. For example, if you add or change a network element, such as adding a WAP, you must delete the old entry and add the new entry in the location database.

Wireless Access Point

When a client connects to the network wirelessly, the location request uses the BSSID address of the WAP to determine its location. If the client is roaming, the WAP indicated may not be the closest one, and it’s even possible to pick up a WAP that is on a different floor of the building. To indicate that the location is approximate, you can prepend the location value with a **Near** or **Close to** descriptor.

This location method assumes that the BSSID of each WAP is static. However, if your WAP vendor uses dynamically-assigned BSSIDs, the BSSID that is obtained from a WAP could change (this can happen following a WAP configuration change), and wireless clients could be left in a situation where they don’t receive a location. To prevent this possibility, you need to populate the Location Information service database with ERLs for all possible BSSID addresses used by each WAP.

LLDP Ports and Switches

Managed Ethernet switches that support Link Layer Discovery Protocol-Media Endpoint Discover (LLDP-MED) can advertise their identity and port information to LLDP-MED compatible clients, which then can be queried against the location database to provide the location of the device. You can associate ERLs solely on the switch chassis ID, or you can map them down to the port level.

Note:

Lync Server 2013 supports using LLDP-MED for determining locations only of Lync Phone Edition devices and Lync 2013 running on Windows 8. If you need to use switch-level Layer 2 data to determine the location of other wired PC-based Lync clients, you need to use the client MAC address method.

Subnet

Layer 3 IP subnets provide a mechanism supported by all Lync Server clients that can be used to automatically detect client location. Using IP subnets is the easiest location method to configure and manage wired clients. Before you decide to use subnets, however, use the following questions to help determine if the location specificity of the subnet is sufficiently fine to accurately locate a client:

- Do one or more client subnets cover multiple floors?
- Do one or more subnets cover more than one building?
- How much floor space is covered by each client subnet?

If the subnet covers too broad an area, you may need to use another mechanism to locate clients. However, if at all practical, we recommend that customers reorganize their IP subnetting to meet the ERL location specificity requirements rather than incurring the cost and complexity of third-party SNMP-based solutions.

Client MAC Address

To use a client computer's MAC address to locate a caller, you need managed Ethernet switches, and you must deploy a third-party SNMP solution that can discover the MAC addresses of Lync clients connected to (or through) those switches. The SNMP solution continually polls the managed switches to get the current mappings of the endpoint MAC addresses connected to each port and obtains the corresponding port IDs. During a Lync client's request to the Location Information service, the Location Information service queries the third-party application by using the client's MAC address, and then returns any matching switch IP addresses and port IDs. The Location Information service uses this information to query its published Layer 2 wiremap for a matching record and returns the location to the client. If you use this option, make sure that the switch port identifiers are consistent between the SNMP application and the published location database records.

Note:

Some third-party SNMP solutions can support unmanaged access switches; if the switch that services the Lync client is unmanaged but has an uplink to a managed distribution switch, the managed switch can report back to the SNMP application the MAC addresses of the clients connected to the access switch. This information enables the Location Information service to identify the location of the user. However, it is possible to assign only a single ERL to all ports on the unmanaged switch, so the location specificity is available only at the chassis level of the access switch, not the port level.

1.3.10.9.2.3 Enabling Users for E9-1-1

Enabling Users for E9-1-1

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-06-06*

During client registration, Lync Server uses a location policy to configure the E9-1-1 properties for Enterprise Voice-enabled users. This policy contains the settings that define how E9-1-1 is implemented. For example, the location policy contains information such as the emergency dial string, and whether or not a user is required to manually enter a location if the Location Information service does not automatically provide one. For a complete definition of a location policy, see Defining the Location Policy.

Lync Server can assign a location policy to clients based on subnet, or to users based on a global, per-site, or per-user policy. To help decide how you will enable users, you should first answer the following questions.

Do you plan to enable all users, or limit support to specific geographic areas of the enterprise?

You can assign a location to all users in your enterprise by using a global location policy. However, by assigning a location policy to a Lync Server network site and then adding subnets to the site, you can limit E9-1-1 support to selected locations within the enterprise and specify E9-1-1 routing behavior on a per-site basis.

Do you plan to enable individual users through a user policy?

You can assign location policies directly to specific users or common area phone contact objects if you want to customize their E9-1-1 support.

When clients roam outside the network or connect from an undefined subnet, should the clients still be enabled for E9-1-1?

If users are assigned a global, site, or per-user location policy, they can be required to manually enter a location into the client if the client is not located within a defined subnet or no location has been found by the Location Information service. For details, see Defining the User Experience for Manually Acquiring a Location.

Managing Locations for SIP Trunk Service Providers

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-10-02*

To configure Lync Server to automatically locate clients within a network, you need to either populate the Location Information service database with a network wiremap and publish the locations, or link to an external database that already contains the correct mappings. As part of this process, you need to validate the civic addresses of the locations with your E9-1-1 service provider. For details, see Configure the Location Database in the Deployment documentation.

You populate the Location Information service database with an Emergency Response Location (ERL), which consists of a civic address and the specific address within a building. The Location Information service **Location** field, which is the specific location within a building, has a maximum length of 20 characters (including spaces). Within that limited length, try to include the following:

- An easy-to-understand name that identifies the location of the 911 caller to help ensure that emergency responders find the specific location promptly when they arrive at the civic address. This location name may include a building number, floor number, wing designator, room number, and so on. Avoid nicknames known only to employees, which might cause emergency responders to go to the wrong location.
- A location identifier that helps users to easily see that their Lync client picked up the correct location. The Lync client automatically concatenates and displays the discovered **Location** and **City** fields in its header. A good practice is to add the street address of the building to each location identifier (for example, "1st Floor <street number>"). Without the street address, a generic location identifier such as "1st Floor" could apply to any building in the city.
- If the location is approximate because it’s determined by a wireless access point, you can add the word **Near** (for example, "Near 1st Floor 1234").

Note:

Locations added to the central location database are not available to the client until they are published by using a Lync Server Management Shell command and are replicated to the pool's local stores. For details, see Publish the Location Database in the Deployment documentation.

The following sections discuss considerations that you need to take into account when populating and maintaining the location database.

Populating the Location Database

The following questions can help you determine how to populate the location database.

What process will you use to populate the location database?

Where does the data exist, and what steps do you need to take to convert the data into the format required by the location database? Will you add locations individually, or in bulk, by using a CSV file?

Do you have a third party database that already contains a mapping of locations?

By using Lync Server's Secondary Location Information service option to connect to a third-party database, you can group and manage locations by using an offline platform. A benefit to this approach is that in addition to associating locations to network identifiers, you can associate locations to a user. This means that the Location Information service can return multiple addresses, originating from the

Secondary Location Information service, to a Lync Server client. The user can then choose the most appropriate location.

To integrate with the Location Information service, the third-party database must follow the Lync Server Location Request/Response schema. For details, see "[MS-E911WS]: Web Service for E911 Support Protocol Specification" at http://go.microsoft.com/fwlink/p/?linkid=213819. For details about deploying a Secondary Location Information service, see Configure a Secondary Location Information Service in the Deployment documentation.

For details about populating the location database, see Configure the Location Database in the Deployment documentation.

Maintaining the Location Database

After you populate the location database, you need to develop a strategy for updating the database as the network configuration changes. The following questions will help you determine how to maintain the location database.

How will you update the location database?

There are several scenarios that require an update to the location database, including adding WAPs, office recabling (resulting in different switch assignments), and subnet expansion. Will you directly update each individual location, or will you perform a bulk update of all the locations by using a CSV file?

Will you use an SNMP application to match Lync client MAC addresses to port and switch identifiers?

If you use an SNMP application, you need to develop a manual process for keeping the switch chassis and port information consistent between the SNMP application and the location database. If the SNMP application returns a chassis IP address or port ID that is not included in the database, the Location Information service will not be able to return a location to the client.

1.3.10.9.2.5 Managing Locations for ELIN Gateways

Managing Locations for ELIN Gateways

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-10-02*

To have Lync Server automatically provide locations for clients within a network, you need to perform the following tasks:

- Populate the Location Information service database with a network wiremap, and include the Emergency Location Identification Numbers (ELINs) in the CompanyName field.
- Publish the locations so that they are available for clients in your network.
- Upload the ELINs to your public switched telephone network (PSTN) carrier's Automatic Location Identification (ALI) database.

For details about how to perform these tasks, see Configure the Location Database in the Deployment documentation.

Note:

Locations added to the central location database are not available to the client until they have been published by using a Lync Server Management Shell command and are replicated to the pool's local stores. For details, see Publish the Location Database in the Deployment documentation.

This section describes things to consider as you plan to update and maintain the location database.

Planning Emergency Locations

When you use ELIN gateways, you populate the Location Information service database with the civic address, a specific location within a building, and at least one ELIN for each location . During the planning phase, it is a good idea to decide how you want to name the locations and how you want to assign ELINs.

Planning Location Names

The Location Information service **Location** field, which holds the specific location within a building, has a maximum length of 20 characters (including spaces). Within that limited length, try to include the following:

- An easy-to-understand name that identifies the location of the 911 caller to help ensure that emergency responders find the specific location promptly when they arrive at the civic address. This location name may include a building number, floor number, wing designator, room number, and so on. Avoid nicknames that are known only to employees, which might cause emergency responders to go to the wrong location.
- A location identifier that helps users to easily see that their Lync client picked up the correct location. The Lync client automatically concatenates and displays the discovered **Location** and **City** fields in its header. A good practice is to add the street address of the building to each location identifier (for example, "1st Floor <street number>"). Without the street address, a generic location identifier such as "1st Floor" could apply to any building in the city.
- If the location is approximate because it’s determined by a wireless access point, you may want to add the word **Near** (for example, "Near 1st Floor 1234").

Planning ELINs

After you decide how you want to divide your building space into locations, you need to decide how many ELINs to assign to each location. For example, in a multifloor or multitenant building, different areas in the building can be assigned different emergency zones. Typically, each floor in a building is designated as a location. Each location is then assigned one or more ELINs, which are used as the calling number(s) during an emergency call. Contact your PSTN carrier for phone numbers that you can use for ELINs. The following table provides an example of locations for a specific street address.

Sample Location and ELIN Assignments

Building Area	Location	ELIN
First floor	1	425-555-0100
Second floor	2	425-555-0111
Third floor	3	425-555-0123

The locations you define should meet the following requirements:

- Comply with local and national/regional regulations in terms of maximum area per location and number of locations per street address.
- Are specific enough to make it easy to locate the emergency caller.

Populating the Location Database

The following questions will help you determine how to will populate the location database.

What process will you use to populate the location database?

Where does the data exist, and what steps do you need to take to convert the data into the format required by the location database? Will you add locations individually, or in bulk, by using a CSV file?

Do you have a third party database that already contains a mapping of locations?

By using Lync Server's Secondary Location Information service option to connect to a third-party database, you can group and manage locations by using an offline platform. A benefit to this approach is that in addition to associating locations to network identifiers, you can associate locations to a user. This means that the Location Information service can return multiple addresses, originating from the Secondary Location Information service, to a Lync Server client. The user can then choose the most appropriate location.

To integrate with the Location Information service, the third-party database must follow the Lync Server Location Request/Response schema. For details, see http://go.microsoft.com/fwlink/p/?linkid=213819. For details about deploying a Secondary Location Information service, see Configure a Secondary Location Information Service in the Deployment documentation.

For details about populating the location database, see Configure the Location Database in the Deployment documentation.

Maintaining the Location Database

After you populate the location database, you need to develop a strategy for updating the database as the network configuration changes. The following questions will help you determine how to maintain the location database.

How will you update the location database?

There are several scenarios that require an update to the location database, including adding wireless access points (WAPs), office recabling (resulting in different switch assignments), and subnet expansion. Will you directly update each individual location, or will you perform a bulk update of all the locations by using a CSV file?

Will you use an SNMP application to match Lync client MAC addresses to port and switch identifiers?

If you use an SNMP application, you need to develop a manual process for keeping the switch chassis and port information consistent between the SNMP application and the location database. If the SNMP application returns a chassis IP address or port ID that is not included in the database, the Location Information service will not be able to return a location to the client.

1.3.10.9.2.6 Defining the User Experience for Manually Acquiring a Location

Defining the User Experience for Manually Acquiring a Location

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-10-03*

If a client is located outside the network, or in an undefined subnet, the user can manually enter a location. But during an emergency call, the call will first be routed to a national/regional E9-1-1 Emergency Call Response Center (ECRC) dispatcher before being routed to a Public Safety Answering Point (PSAP). The ECRC will verbally query the caller for a location and then forward the call to the appropriate PSAP, based on the information provided.

Should users be prompted to enter a location when one is not automatically provided by the Location Information service?

For example, if a client is located in an undefined subnet, at home, in a hotel, or anywhere else outside the network, should the user be required to enter a location?

You can configure the **Location Required** setting in the location policy to define the client behavior. Setting this value to No means that the user will not be prompted for a location. Setting this value to Yes means that the user will be prompted for a location, but can dismiss the prompt. Setting this value to Disclaimer means that the user will be prompted for a location, and will be shown a disclaimer if they try to dismiss the prompt. In all cases, the user can continue to use the client as usual.

When a user manually enters a location, the location is mapped to the MAC address of the default gateway of the client's network, and is stored in a per-user table located on the client. When the user returns to any previously stored location, the Lync client automatically sets itself to that location.

Note:

You can modify only the current location of your client, but you can also delete any location stored in the local user's table.

1.3.10.9.2.7 Designing the SIP Trunk for E9-1-1

Designing the SIP Trunk for E9-1-1

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-10-03*

Lync Server uses SIP trunks to connect an emergency call to the E9-1-1 service provider. You can set up emergency service SIP trunks for E9-1-1 at one central site, at multiple central sites, or at each branch site. However, if the WAN link between the caller's site and the site that hosts the emergency service SIP trunk is unavailable, then a call placed by a user at the disconnected site will need a special phone usage record in the user's voice policy that will route the call to the ECRC through the local public switched telephone network (PSTN) gateway. The same is true if call admission control concurrent call limits are in effect.

Note:

There are two ways to implement a SIP trunk in a Lync Server environment:

- Use multihomed Mediation Servers that use their outward-facing publicly-routed interfaces to communicate with the SIP trunk provider.
- Use an on-premises Session Border Controller (SBC) to provide a secure demarcation point between the Mediation Servers and the SIP trunk provider's services.

If you choose the latter method, be sure that the SBC make and model that you choose has been certified and supports passing Presence Information Data Format Location Object (PIDF-LO) location data as part of its SIP INVITE. Otherwise, the calls will arrive at the emergency services service provider stripped of their location information. For details about certified SBCs, see "Infrastructure Qualified for Microsoft Lync" at http://go.microsoft.com/fwlink/p/?LinkId=248425.

E9-1-1 service providers supply you with access to a pair of SBCs for redundancy. You need to make several decisions regarding the Mediation Server topology and call routing configuration. Will you treat both SBCs as equal peers and use round-robin routing for calls between them, or will you designate one SBC as primary and the other as secondary?

For details about deploying a SIP trunk in Lync Server, see How Do I Implement SIP Trunking?. The following questions will help you decide how to deploy the SIP trunks for

E9-1-1.

Should you deploy the SIP trunk over a dedicated leased or a shared internet connection?

It is important that emergency calls always connect. A dedicated line provides a connection that will not be preempted by other traffic on the network, and gives you the ability to implement Quality of Service (QoS). Remember that if you are connecting to emergency services service providers over the public Internet and you need to guarantee the confidentiality of emergency calls, IPSec encryption is required.

Is your E9-1-1 deployment designed for disaster tolerance?

Because this is an emergency solution, resiliency is important. Deploy your primary and secondary Mediation Servers and SIP trunks in disaster tolerant locations. It is a good idea to deploy your primary Mediation Server closest to the users that it is supporting, and route failover calls through the secondary Mediation Server (located in a different geographic location).

Should you deploy a separate SIP trunk for each branch office?

Lync Server provides several strategies for handling voice resiliency in branch offices, including: having resilient data networks, deploying a SIP trunk at each branch, or pushing calls out to the local gateway during outages. For details, see Branch Site SIP Trunking.

Is call admission control (CAC) enabled?

Lync Server does not handle emergency calls any differently than an ordinary call. For this reason, bandwidth management, or call admission control (CAC), can have a negative impact on an E9-1-1 configuration. Emergency calls will be blocked or routed to the local PSTN gateway if a CAC is enabled and the configured limit is exceeded on a link where emergency calls are being routed. As indicated earlier in this topic, such calls will not have location data and must be manually routed to the ECRC.

1.3.10.9.2.8 Including the Security Desk

Including the Security Desk

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-10-02*

Your company may require the security desk to become involved in an emergency call. To help decide how to integrate the Security Desk into you E9-1-1 deployment, you should answer the following questions.

Do you want the security desk to be notified when there is an emergency call?

You can configure the location policy so that Lync Server sends instant messaging (IM) alerts to the Lync SIP addresses of one or more security personnel. These alerts contain the name, number, and location of the person placing the emergency call, and facilitate security personnel in assisting with the emergency situation.

Do you want to conference the security desk in on each emergency call?

If supported by the emergency services service provider, you can configure the location policy to include a callback number with each emergency call. This number is then used by the provider to conference your organization's security personnel into emergency calls. This conferencing can be configured in the location policy to be one-way (listen-only) or two-way (bidirectional).

Note:

If desired, you can configure different emergency personnel for each location policy. This allows you to customize the response for different areas within your company, or create different behavior for emergency calls that originate from inside as opposed to outside the network. You can use distribution groups to specify the personnel you want to notify.

1.3.10.9.2.9 Choosing an E9-1-1 Service Provider

Choosing an E9-1-1 Service Provider

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-06-06*

The E9-1-1 service provider routes emergency calls originating from Lync Server to the correct Public Safety Answering Point (PSAP) based on the location information contained within the call.

To support E9-1-1 as part of a Lync Server deployment, you must obtain E9-1-1 routing service from a Lync Open Interoperability Program qualified E9-1-1 service provider. Choose the provider that best fits your organizational requirements.

1.3.10.9.2.10 Defining the Location Policy

Defining the Location Policy

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-10-29*

Each location policy contains the following information:

Emergency Services Enabled

When this value is **Yes**, the client is enabled for E9-1-1. When a client registers, it attempts to acquire a location from the Location Information service and will include the location information as part of an emergency call.

Location Required

This setting is used only when **Emergence Services Enabled** is set to **Yes**.

You can configure the **Location Required** setting to define the client behavior. Setting the value to **No** means that the user will not be prompted for a location. Setting the value to **Yes** means that the user will be prompted for a location, but can dismiss the prompt. Setting the value to **Disclaimer** means that the user will be prompted for a location and also will be shown a disclaimer if they try to dismiss the prompt. In all cases, the user can continue to use the client.

Note:

The disclaimer text will not appear if a user manually entered a location before being enabled for E9-1-1. Updates to the disclaimer text will not be viewed by users that have already viewed the disclaimer.

Enhanced Emergency Service Disclaimer

This setting specifies the disclaimer that users see if they dismiss the prompt for a location. In Lync Server 2013, you can use location policy to set different disclaimers for different locales or different sets of users.

Note:

This location policy setting differs from Lync Server 2010, where you used the **Set-**

CsEnhancedEmergencyServiceDisclaimer cmdlet to set a global disclaimer for the entire organization. If a global disclaimer already exists, you need to specify that disclaimer in location policy. That is, Lync Server 2013 uses only disclaimers specified in location policy.

Emergency Dial String

This dial string (less the leading "+", but including any normalization done by the Lync user's Dial Plan) signifies that a call is an emergency call. The **Emergency Dial String** causes the client to include location and callback information with the call.

Note:

If your organization does not use an external line access prefix, you do not need to create a corresponding Dial Plan normalization rule that adds a "+" to the 911 string prior to sending the call to Outbound Routing on a Lync pool server; the "+" will be automatically prepended by the Lync client as a result of the location policy. However, if your site uses an external access prefix, you need to add a normalization rule to the applicable Dial Plan policy that strips the external access prefix and adds the "+". For example, if your location uses an external access prefix of 9 and a user dials 9 911 to place an emergency call, the client will use its Dial Plan policy to normalize this to +911 before the the dialed number is evaluated by the routes in the caller's location profile.

Emergency Dial String Masks

A semicolon-separated list of dial strings that is translated into the specified **Emergency Dial String**. For example, you may want to add 112, which is the emergency service number for most of Europe. A visiting Lync user from Europe may not know that 911 is the U.S. emergency number, but they can dial 112 and get the same result. As with the Emergency Dial String, do not include a "+" before each number, and if you use external line access codes, be sure there are normalization rules in the user's Dial Plan policy to strip off the access code digit.

PSTN Usage

The name of the PSTN Usage that contains the routing paths that determine which SIP trunk, PSTN gateway, or ELIN gateway emergency calls will go to.

Note:

Only one usage can be assigned to a location policy. This PSTN Usage overrides the PSTN Usages assigned to the user's voice policy, but applies only to calls placed to the Emergency Dial String or to one of the Emergency Dial String Masks.

Notification URI

Specifies one or more SIP URIs of the security personnel who receive an instant messaging (IM) notification when an emergency call is placed. Distribution groups are supported.

Conference URI

Specifies a direct inward dialing (DID) number (typically, a security desk number) that should be conferenced in when an emergency call is placed.

Conference Mode

Specifies if the conference URI will be conferenced into the emergency call by using one-way or two-way communication.

Location Refresh Interval

Specifies the amount of time (in hours) between client requests for a location update from the Location Information service. The value can be set to any value between 1 and 12. The default value is 4.

1.3.10.9.2.11 Assigning Location Policy Scope

Assigning Location Policy Scope

Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) > Defining Your Requirements for Emergency Calls >

Topic Last Modified: *2012-06-06*

As with other Lync Server policies, location policies can be assigned at multiple scope levels: global, site, and user. However, the scope of user-level location policies behaves a bit differently than with other Lync Server policies. Not only can per-user location policies be applied to endpoint objects (such as Users and Common Area Phone contact objects), they can also be applied to Lync Server network sites. Network sites are groupings of client subnets associated with a geographical location (but may not necessarily be all subnets in an entire central site or branch site). Any clients connected to the subnets in a network site automatically pick up the location policy assigned to that network site. In cases where a user-level location policy is assigned both to a user and to a network site, the network site-based location policy overrides any per-user policy setting.

Each network site has a location policy assigned to it, and each policy will have different PSTN Usages, Notification URIs, and Conference URIs values assigned to it.

Note:
The reason for this special policy scoping behavior is so that when a user homed on a pool at one office site visits another site and has to make an emergency call, the E9-1-1 call routing settings appropriate to that network site will apply no matter what pool or site the user is assigned to.

1.3.10.9.3 Deployment Checklist for E9-1-1

Deployment Checklist for E9-1-1

Planning > Planning for Enterprise Voice > Planning for Emergency Services (E9-1-1) >

Topic Last Modified: *2012-10-03*

To plan effectively for Enhanced 9-1-1 (E9-1-1), be sure to include the following deployment requirements:

- Prerequisites for deploying E9-1-1.
- Steps that are required to deploy E9-1-1.

Deployment Prerequisites for E9-1-1

Before you deploy E9-1-1, you must already have deployed your Lync Server internal servers, including a Central Management store, a Front End pool or a Standard Edition server, one or more Mediation Servers or Mediation Server pools, and Lync Server clients. In addition, an E9-1-1 deployment requires a SIP trunk to a qualified E9-1-1 service provider or an Emergency Location Identification Number (ELIN) gateway to your public switched telephone network (PSTN). Lync Server supports using E9-1-1 service providers only inside the United States.

Deployment Process

The following table provides an overview of the E9-1-1 deployment process. For details about deployment steps, see Configure Enhanced 9-1-1 in the Deployment documentation.

Phase	Steps	Roles	Deployment documentation
Configure voice usages, routes, and trunk configurations	1. Create a new PSTN usage record. This is the same name that is used for the **PSTN Usage** setting in the location policy. 2. Create or assign a voice route to the PSTN usage record created in the previous step and then point the gateway attribute to the E9-1-1 SIP trunk or ELIN gateway. 3. For a SIP trunk E9-1-1 service provider, set the trunk that will be handling E9-1-1 calls over the SIP to pass PIDF-LO data by using the **Set-CsTrunkConfiguration –EnablePIDFLOSupport** cmdlet. 4. Optionally, for a SIP trunk E9-1-1 service provider, create or assign a local PSTN route for calls that are not handled by the E9-1-1 service provider's SIP trunk. This route will be used if the connection to the E9-1-1 service provider is not available. If supported by your E9-1-1 service provider, assign a trunk configuration rule to the gateway that translates the 911 dial string into the direct inward dialing (DID) number of the national/ regional Emergency Call Response Center (ECRC).	CSVoiceAdmin	Configure an E9-1-1 Voice Route
Create location	1. Review the global	CSVoiceAdmin	Create Location

policies and assign them to users and subnets	location policy. 2. Create a location policy with a user-level scope; or, if the organization has more than one site with different emergency usages, create a location policy with a network-level scope. 3. Assign the location policy to network sites. 4. Add the appropriate subnets to the network site. 5. (Optional) Assign the location policy to user policies.	CSLocationAdmin (except for creating Location Policies)	Policies Add a Location Policy to a Network Site Associate Subnets with Network Sites for E9-1-1
Configure the location database	1. Populate the database with a mapping of network elements to locations. 2. For ELIN gateways, add the ELINs to the <CompanyName> column. 3. Configure the connection to the E9-1-1 service provider for validating addresses. 4. Validate the addresses with the E9-1-1 service provider. 5. Publish the updated database. 6. For ELIN gateways, upload the ELINs to your PSTN carrier's Automatic Location Identification (ALI) database.	CSVoiceAdmin CSLocationAdmin	Configure the Location Database
Configure Advanced Features (optional)	1. Configure the URL for the SNMP application. 2. Configure the URL for the location of the Secondary Location Information service.	CSVoiceAdmin	Configure an SNMP Application Configure a Secondary Location Information Service

1.3.10.10 Planning for Media Bypass

Planning for Media Bypass

See Also

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-09-21*

Media bypass refers to removing the Mediation Server from the media path whenever possible for calls whose signaling traverses the Mediation Server.

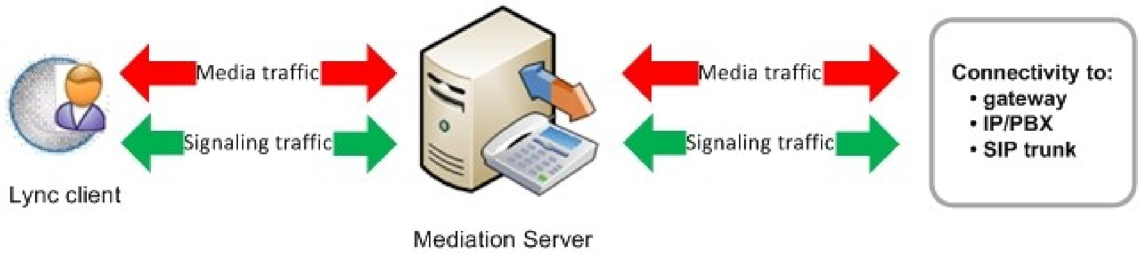
Media bypass can improve voice quality by reducing latency, needless translation, possibility of packet loss, and the number of points of potential failure. Scalability can be improved, because elimination of media processing for bypassed calls reduces the load on the Mediation Server. This reduction in load complements the ability of the Mediation Server to control multiple gateways.

Where a branch site without a Mediation Server is connected to a central site by one or more WAN links with constrained bandwidth, media bypass lowers the bandwidth requirement by allowing media from a client at a branch site to flow directly to its local gateway without first having to flow across the WAN link to a Mediation Server at the central site and back.

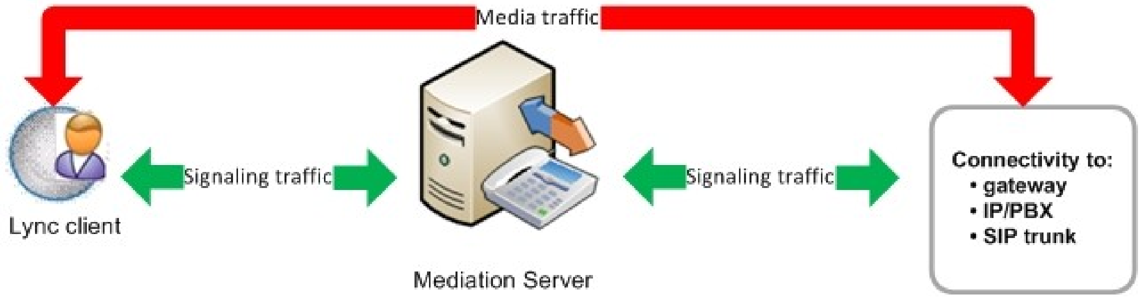
By relieving the Mediation Server from media processing, media bypass may also reduce the number of Mediation Servers that an Enterprise Voice infrastructure requires.

The following figure shows basic media and signaling pathways in topologies with and without media bypass.

No Media Bypass:



Media Bypass:



As a general rule, enable media bypass wherever possible.

- Overview of Media Bypass
- Media Bypass Modes
- Media Bypass and Call Admission Control

- Technical Requirements for Media Bypass

⊟Related Sections

Deploying Advanced Enterprise Voice Features

⊟See Also

Tasks

Configure a Trunk with Media Bypass

Concepts

Global Media Bypass Options

1.3.10.10.1 Overview of Media Bypass

Overview of Media Bypass

See Also

Planning > Planning for Enterprise Voice > Planning for Media Bypass >

Topic Last Modified: *2012-09-21*

Media bypass is useful when you want to minimize the number of Mediation Servers deployed. Typically, a Mediation Server pool will be deployed at a central site, and it will control gateways at branch sites. Enabling media bypass allows media for public switched telephone network (PSTN) calls from clients at branch sites to flow directly through the gateways at those sites. Lync Server 2013 outbound call routes and Enterprise Voice policies must be properly configured so that PSTN calls from clients at a branch site are routed to the appropriate gateway.

Wi-Fi networks typically experience more packet loss than wired networks. Recovery from this packet loss is not typically something that can be accommodated by gateways. Therefore, we recommend that you evaluate the quality of a Wi-Fi network before determining whether bypass should be enabled for a wireless subnet. There is a tradeoff in latency reduction versus recovery from packet loss to consider, as well. RTAudio, a codec which is available for calls that do not bypass the Mediation Server, is better suited for handling packet loss.

After your Enterprise Voice structure is in place, planning for media bypass is straightforward.

- If you have a centralized topology without WAN links to branch sites, you can enable global media bypass, because fine-tuned control is unnecessary.
- If you have a distributed topology that consists of one or more network regions and their affiliated branch sites, determine the following:
    - Whether your Mediation Server peers are able to support the capabilities required for media bypass.
    - Which sites in each network region are well-connected.
    - Which combination of media bypass and call admission control is appropriate for your network.

When you enable media bypass, a unique bypass ID is automatically generated for a network region, and for all network sites without bandwidth constraints within that region. Sites with bandwidth constraints within the region and sites connected to the region over WAN links with bandwidth constraints are each assigned their own unique bypass IDs.

When a user makes a call to the PSTN, the Mediation Server compares the bypass ID of the client subnet with the bypass ID of the gateway subnet. If the two bypass IDs match, media bypass is used for the call. If the bypass IDs do not match, media for the call must flow through the Mediation Server.

When a user receives a call from the PSTN, the user’s client compares its bypass ID to that of the PSTN gateway. If the two bypass IDs match, media flows directly from the gateway to the client, bypassing the Mediation Server.

Only Lync 2010 or above clients and devices support media bypass interactions with a Mediation Server.

◆**Important:**
In addition to enabling media bypass globally, you must enable media bypass individually on each PSTN trunk. If bypass is enabled globally, but is not enabled for a particular PSTN trunk, media bypass will not be invoked for any calls involving that PSTN trunk. In addition, when media bypass is set to **Use Site and Region Information**, you must associate all routable subnets with the sites in which they are located. If there are routable subnets within a site for which bypass is not wanted, these subnets should be grouped within a new site before you enable media bypass. Doing so will assure that the unroutable subnets are assigned a different bypass ID.

Concepts

Media Bypass Modes
Media Bypass and Call Admission Control
Technical Requirements for Media Bypass

1.3.10.10.2 Media Bypass Modes

Media Bypass Modes

See Also

Planning > Planning for Enterprise Voice > Planning for Media Bypass >

Topic Last Modified: *2012-10-05*

You must configure media bypass both globally and for each individual PSTN trunk. When enabling media bypass globally, you have two choices: **Always Bypass** and **Use Site and Region Information**.

As the name suggests, **Always Bypass** means that bypass will be attempted for all PSTN calls. **Always Bypass** is used for deployments where there is no need to enable call admission control, nor is there a need to specify detailed configuration information regarding when to attempt media bypass. Furthermore, **Always Bypass** is used when there is full connectivity between clients and PSTN gateways. In this configuration, all subnets are mapped to one and only one bypass ID, which is computed by the system.

With **Use Site and Region Information**, the bypass ID associated with site and region configuration is used to make the bypass decision. This configuration provides the flexibility to configure bypass for most common topologies, as it gives you fine-grained control over when bypass happens, in addition to supporting interactions with call admission control (CAC). The system tries to ease your task by automatically assigning bypass IDs as follows.

- The system automatically assigns a single unique bypass ID to each region.
- Any site connected to a region over a WAN link without bandwidth constraints inherits the same bypass ID as the region.
- A site associated with the region over a WAN link with constrained bandwidth is assigned a different bypass ID from that of the region.
- Subnets associated with each site inherit the bypass ID for that site.

Concepts

Overview of Media Bypass
Media Bypass and Call Admission Control
Technical Requirements for Media Bypass

Media Bypass and Call Admission Control

See Also

Planning > Planning for Enterprise Voice > Planning for Media Bypass >

Topic Last Modified: *2012-10-05*

Media bypass and call admission control (CAC) work together to manage bandwidth control for call media. Media bypass facilitates media flow over well-connected links; CAC manages traffic on links with bandwidth constraints. Because Media Bypass and CAC are mutually exclusive, you must be mindful of one when planning for the other. The following combinations are supported:

- CAC and Media Bypass are both enabled. Media Bypass must be set to **Use Site and Region Information**. This site and region information is the same as that used for CAC.

  If you enable CAC, you cannot select **Always Bypass**, and vice-versa, because the two configurations are mutually exclusive. That is, only one of the two will apply to any given PSTN call. First, a check is made to determine if media bypass applies to the call. If it does, then CAC is not used. This makes sense, because if a call is eligible for bypass, it is by definition using a connection where CAC is not needed. If bypass cannot be applied to the call (that is, if the client’s and gateway’s bypass IDs do not match), then CAC is applied to the call.

- CAC not enabled and Media Bypass set to **Always Bypass**.

  In this configuration, both client and trunk subnets are mapped to one and only one bypass ID, which is computed by the system.

- CAC not enabled and Media Bypass set to **Use Site and Region Information**.

  Where **Use Site and Region Information** is enabled, bypass determination works essentially the same way, regardless of whether CAC is enabled or not. That is, for any given PSTN call, the client’s subnet is mapped to a particular site, and the bypass ID for that subnet is extracted. Similarly, the gateway’s subnet is mapped to a particular site, and the bypass ID for that subnet is extracted. Only if the two bypass IDs are identical will bypass happen for the call. If they are not identical, media bypass will not occur.

  Even though CAC is disabled globally, bandwidth policy needs to be defined for each site and link if you want to use site-and-region configuration to control the bypass decision. The actual value of the bandwidth constraint or its modality doesn’t matter. The ultimate goal is to have the system automatically calculate different bypass IDs to associate with different locales that are not well connected. Defining a bandwidth constraint by definition means a link is not well connected.

- CAC is enabled and media bypass is not enabled. This would apply only where all gateways and IP-PBXs are not well connected or do not meet other requirements for media bypass. For details about requirements for media bypass, see Technical Requirements for Media Bypass.

Concepts

Overview of Media Bypass
Media Bypass Modes

Technical Requirements for Media Bypass

1.3.10.10.4 Technical Requirements for Media Bypass

Technical Requirements for Media Bypass

See Also

Planning > Planning for Enterprise Voice > Planning for Media Bypass >

Topic Last Modified: *2012-09-21*

For each call to the PSTN, the Mediation Server determines whether media from the Lync endpoint of origin can be sent directly to a Mediation Server peer without traversing the Mediation Server. The peer can be a PSTN gateway, IP-PBX, or Session Border Controller (SBC) at an Internet telephony service provider (ITSP) that is associated with the trunk between the Mediation Server where the call is routed.

Media bypass can be employed when the following requirements are met:

- A Mediation Server peer must support the necessary capabilities for media bypass, the most important being the ability to handle multiple forked responses (known as “early dialogs”). Contact the manufacturer of your gateway or PBX, or your ITSP, to obtain the value for the maximum number of early dialogs that the gateway, PBX, or SBC can accept.
- The Mediation Server peer must accept media traffic directly from Lync endpoints. Many ITSPs allow their SBC to receive traffic only from the Mediation Server. Contact your ITSP to determine whether its SBC accepts media traffic directly from Lync endpoints.
- Lync clients and a Mediation Server peer must be well connected, meaning that they are either located in the same network region or at network sites that connect to the region over WAN links that have no bandwidth constraints

Concepts

Media Bypass Modes
Media Bypass and Call Admission Control

1.3.10.11 Planning for Private Telephone Lines

Planning for Private Telephone Lines

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2013-02-11*

Lync Server 2013 introduces the ability to give users a second, private telephone line in addition to their primary telephone line. Private telephone lines are often assigned to executives and others who want an unlisted telephone number at which they can be reached directly.

Private telephone lines can only be configured with the Lync Server Management Shell. You cannot configure private telephone lines with the Lync Server Control Panel. Private telephone lines should be configured only in deployments of Lync Server and not in mixed deployments.

Characteristics of Private Telephone Lines

Although the concept of a second, private telephone line is fundamentally simple, it is important to understand the characteristics of private lines and the ways in which they are similar to and different from users’ primary telephone lines.

General Characteristics of Private Telephone Lines

- A user can have only one private telephone line.
- A user with a private telephone line has only one voice mailbox and receives missed call notifications at a single email address.
- A user with a private telephone line does not have a second SIP address, and a second, private telephone line does not give a user a second presence on the network (such as a second instant messaging identity).
- Private telephone lines are available for on-premises deployments only. They are not available with hosted deployments of Lync Server.

How Private Telephone Lines Differ from Primary Telephone Lines

- The telephone numbers for private telephone lines do not appear in the telephone directories or Contacts lists that are derived from Active Directory Domain Services.
- None of the following features are available with a private telephone line: call forwarding, team call, delegation, team ring, Group Call Pickup, and Response Group application.
- Calls to a private telephone line have a special ring, and the system notification for the call tells the user that the incoming call is on his or her private line.
- Calls to the private telephone line always ring through. They do not follow "do not disturb" rules.
- Private telephone lines are inbound only and cannot be used to make outgoing calls. When a user with a private telephone line makes a call, the call originates from the user’s primary telephone line and does not hide the user’s name or the user’s primary telephone number from the person called.

How Private Telephone Lines Are Similar to Primary Telephone Lines

- Unanswered calls to a private telephone line are routed to the same voice mail inbox as for the primary telephone line (if voice mail is enabled).
- Call park and call pickup work with private telephone lines in exactly the same manner as they do with the user’s primary telephone line.
- When simultaneous ringing is enabled on a user’s primary telephone line, it is also enabled on the private telephone line.
- The telephone number for a private telephone line is recorded in the call detail record in the same manner as the telephone number for a user’s primary telephone line, but with an indication that it is a private telephone number.
- After a user answers a call on a private telephone line, the call is treated the same as a call on the user’s primary telephone line. For example, if a user who receives a call on a private telephone line forwards the call or invites others to a conference call, the user’s name appears in Lync 2013, and the telephone number for the user’s primary telephone line appears in caller ID.
- A user can deflect a call (redirect the call to another destination, such as a mobile phone or home phone, before answering) from the private telephone line in the same manner as with a primary telephone line.

Note:

When a call to a private line is routed to an alternate telephone number, the telephone number for the private telephone line is made available to the alternate telephone number and can be displayed in the logs for that number.

Note:

Calls from a conference to the private telephone line will not have a *private-line* indication in the incoming system notification.

Administering Private Telephone Lines

In addition to the technical aspects of creating and managing private telephone lines, you will need to establish administrative procedures for them. This includes determining policies for who in the organization is eligible for a private line, creating and maintaining lists of people and their telephone lines, possibly creating a private telephone directory for executives, arranging for user training, and related tasks.

Note:
The private telephone line is stored in Active Directory as an msRTCSIP-PrivateLine attribute on the user object. By default any member of the Authenticated Users group has read access to this attribute.

Assigning Telephone Numbers

Accounts for new users who need private telephone lines are created in the same manner as accounts without private telephone lines, using Lync Server Control Panel or Lync Server Management Shell.

Use the **Set-CsUser** cmdlet in the Lync Server Management Shell to assign a telephone number to a private telephone line for a user, for example, **Set-CsUser -Identity "sip:joe@contoso.com" -PrivateLine "Tel:+14255551212"**.

Telephone numbers for private telephone lines can be between 3 and 15 numbers in length and must be preceded with the "TEL:" prefix. They can have any area code and any country/region code as long as your organization has direct inward dialing for that area code and country/region code.

For details about cmdlets and Lync Server Management Shell, see the Lync Server Management Shell documentation.

Private Telephone Lines in Mixed Deployments

Private telephone lines should be configured only for deployments of Lync Server. In a deployment in which there are both Lync Server and Office Communications Server 2007 or Office Communications Server 2007 R2 servers, when a user on earlier version attempts to call a private telephone line, routing of the call fails because the server cannot perform a reverse number lookup on a private telephone line.

1.3.10.12 Planning for Location Based Routing

Planning for Location Based Routing

See Also

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2013-03-09*

The information in this topic pertains to Cumulative Updates for Lync Server 2013: February 2013.

Location-Based Routing makes it possible to restrict the routing of calls between VoIP endpoints and PSTN endpoints based on the location of the parties in the call. Location-Based Routing is part of the Lync Server 2013 Enterprise Voice infrastructure. Location-Based Routing is a call management feature that controls how calls are routed by Lync Server 2013 CU1. It enforces call authorization rules on whether calls can be routed to PBX or PSTN endpoints based on the Lync caller’s geographic location.

- Overview of Location-Based Routing
- Guidance for Location-Based Routing

- Scenarios for Location-Based Routing
- Technical Considerations for Location-Based Routing
- Client and Server Support for Location-Based Routing
- Capabilities not supported by Location-Based Routing
- Deployment Process for Location-Based Routing

⊟See Also

Concepts

Planning for Enterprise Voice

1.3.10.12.1 Overview of Location-Based Routing

Overview of Location-Based Routing

See Also

Planning > Planning for Enterprise Voice > Planning for Location Based Routing >

Topic Last Modified: *2013-02-21*

Location-Based Routing introduces a new set of rules that modifies the routing of national and international PSTN calls to prevent toll bypass. Location-Based Routing provides the flexibility to scope these rules to specific regions, specific gateways or to specific set of users only.

The following scenarios illustrate the main types of restrictions Location-Based Routing can enforce:

- Egress calls – Location-Based Routing can enforce outgoing calls to egress from a PSTN gateway that is located in the same region as where the caller is to prevent PSTN toll bypass, which prevents calls to egress from a PSTN gateway located in a different region as the caller.
- Ingress calls – Location-Based Routing can prevent incoming PSTN calls to ring Lync endpoints if the PSTN gateway routing the incoming call is not located in the same region as the called Lync user.
- Unknown regions – Location-Based Routing restricts incoming and outgoing PSTN calls to and from users that are located in undetermined locations (i.e. remote users connecting from the Internet or located in unknown regions).
- International regions – Location-Based Routing enforces routing of outgoing calls through international PSTN gateways if a gateway local to the user’s location cannot be found.

Other Resources

Planning for Location Based Routing

1.3.10.12.2 Guidance for Location-Based Routing

Guidance for Location-Based Routing

See Also

Planning > Planning for Enterprise Voice > Planning for Location Based Routing >

Topic Last Modified: *2013-02-21*

Location-Based Routing depending on the situation can be applied at the user’s endpoint network site location or at the PSTN gateway’s network site location. This topic provides guidance on how Location-Based Routing is applied.

- User's location

- PSTN gateway's location

⊟See Also

Other Resources

Planning for Location Based Routing

1.3.10.12.2.1 User's location

User's location

See Also

Planning for Enterprise Voice > Planning for Location Based Routing > Guidance for Location-Based Routing >

Topic Last Modified: *2013-03-09*

Location-Based Routing leverages the same network regions, sites and subnets as defined in Lync Server used by E9-1-1, CAC and Media Bypass to apply call routing restrictions to prevent PSTN toll bypass. A user’s location is determined by the IP subnet of the user’s Lync endpoint(s) are connected from. Each IP subnet is associated to a network site, which are aggregated into network regions defined by the administrator. Location-Based Routing is enforced based on the user’s network site.

Location-Based Routing rules are applied on a per network site basis, meaning that a given set of rules will be applied to all endpoints enabled for Location-Based Routing that are located within the same network site. Administrators can apply Location-Based Routing to network sites that require it.

Voice routing policies can be defined on a per network site basis to define a particular PSTN gateway that should be used by all users located in the network site to call PSTN phone numbers. Such voice routing policies will take precedence over the routing defined by the user’s voice policy when the user is located in a network site enabled for Location-Based Routing, and it will prevent the routing of calls via other PSTN gateways that are enabled for Location-Based Routing. When a Lync user places a PSTN call, the user’s voice policy determines whether the user can be authorized to place the call. If the user’s voice policy allows the user to place the call, Location-Based Routing determines which PSTN gateway the call should egress from. Location-Based Routing makes this determination based on the user’s location.

A user location can be categorized in the following ways:

- The user is located in a known network site enabled for Location-Based Routing and his DID (Direct Inward Dial) number terminates on a PSTN gateway placed in the same network site (i.e. office). The routing of outbound calls will be through the voice routing policy of the network site in which the user is located. Incoming PSTN calls to the user are routed to endpoints that are located in the same network site as the PSTN gateway.
- The user is located in a known network site that is in different from the network site where the PSTN gateway is located. (i.e. the user traveled to another corporate office). The routing of outbound calls will be using the voice routing policy of the network site in which the user is located. Incoming PSTN calls to the user will not be routed to endpoints that are located in different sites than the PSTN gateway to prevent PSTN toll bypassing.
- When a user is located in a network site that is unknown to the Lync Server deployment, the routing of outbound calls will be based on the voice policy assigned to the user to PSTN gateways not bound to Location-Based Routing restrictions. Incoming PSTN calls will not be routed to endpoints that are located in unknown network sites to prevent PSTN toll bypassing.

Other Resources

Guidance for Location-Based Routing

1.3.10.12.2.2 PSTN gateway's location

PSTN gateway's location

See Also

Planning for Enterprise Voice > Planning for Location Based Routing > Guidance for Location-Based Routing >

Topic Last Modified: *2013-03-09*

Calls routed via PSTN gateways and PBXs might require Location-Based Routing restrictions depending on the location of such systems. Location-Based Routing can be enabled at the granularity on a per trunk basis.

Location-Based Routing introduces the following set of rules when enabled on a trunk:

- When Location-Based Routing is enabled on a per trunk basis, the rules define on that trunk will be applied only to calls routed through that trunk.
- To prevent PSTN tolls bypass where calls originate from a network site different that the network site where the PSTN gateway is located, Location-Based Routing introduces the association of a network site to a given trunk. This defines the network site that allows calls to be routed to a given trunk.

Trunks can be enabled for Location-Based Routing in two ways:

- The trunk is defined for a PSTN gateway that egresses calls to the PSTN. Incoming calls routed by a trunk of this type will be routed only to endpoints located within the same network site as the trunk.
- The trunk is defined for a Mediation Server peer that doesn’t egress calls to the PSTN and services users with legacy phones in a static locations (i.e. PBX phones). For this particular configuration, all incoming calls routed by a trunk of this type will be considered to be originating from the same network site as the trunk. Calls from PBX users will have the same Location-Based Routing enforcement as Lync users who are located in the same network site as the trunk. If two PBX systems located in separate network sites are connected through Lync Server, Location-Based Routing will allow routing from one PBX endpoint in one network site to another PBX endpoint in the other network site. This scenario will not be blocked by Location-Based Routing. In addition to this scenario and in a similar way as a Lync user in the same location, endpoints connected to a Mediation Server peer with this configuration will be able to make or receive calls to and from other Mediation Server peer that do not route calls to the PSTN (i.e. an endpoint connected to a different PBX) regardless of the network site to which the Mediation Server peer is associated. All inbound calls, outbound calls, call transfers and call forwards involving PSTN endpoints will be subject to Location Based Routing to use only PSTN gateways that are defined as local to such Mediation Server peer.

Other Resources

Guidance for Location-Based Routing

1.3.10.12.3 Scenarios for Location-Based Routing

Scenarios for Location-Based Routing

See Also

Planning > Planning for Enterprise Voice > Planning for Location Based Routing >

Topic Last Modified: *2013-02-21*

Location-Based Routing applies the following general rules when routing calls in the following scenarios.

- Outgoing calls
- Incoming calls
- Call transfers and call forwarding
- Simultaneous ringing
- Delegation

⊟See Also

Other Resources

Planning for Location Based Routing

1.3.10.12.3.1 Outgoing calls

Outgoing calls

See Also

Planning for Enterprise Voice > Planning for Location Based Routing > Scenarios for Location-Based Routing >

Topic Last Modified: *2013-03-09*

The routing of outbound calls of users enabled for Location-Based Routing is affected by the network location of the user's endpoint. The following table illustrates how Location-Based Routing affects the routing of outbound calls depending on the location of the caller's endpoint.

Caller placing an outbound call to the PSTN

	User endpoint located in a network site enabled for Location-Based Routing	User endpoint located in unknown network site or not enabled for Location-Based Routing
Authorization of outbound calls	Call is authorized based on user's voice policy	Call is authorized based on user's voice policy
Routing of outbound call	Call is routed according to the network site's voice routing policy	Call is routed according to user's voice policy and only through trunks not enabled for Location-Based Routing (if available)

Other Resources

Scenarios for Location-Based Routing

1.3.10.12.3.2 Incoming calls

Incoming calls

See Also

Planning for Enterprise Voice > Planning for Location Based Routing > Scenarios for Location-Based Routing >

Topic Last Modified: *2013-03-09*

The routing of incoming calls to users enabled for Location-Based Routing depends on the location of the user's endpoint. The routing of incoming calls is affected in the following way. If a user has an incoming call to an endpoint located in a Location-Based Routing enabled network site, and the endpoint is located in the same network site as the PSTN gateway, the call will be routed. If a user has an incoming call to an endpoint located in a Location-Based Routing enabled network site, and the endpoint is located in a different network site than the PSTN gateway, the call will not be routed. When a user has no endpoints located in the same network site as the PSTN gateway where the incoming call is originating from, the incoming call will be routed directly to the user's voicemail and a missed call notification will be sent to the called party.

The call forwarding settings of a user that is enabled for Location-Based Routing will continue to be enforced, however, calls forwarded will be subject to Location-Based Routing restrictions of the user.

The following table illustrates how Location-Based Routing affects the routing of inbound calls depending on the location of the callee's endpoint. The network site of the PSTN gateway is enabled for Location-Based Routing, and Location-Based Routing only permits routing of PSTN calls to endpoints within the same network site.

Callee receiving an inbound call from the PSTN

	Callee's endpoint located in the same network site as PSTN gateway	**Callee's endpoint not located in the same network site as PSTN gateway**	**Callee's endpoint located in unknown network site or not enabled for Location-Based Routing**
Routing of inbound PSTN call	Incoming call is routed to callee's endpoints	Incoming call is not routed to callee's endpoints	Incoming call is not routed to callee's endpoints

Other Resources

Scenarios for Location-Based Routing

1.3.10.12.3.3 Call transfers and call forwarding

Call transfers and call forwarding

See Also

Planning for Enterprise Voice > Planning for Location Based Routing > Scenarios for Location-Based Routing >

Topic Last Modified: *2013-03-09*

When a PSTN endpoint is involved, Location-Based Routing analyzes the location of the calle's endpoint and the endpoint where the call will be transferred or forwarded to (i.e. transfer/forward target). Location-Based Routing determines whether the call should be transferred or forwarded depending on the location of both endpoints.

The following table illustrates the scenario of a Lync user in a call with a PSTN endpoint, and the Lync user transfers the call to another Lync user. Depending on the network site location of the transferee's endpoint, Location-Based Routing affects the routing of the call transfer or forward.

Initiating call transfer or forward

User initiating the call transfer/ forward	**Target endpoint is in same network site as user initiating call transfer or forward**	**Target endpoint is in different network site as user initiating call transfer or forward**	**Target endpoint is in unknown network site or network site not enabled for Location-Based**

			Routing
Lync user	Call forward or transfer is allowed	Call forward or transfer is not allowed	Call forward or transfer is not allowed

For example: a Lync user in a call with a PSTN endpoint transfers the call to another Lync user that is in the same network site. In this case, the call transfer is allowed.

The following table illustrates the scenario of a Lync user in a call with another Lync user, and one of the users transfers the call to a PSTN endpoint. Depending on the location of the user the call is being transferred to, the table details how Location-Based Routing affects the call.

Call transfer or forward to PSTN endpoint

Call transfer/ forward endpoint target	**Lync users in same network site**	**Lync users in different network sites**	**One or both Lync users in unknown network site or network site not enabled for Location-Based Routing**
PSTN endpoint	Call forward or transfer allowed by the transferred user's site voice routing policy	Call forward or transfer allowed by the transferred user's site voice routing policy	Call forward or transfer allowed by the transferred user's voice policy only through trunks not enabled for Location-Based Routing

For example: a Lync user in a call with another Lync user that is in the same network site transfers the call to a PSTN endpoint and the call transfer is allowed.

Other Resources

Scenarios for Location-Based Routing

1.3.10.12.3.4 Simultaneous ringing

Simultaneous ringing

See Also

Planning for Enterprise Voice > Planning for Location Based Routing > Scenarios for Location-Based Routing >

Topic Last Modified: *2013-03-09*

When the called party has simultaneous ringing enabled, Location-Based Routing analyzes the location of the calling party and the endpoints of the called parties to determine whether the call should be routed.

The following table illustrates a user configured with simultaneous ringing, and the simultaneous ringing target is a user in the same network site, in a different network site, or in an unknown network site.

Incoming PSTN call for	**Located in the same network site as**	**Located in different network site than**	**Located in unknown network site or not**

	callee	callee	enabled for Location-Based Routing
Lync user	Simultaneous ring allowed	Simultaneous ring not allowed	Simultaneous ring not allowed

The following table illustrates a call from a Lync user (i.e. Lync caller) in the same network site, in a different network site, or from an unknown network site. The callee has a PSTN endpoint (i.e. cellphone) configured as a simultaneous ring target. In this scenario, Location-Based Routing will determine whether the call should be routed to the simultaneous ring target (i.e. cellphone) of the callee or not.

Simultaneous ring target	Located in the same network site as callee	Located in different network site than callee	Located in unknown network site or not enabled for Location-Based Routing
PSTN endpoint	Simultaneous ring allowed through the caller's site voice routing policy	Simultaneous ring allowed through the caller's site voice routing policy	Simultaneous ring allowed through the caller's voice policy to trunks not enabled for Location-Based Routing

Other Resources

Scenarios for Location-Based Routing

1.3.10.12.3.5 Delegation

Delegation

See Also

Planning for Enterprise Voice > Planning for Location Based Routing > Scenarios for Location-Based Routing >

Topic Last Modified: *2013-03-09*

The delegation capabilities in Lync are affected by Location-Based Routing in the following manner:

- When a delegate enabled for Location-Based Routing places a call on behalf of a manager, the delegate's voice policy is used to authorize the call and the delegate's site voice routing policy will be used to route the call
- For incoming PSTN calls to a manager, the same rules applicable for call forwarding or simultaneously ringing will apply as described in the Call transfers and forwarding and Simultaneous ringing topics.
- When a delegate sets a PSTN endpoint as a simultaneous ring target, for an incoming call to the manager, the voice routing policy of the site that is associated to the incoming trunk will be used to route the call to the delegate's PSTN endpoint.
- For delegation, it's recommended that the manager and his associated delegates to be usually located in the same network site.

Other Resources

Scenarios for Location-Based Routing

1.3.10.12.4 Technical Considerations for Location-Based Routing

Technical Considerations for Location-Based Routing

See Also

Planning > Planning for Enterprise Voice > Planning for Location Based Routing >

Topic Last Modified: *2013-03-09*

When planning Location-Based Routing, you should consider the impact to the following scenarios.

Disaster Recovery

During a failover from the primary pool to a backup pool as well as when restoring normal operations to the primary pool, Location-Based Routing remains enforced at all times during a disaster and recovery procedure.

Survivable Branch Appliance

Configuring Location-Based Routing impacts the planning of where you deploy the gateways associated to your Survivable Branch Appliances. The gateway associated to your SBA must be located in the same network site as your Survivable Branch Appliance; otherwise, users homed on your Survivable Branch Appliance will not be permitted to place outbound calls if Location-Based Routing is configured. When the WAN connection between your Survivable Branch Appliance and the central site is down, Location-Based Routing restrictions remains enforced.

⊟See Also

Other Resources

Planning for Location Based Routing

1.3.10.12.5 Client and Server Support for Location-Based Routing

Client and Server Support for Location-Based Routing

See Also

Planning > Planning for Enterprise Voice > Planning for Location Based Routing >

Topic Last Modified: *2013-03-09*

Location-Based Routing is enforced by Lync Server. Lync Server can identify the network sites where users are connecting from within the corporate network. Since remote users are outside the corporate network, their location is considered to be unknown.

Lync Server Support

Location-Based Routing requires that Lync Server 2013 CU1 is deployed on all Front End pools and Standard Edition servers in a given topology. If Lync Server 2013 CU1 is not installed on certain Lync components in the topology, Location-Based Routing restrictions cannot be fully enforced.

The following table identifies the combination of server roles and versions that is supported for Location-Based Routing.

Pool version	Mediation Server version	Supported
Lync Server 2013 CU1	Lync Server 2013 CU1	yes
Lync Server 2013 CU1	Lync Server 2013	no
Lync Server 2013 CU1	Lync Server 2010	no
Lync Server 2013 CU1	Office Communications Server 2007 R2	no
Lync Server 2013	any	no
Lync Server 2010	any	no
Office Communications Server 2007 R2	any	no

Lync Client Support

The following table identifies the clients that Location-Based Routing supports.

Client type	Supported	Details
Lync 2013	yes	Including Lync 2013 CU1
Lync 2010	yes	
Office Communicator 2007 R2	no	
Lync Phone Edition	yes	
Lync Attendant	yes	
Lync for Windows 8	yes	
Lync Mobile 2013	no	VoIP must be disabled for Lync Mobile 2013 clients if used by users with Location-Based Routing enabled.
Lync Mobile 2010	yes	

Note:

To disable VoIP for Lync Mobile 2013 clients, assign a mobility policy with the setting, IP Audio/Video, disabled for all users enabled for Location Based Routing. For more details about mobility policy, see New-CsMobilityPolicy.

See Also

Other Resources

Planning for Location Based Routing

1.3.10.12.6 Capabilities not supported by Location-Based Routing

Capabilities not supported by Location-Based Routing

See Also

Planning > Planning for Enterprise Voice > Planning for Location Based Routing >

Topic Last Modified: *2013-02-21*

The following capabilities are not supported by Location-Based Routing. Location-Based Routing is not enforced when Lync endpoints interact with PSTN endpoints using these capabilities.

- PSTN dial-in to conferences
- PSTN dial-out from conferences
- Escalations from peer-to-peer audio conversations to conferencing involving PSTN endpoints
- Consultative transfers involving PSTN endpoints
- Incoming and outgoing PSTN calls through Response Group
- Call park or retrieval of PSTN calls through Call Park
- Incoming PSTN calls to Announcement Service
- Incoming PSTN calls retrieved via Group Call Pickup

Other Resources

Planning for Location Based Routing

1.3.10.12.7 Deployment Process for Location-Based Routing

Deployment Process for Location-Based Routing

See Also

Planning > Planning for Enterprise Voice > Planning for Location Based Routing >

Topic Last Modified: *2013-03-09*

This topic provides an overview of the process involved in configuring Location-Based Routing. You must deploy Lync Server Enterprise Edition or Standard Edition with Enterprise Voice before you configure Location-Based Routing. The components required by Location-Based Routing are already installed and enabled when you deploy Enterprise Voice.

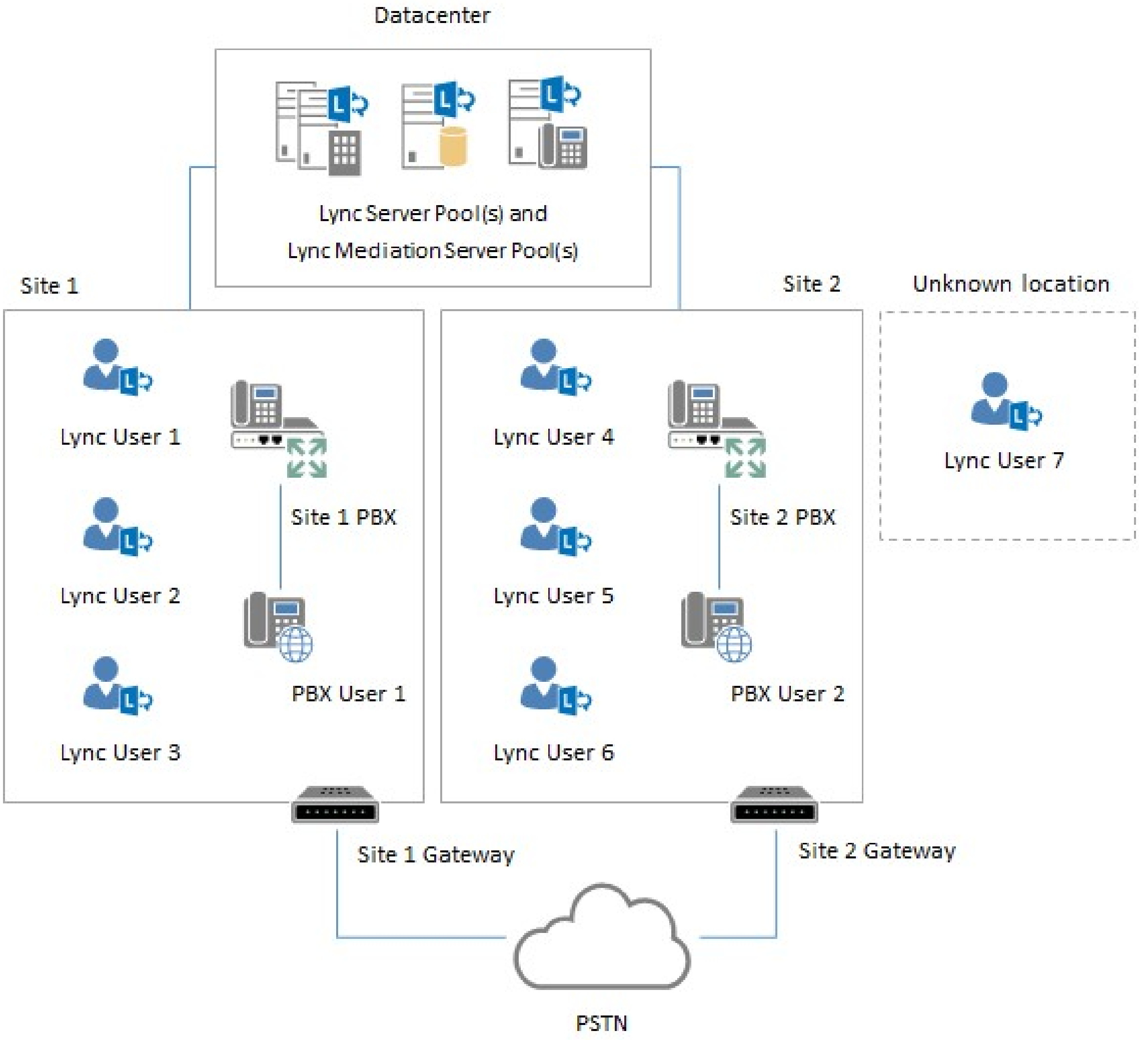
Location-Based Routing Deployment Process

Phase	Steps	Required groups and roles	Deployment documentation
Deploy Enterprise Voice	• Configure Trunks • Create Voice Policies • Define Voice Routes	CSVoiceAdmins CsAdministrator CsServerAdministrator	Deploying Enterprise Voice
Verify your Enterprise Voice deployment		CSVoiceAdmins CsAdministrator CsServerAdministrator	
Configure network regions, sites, and subnets	• Create network regions • Create network sites • Associates subnets with network sites	CSVoiceAdmins CsAdministrator CsServerAdministrator	About Network Regions, Sites, and Subnets Create or Modify a Network Region Create or Modify a Network Site Associate a Subnet with a Network Site

Configure Location-Based Routing	• Create voice routing policies • Define separate trunk configuration per trunk • Modify voice policies • Enable Location-Based Routing configuration	CSVoiceAdmins CsAdministrator CsServerAdministrator	

Sample Deployment

The following deployment is used to illustrate further the mechanisms enabled by Location-Based Routing.



Incoming PSTN calls

An administrator can enable the trunk defined to route calls to "Site 1 Gateway" for Location-Based Routing and associate the "Site 1 Gateway" to site 1. Once enabled, calls that are routed through "Site 1 Gateway" will only be routed to users that are located in site 1. All calls routed through the "Site 1 Gateway" trunk destined to users in a different site, such as site 2 will be blocked to prevent PSTN toll bypass.

All incoming PSTN calls through "Site 1 Gateway" will only be allowed to route to endpoints located in site 1. For example, when "Lync user 1" travels to site 2, all incoming PSTN calls through "Site 1 Gateway" will not be routed to "Lync user 1" endpoints located in site 2. The same routing rule applies if "Lync user 1" travels to an unknown network site where the user's location can't be determined.

The following table outlines the user experience of "Lync user 1" in this context.

	Lync user 1 endpoints located in network site 1	**Lync user 1 endpoints located in network site 2**	**Lync user 1 endpoints located in unknown network site**
Inbound PSTN calls to Lync user 1	Calls are routed to endpoints in this location	Calls are not routed to endpoints in this location	Calls are not routed to endpoints in this location

Outgoing PSTN calls

Voice routes are referenced in both Voice Policies assigned directly to users, and Voice Routing Policies assigned to network sites. Both policies contain references to routes, which can be used to route a call differently. For example, an administrator can define a Voice Routing Policy for all users located in network site 1 to route all outbound calls through the "Site 1 Gateway" while the Voice Policy of some users define a route for all outbound calls through the "Site 2 Gateway". While these users are located in network site 1, their outbound calls will be routed through the "Site 1 Gateway".

When a user is located in a network site configured for Location-Based Routing, the network site's Voice Routing Policy route overrides the user's Voice Policy route. This rule is particularly useful for users that temporarily move to a different site. In this particular case a user will always use a gateway that is local to his location; if "Lync user 3" is located at "Site 2", all his outbound calls will be routed via "Site 2 Gateway", but if he travels to site 1, all his outbound calls placed while he's at site 1 will be routed through "Site 1 Gateway".

The following table illustrates the user experience of Lync user 1 placing an outbound call from the following network sites.

	Network site 1	**Network site 2**	**Unknown network site or not enabled for Location-Based Routing**
Authorization of outbound calls	Lync user 1 voice policy	Lync user 1 voice policy	Lync user 1 voice policy
Routing of outbound calls	Site 1 voice routing policy	Site 2 voice routing policy	User's voice policy and only to systems not enabled for Location-Based Routing

Call transfers and forwards

When calls are transferred or forwarded, the routing of calls is affected by Location-Based Routing.

The following table depicts Lync user 1 transferring or forwarding a PSTN call to another Lync user.

User initiating call transfer or forward	**Lync user 2**	**Lync user 4**	**Lync user in network site not enabled for Location-Based Routing**

Lync user 1	Call forward or transfer is allowed	Call forward or transfer is not allowed	Call forward or transfer is not allowed

The following table illustrates how Location-Based Routing affects how the call is routed based on the location of the Lync user being transferred (Lync user 2, Lync user 4, etc) to a PSTN endpoint

Endpoint where call is transferred or forwarded to	**Lync user 2**	**Lync user 4**	**Lync user in network site not enabled for Location-Based Routing**
PSTN endpoint	Call forward or transfer is routed through site 1 voice routing policy and egress via Site 1 Gateway	Call forward or transfer is routed through site 2 voice routing policy and egress via Site 2 Gateway	Call forward or transfer is routed through the Lync user voice policy and egress via a gateway not enabled for location-based routing (if available)

Simultaneous ringing

Once location-based routing is configured in the sample topology, the following interactions are enforced.

The following table illustrates whether Location-Based Routing allows simultaneous ringing for different Lync users (i.e. Lync user 2, Lync user 4, etc).

Incoming PSTN call target	**Lync user 2**	**Lync user 4**	**Lync user in network site not enabled for Location-Based Routing**
Lync user 1	Simultaneous ring is allowed	Simultaneous ring is not allowed	Simultaneous ring is not allowed

The following table illustrates whether Location-Based Routing allows simultaneous ringing to a PSTN endpoint from different Lync users (i.e. Lync user 2, Lync user 4, etc).

Simultaneous ring target	**Lync user 2**	**Lync user 4**	**Lync user in network site not enabled for Location-Based Routing**
Lync user 1 mobile phone (PSTN endpoint)	Call routed through network site 1's voice routing policy and egress via site 1 gateway	Call routed through network site 2's voice routing policy and egress via site 2 gateway	Call routed through the caller voice policy and will egress via a PSTN gateway not enabled for Location-Based Routing

⊟See Also

Other Resources

Planning for Location Based Routing

1.3.10.13 Planning for Call Management Features

Planning for Call Management Features

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

***Topic Last Modified:** 2012-12-17*

Enterprise Voice call management features control how incoming calls are routed and answered. Lync Server 2013 provides the following call management features:

- **Call Park**: Enables voice users to temporarily park a call and then pick it up from the same or another phone.
- **Group Pickup**: Enables voice users to pick up calls that are ringing for other voice users who are assigned to call pickup groups.

  Note:
  Group Pickup is new with Cumulative Updates for Lync Server 2013: February 2013.
- **Response Group**: Routes incoming calls to groups of agents by using hunt groups or interactive voice response (IVR) questions and answers.
- **Announcement:** Plays a message for calls made to an unassigned number, or routes the call elsewhere, or both.

If you plan to deploy Enterprise Voice, you can choose to implement any or all of these call management features.

- Planning for Call Park
- Planning for Group Call Pickup
- Planning for Response Groups
- Planning for Announcements

1.3.10.13.1 Planning for Call Park

Planning for Call Park

Planning > Planning for Enterprise Voice > Planning for Call Management Features >

***Topic Last Modified:** 2012-09-07*

The Lync Server Call Park application makes it possible for Enterprise Voice users to put a call on hold and then retrieve it later from any phone. The user who parked the call can either dial the orbit number provided by Call Park to retrieve the parked call or use an external mechanism, such as instant messaging or a paging system, to ask someone else to retrieve the call. This section includes planning information that is specific to Call Park.

- Overview of Call Park
- Components Used by Call Park
- Technical Requirements for Call Park
- Clients Supported for Call Park
- Capacity Planning for Call Park
- Deployment Process for Call Park

1.3.10.13.1.1 Overview of Call Park

Overview of Call Park

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Call Park >

***Topic Last Modified:** 2012-10-29*

The Lync Server 2013 Call Park application lets Enterprise Voice users do any of the following:

- Put a call on hold and then retrieve the call from the same phone or another phone.
- Put a call on hold to transfer it to a department or general area (for example, to a sales department or a warehouse where there is a common area phone).
- Put a call on hold and keep the original answering phone free for other calls.

When a user parks a call, Lync Server transfers the call to a temporary number, called an *orbit*, where the call is held until it is retrieved or it times out. Lync Server sends the orbit to the user who parked the call. To retrieve the parked call, the user can dial the orbit number or click the orbit link or button in the Conversation window.

The user who parked a call can notify someone to retrieve the call by using an external mechanism, such as instant messaging (IM) or a paging system, to communicate the orbit number to someone else. The user who parked the call can leave the Conversation window open to receive notification when the call is retrieved.

Because orbit ranges are globally unique, it is possible to retrieve calls from any Lync Server site or PBX phone if routing is configured appropriately. If no one retrieves the call within a configurable amount of time, the call rings back to the person who parked it. If that person does not answer the ringback, the call is transferred to a fallback destination, such as to an operator, if so configured. You can configure the number of times the call rings back before being transferred from one to ten times. If no one answers a transferred call, the call is disconnected. The orbit is freed when the call is retrieved or disconnected.

When you deploy Call Park, you need to reserve ranges of extension numbers for parking calls. These extensions need to be virtual extensions: extensions that have no user or phone assigned to them. You then configure the call park orbit table with the ranges of extension numbers and specify which Application service hosts the Call Park application that handles each range. Each Front End pool has a Call Park table on the corresponding Back End Server that is used to manage calls that are parked on the pool. The list of orbit ranges is stored in Central Management store and is used to route orbits to the destination pool. Each Lync Server pool where the Call Park application is deployed and configured can have one or more orbit ranges. Orbit ranges must be globally unique across the Lync Server deployment.

You also configure other Call Park settings, such as where calls are redirected if they time out and whether the person on the phone hears music while parked. You can also specify the music file to play while the call is on hold.

Note:

Customized music-on-hold files for Call Park are not backed up as part of the Lync Server 2013 disaster recovery process and will be lost if the files uploaded to the pool are damaged, corrupted, or erased. Always keep a separate backup copy of the customized music-on-hold files that you have uploaded for Call Park.

The Call Park application is a component of Enterprise Voice. When you deploy Enterprise Voice, the Call Park application is installed and activated automatically. Before you can use Call Park, however, the Enterprise Voice administrator must configure it and enable it for users through voice policy.

1.3.10.13.1.2 Components Used by Call Park

Components Used by Call Park

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Call Park >

Topic Last Modified: *2012-09-13*

The Call Park application is automatically installed when you deploy Enterprise Voice. You enable Call Park by configuring voice policy. The following Lync Server 2013 components support the Call Park application:

- **Application service** Application service provides a platform for deploying, hosting, and managing unified communications applications, such as the Call Park application. Application service is automatically installed on every Front End Server in a Front End pool and on every Standard Edition server.
- **Call Park application** The Call Park application is one of the unified communications applications that are hosted by Application service. It is included automatically when you deploy Enterprise Voice. Call Park parks and retrieves calls and manages call park orbits.
- **Music-on hold-file** If music in enabled, the music file is played while a call is parked. A default music file is included when the Call Park application is installed.
- **File Store** The Call Park application uses File Store to hold custom audio files.
- **Lync Server Control Panel** You can use Lync Server Control Panel to configure the call park orbit table and to enable Call Park for users.
- **Lync Server Management Shell** All Call Park application configuration can be performed by using Lync Server Management Shell cmdlets.

1.3.10.13.1.3 Technical Requirements for Call Park

Technical Requirements for Call Park

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Call Park >

Topic Last Modified: *2012-09-30*

This section describes the following technical requirements for Call Park:

- Hardware requirements
- Software requirements
- Port requirements
- Audio file requirements

Hardware Requirements

The Call Park application has the same hardware requirements as Front End Servers. For details about hardware requirements, see Server Hardware Platforms in the Supportability documentation.

Software Requirements

The Call Park application has the same operating system requirements and software prerequisites as Front End Servers. For details about software requirements, see Server and Tools Operating System Support in the Supportability documentation.

All Front End Servers and Standard Edition servers where the Call Park application is deployed must have the Windows Media Format Runtime installed for servers running

Windows Server 2008 R2, or Microsoft Media Foundation for servers running Windows Server 2012. For Windows Server 2008 R2, Windows Media Format Runtime is installed as part of Windows Desktop Experience. Windows Media Format Runtime or Microsoft Media Foundation is required for Windows Media Audio (.wma) files that Call Park plays for music on hold.

Port Requirements

The Call Park application uses the following port:

- **Port 5075** Used for SIP listening requests.

Note:

This port is a default setting that you can change by using the **Set-CsApplicationServer** cmdlet. For details about this cmdlet, see the Lync Server Management Shell documentation.

Audio File Requirements

The Call Park application supports only Windows Media Audio (.wma) files for music on hold. You can use the Microsoft Expression Encoder 4 to customize files for music on hold. To download Expression Encoder 4, see "Expression Encoder 4" at http://go.microsoft.com/fwlink/p/?linkId=202843. Use the tool to convert the file to a .wma format. The recommended format for Call Park music-on-hold files is Media Audio 9, 44 kHz, 16 bits, Mono, CBR, 32 kbps.

Note:

The converted file plays over the phone only at 16 kHz, even if it was recorded at 44 kHz.

1.3.10.13.1.4 Clients Supported for Call Park

Clients Supported for Call Park

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Call Park >

Topic Last Modified: *2012-09-13*

This section identifies the clients that can be used to park calls and the clients that can be used to retrieve parked calls.

Clients Supported for Parking Calls

Calls from any IP, private branch exchange (PBX), public switched telephone network (PSTN), or mobile phone can be parked.

Note:

Only audio calls can be parked. Instant messages and conferences cannot be parked.

The following clients can use Call Park to park calls:

- Lync 2013
- Lync 2010
- Lync 2010 Attendant
- Lync Phone Edition

Note:

Mobile phones cannot use Call Park to park calls.

Clients Supported for Retrieving Calls

Orbit ranges are configured as blocks of virtual extensions (extensions without an assigned user or phone). When you configure orbits as virtual extensions, mobile phones and PSTN phones cannot retrieve parked calls.

Federated users cannot retrieve parked calls.

The following clients can retrieve calls that are parked on Call Park:

- Lync 2013
- Lync 2010
- Lync 2010 Attendant
- Lync Phone Edition
- IP common area phones
- Non-IP phones that are connected to the Lync Server 2013 infrastructure, including common area phones and private branch exchange (PBX) phones

1.3.10.13.1.5 Capacity Planning for Call Park

Capacity Planning for Call Park

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Call Park >

Topic Last Modified: *2012-09-13*

The following table describes the Call Park user model that you can use as the basis for capacity planning requirements.

◆**Important:**
Keep in mind that, for disaster recovery capacity planning, each pool of a paired pool should be able to handle the workloads for Call Park services in both pools.

Call Park User Model

Metric	**Per Front End pool (with 8 Front End Servers)**	**Per Standard Edition server**
Park rate	8 per minute	1 per minute
Retrieve parked call rate	8 per minute	1 per minute
Average park duration	60 seconds	60 seconds

1.3.10.13.1.6 Deployment Process for Call Park

Deployment Process for Call Park

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Call Park >

Topic Last Modified: *2013-02-25*

This section provides an overview of the steps involved in deploying the Call Park application. You must deploy Enterprise Edition or Standard Edition with Enterprise Voice before you configure Call Park. The components required by Call Park are installed and enabled when you deploy Enterprise Voice.

Call Park Deployment Process

Phase	**Steps**	**Required groups**	**Deployment**

		and roles	documentation
Configure the call park orbit ranges in the orbit table	Use Lync Server Control Panel or the **New-CSCallParkOrbit** cmdlet to create the orbit ranges in the call park orbit table and associate them with the Application service that hosts the Call Park application. **Note:** For seamless integration with existing dial plans, orbit ranges are typically configured as a block of virtual extensions. Assigning Direct Inward Dialing (DID) numbers as orbit numbers in the call park orbit table is not supported.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Create or Modify a Call Park Orbit Range
Configure Call Park settings	Use the **Set-CsCpsConfiguration** cmdlet to configure Call Park settings. At a minimum, we recommend that you configure the **OnTimeoutURI** option to configure the fallback destination to use when a parked call times out. You can also configure the following settings: • (Optional) **EnableMusicOnHold** to enable or disable music on hold. • (Optional) **MaxCallPickupAttempts** to determine the number of times a parked call rings back to the answering phone before forwarding the call to the fallback Uniform Resource Identifier (URI). • (Optional) **CallPickupTimeoutThreshold** to determine the amount of time that elapses after a call has been parked before it rings back to the phone where the call was answered.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Configure Call Park Settings
Optionally, customize the	Use the **Set-CsCallParkServiceMusicOnHol**	RTCUniversalServerAdmins	Customize Call Park Music on Hold

music on hold	**dFile** cmdlet to customize and upload an audio file, if you don't want to use the default music on hold.	CsVoiceAdministrator CsServerAdministrator CsAdministrator	
Configure voice policy to enable Call Park for users	Use Lync Server Control Panel or the **Set-CSVoicePolicy** cmdlet with the **EnableCallPark** option to enable Call Park for users in voice policy. **Note:** By default, Call Park is disabled for all users. **Note:** If you have multiple voice policies, make sure the EnableCallPark property is set for each voice policy, not just for the default policy.	RTCUniversalServerAdmins CsVoiceAdministrator CsUserAdministrator CsAdministrator	Enable Call Park for Users
Verify normalization rules for Call Park	Call park orbits must not be normalized. Verify that your normalization rules do not include any of your orbit ranges. If necessary, create additional normalization rules to prevent orbits being normalized.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Verify Normalization Rules for Call Park
Verify your Call Park deployment	Test parking and retrieving calls to make sure that your configuration works as expected.	-	(Optional) Verify Call Park Deployment

1.3.10.13.2 Planning for Group Call Pickup

Planning for Group Call Pickup

Planning > Planning for Enterprise Voice > Planning for Call Management Features >

Topic Last Modified: *2013-02-01*

Cumulative update for Lync Server 2013: February 2013 introduces Group Call Pickup as a new Enterprise Voice feature. Group Call Pickup lets users pick up calls that are ringing for another user by dialing a call pickup group number. This section includes planning information that is specific to Group Call Pickup.

- Overview of Group Call Pickup
- Components Used by Group Call Pickup
- Technical Requirements for Group Call Pickup
- Clients Supported for Group Call Pickup
- Deployment Process for Group Call Pickup

1.3.10.13.2.1 Overview of Group Call Pickup

Overview of Group Call Pickup

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Group Call Pickup >

Topic Last Modified: *2013-02-12*

Group Call Pickup, a new feature in Cumulative Updates for Lync Server 2013: February 2013, lets users answer incoming calls to their colleagues from their own phones. This new feature increases the availability of a user's line by enabling other users to answer an incoming call by dialing a call pickup group number. When Group Call Pickup is deployed, the number of incoming calls that are routed to voice mail can be significantly reduced, which is particularly useful for calls from customers who are external to your organization.

The Group Call Pickup feature is designed in particular for business units in open office environments. Incoming calls are not disruptive because they ring only at the intended destination. Other users who hear the ring, however, can still pick up the call simply by dialing the group number.

In environments where users are not located in an open office layout, or where users who share a common responsibility are geographically distributed, team call presents the most suitable solution. The primary difference between Group Call Pickup and team call is that, with Group Call Pickup, an incoming call rings only at the intended destination, but anyone can still choose to answer it by dialing a group number. With team call, the call rings at all the team members' phones, and any user in the team can pick up the phone to answer the call. An additional difference between Group Call Pickup and team call is that Group Call Pickup is managed by an administrator, through Lync Server. With team call, end users manage the feature by using the Lync client. With Group Call Pickup, therefore, this aspect of call management can be centralized.

Group Call Pickup is built on the Call Park application. When you deploy Group Call Pickup, you configure the call park orbit table with separate ranges of extension numbers that are designated as call pickup group numbers. Like call park orbit numbers, call pickup group numbers must be virtual extensions that have no user or phone assigned to them. Each Front End pool where you deploy Group Call Pickup can have one or more ranges of call pickup group numbers. The group number ranges must be globally unique across the Lync Server deployment.

Note:

Number ranges that are designated as Group Call Pickup numbers in the call park orbit table cannot be managed or viewed by using the Lync Server Control Panel. The only way to see all the number ranges in the call park orbit table is to use Lync Server Management Shell. Similarly, the only way to add, modify, or remove Group Call Pickup numbers is to use Lync Server Management Shell.

After you configure the call pickup group numbers, you assign users to a call pickup group. Any user who is assigned to a call pickup group can have their calls answered by other users. When a call comes in to a user who is assigned to a call pickup group, any other user who notices the call can answer it by manually dialing the call pickup group number. The user who picks up the call does not need to be a member of the group. When a call is picked up by another user, a notification is sent to the number originally called.

Note:

A user can be a member of only one call pickup group.

Note:

Although any user in the Lync Server deployment can answer a call to a call pickup group member, the person answering the call must know the correct call pickup group number to dial.

If a user dials a call pickup group number to answer a call when multiple phones in the group are ringing, the user answers the call that has been ringing the longest.

Simultaneous ringing settings will work for users who have group call pickup. That is, a call made to a user who has Group Call Pickup will ring for all the configured destinations, and another user can answer the call. The exception to this rule is when the user configures simultaneous ringing to call all the team members.

Group Call Pickup cannot be used to answer the following types of calls:

- Calls to a private line
- Calls from a contact who has been assigned the Friends and Family privacy relationship

  Tip:

  A user who is a member of a call pickup group can prevent certain calls from being retrieved through Group Call Pickup by marking the contact as a personal contact in the Lync client. To mark a contact as a personal contact, set the Privacy Relationship for the contact to Friends and Family. Any incoming call from contacts with the Privacy Relationship set to Friends and Family cannot be retrieved by using Group Call Pickup.
- Video portion of audio/video calls

  Note:

  If a user answers an audio/video call, the user receives only the audio. Either the person calling or the person answering the call can escalate the call to add video.
- Simultaneous ringing calls that are routed to team call members
- Calls routed to a delegate
- Calls routed to a response group

The following types of users cannot participate in Group Call Pickup. That is, they should not be included in a Group Call Pickup group, and they cannot pick up calls for users who have Group Call Pickup enabled.

- Users who are homed online in a hybrid deployment
- Users who are not homed on a Lync Server 2013 pool with Cumulative Updates for Lync Server 2013: February 2013 in an on-premises deployment

If no one answers a call to a member of a call pickup group, the call is routed as specified in the client settings. That is, the call goes to voicemail or is forwarded to a different destination, as specified in the client settings.

1.3.10.13.2.2 Components Used by Group Call Pickup

Components Used by Group Call Pickup

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Group Call Pickup >

Topic Last Modified: *2013-01-30*

Group Call Pickup is automatically deployed when you deploy Enterprise Voice and the Call Park application. You enable Group Call Pickup by configuring the Call Park orbit table with separate ranges of numbers designated as call pickup group numbers, and then by assigning users to call pickup groups and enabling the users for Group Call Pickup. The following Lync Server components support Group Call Pickup:

- **Application service** Application service provides a platform for deploying, hosting, and managing unified communications applications, such as the Call Park application. Application service is automatically installed on every Front End Server in a Front End pool and on every Standard Edition server.
- **Call Park application** The Call Park application is one of the unified communications applications that are hosted by Application service. Group Call Pickup is based on the Call Park application.
- **Lync Server Management Shell** You use Lync Server Management Shell to manage Group Call Pickup groups.
- **SEFAUtil resource kit tool** You use the secondary extension feature activation utility (SEFAUtil) to assign users to a call pickup group and to enable or disable call pickup for users.

1.3.10.13.2.3 Technical Requirements for Group Call Pickup

Technical Requirements for Group Call Pickup

See Also

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Group Call Pickup >

Topic Last Modified: *2013-01-30*

Group Call Pickup has the same hardware, software, and port requirements as the Call Park application. Group Call Pickup does not use audio files.

Concepts

Technical Requirements for Call Park

1.3.10.13.2.4 Clients Supported for Group Call Pickup

Clients Supported for Group Call Pickup

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Group Call Pickup >

Topic Last Modified: *2013-02-12*

Any of the following clients can be used to answer calls to Group Call Pickup members:

- Lync 2013
- Lync 2010
- Lync Phone Edition

Note:

Users can use any of these clients to answer calls to Group Call Pickup members, but the users must be homed on a Lync Server 2013 pool with Cumulative Updates for Lync Server 2013: February 2013.

In Cumulative Updates for Lync Server 2013: February 2013, the following clients and devices are not supported for picking up calls to Group Call Pickup members:

- Lync Mobile
- Lync app for Windows 8 and Windows RT
- Lync for iPad
- Analog phones
- Phones with public switched telephone network (PSTN) numbers

1.3.10.13.2.5 Capacity Planning for Group Call Pickup

Capacity Planning for Group Call Pickup

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Group Call Pickup >

Topic Last Modified: *2013-02-12*

The following table describes the Group Call Pickup user model that you can use as the basis for capacity planning requirements.

Important:

Group Call Pickup is based on the Call Park application. Keep in mind that, for disaster recovery capacity planning, each pool of a paired pool should be able to handle the workloads for Call Park services, including Group Call Pickup, in both pools.

Group Call Pickup User Model

Metric	Per Front End pool (with 8 Front End Servers)	Per Standard Edition server
Recommended number of users per group	50	50
Recommended number of groups	500	60
Maximum number of users per pool enabled for Group Call Pickup	25,000	3,000
Maximum rate of incoming calls to total users enabled for Group Call Pickup per pool per minute	500	60
Maximum rate of calls retrieved by users with Group Call Pickup per pool per minute	200	25

Note:

- For Front End pools that have fewer than eight Front End Servers, calculate the metrics linearly. For example, if your Front End pool has one Front End Server, calculate the maximum load as 1/8 of the values shown in the table.
- You can increase or decrease the recommended number of users per group and number of groups as long as you do not exceed the maximum number of users per pool. For example, your Standard Edition server can have 120 groups with 25 users per group because the number of users enabled for Group Call Pickup is still within the user model maximum (that is, 120 groups times 25 users is 3,000 users enabled for Group Call Pickup).

1.3.10.13.2.6 Deployment Process for Group Call Pickup

Deployment Process for Group Call Pickup

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Group Call Pickup >

Topic Last Modified: *2013-02-25*

This section provides an overview of the steps involved in deploying Group Call Pickup. You must deploy Enterprise Edition or Standard Edition with Enterprise Voice before you configure Group Call Pickup. The components required by Group Call Pickup are installed and enabled when you deploy Enterprise Voice.

Group Call Pickup Deployment Process

Phase	Steps	Required groups and roles	Deployment documentation
Enable the SEFAUtil resource kit tool in the topology	1. Use the **New-CsTrustedApplicationPool** cmdlet to create a new trusted application pool. 2. Use the **New-CsTrustedApplication** cmdlet to specify the SEFAUtil tool as trusted application. 3. Run the **Enable-CsTopology** cmdlet to enable the topology. 4. Install the resource kit tools on a Front End Server that is in the trusted application pool created in step 1. 5. Verify that SEFAUtil is running correctly by running it to display the call forwarding settings of a user in the deployment.	RTCUniversalServerAdmins	Deploy the SEFAUtil tool
Configure call pickup number ranges in the call park orbit table	Use the **New-CSCallParkOrbit** cmdlet to create call pickup number ranges in the call park orbit table and assign the call pickup ranges the type GroupPickup. **Note:** You must use Lync Server Management Shell to create, modify, remove, and view Group Call Pickup number ranges in the call park orbit table. Group Call Pickup number ranges are not available in Lync Server Control Panel. **Note:** For seamless integration with existing dial plans, number ranges are typically configured as a block of virtual extensions.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Configure Call Pickup Group Numbers

	Assigning Direct Inward Dialing (DID) numbers as range numbers in the call park orbit table is not supported.		
Assign a call pickup number to users, and enable Group Call Pickup for the users	Use the /enablegrouppickup parameter in the SEFAUtil resource kit tool to enable Group Call Pickup and assign a call pickup number for users.	-	Enable Group Call Pickup for Users and Assign a Group Number
Notify users of their assigned call pickup number and any other number of interest	Because any user can retrieve a call made to a Group Call Pickup user, users may want to monitor more than one group.	-	Communicate Group Call Pickup Assignment to Users
Verify your Group Call Pickup deployment	Test placing and retrieving calls to make sure that your configuration works as expected.	-	(Optional) Verify the Group Call Pickup Deployment

1.3.10.13.3 Planning for Response Groups

Planning for Response Groups

Planning > Planning for Enterprise Voice > Planning for Call Management Features >

Topic Last Modified: *2012-06-19*

If your organization has groups of people who answer and manage certain types of calls, such as for customer service, an internal help desk, or general telephone support for a department, you can deploy the Lync Server Response Group application to manage these types of calls. The Response Group application routes and queues incoming calls to designated persons, who are known as agents. You can increase the use of telephone support services and reduce the overhead of running these services by using response groups. This section describes planning considerations for Response Group.

- Overview of Response Groups
- Components Used by Response Group
- Technical Requirements for Response Groups
- Clients Supported for Response Group
- Capacity Planning for Response Group
- Deployment Process for Response Group

1.3.10.13.3.1 Overview of Response Groups

Overview of Response Groups

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Response Groups >

Topic Last Modified: *2012-09-11*

When a caller calls a response group, the call is routed to an agent based on a hunt group or the caller's answers to interactive voice response (IVR) questions. The Response Group application uses standard response group routing methods to route the call to the next available agent. Call routing methods include serial, longest-idle, parallel, round robin, and Attendant routing (that is, all agents are called at the same time for every incoming call, regardless of their current presence). If no agents are available, the call is held in a queue until an agent is available. While in the queue, the caller hears music until an available agent accepts the call. If the queue is full, or if the call times out while in the queue, the caller might hear a message and then is either disconnected or transferred to a different destination. When an agent accepts the call, the caller might or might not be able to see the agent's identity, depending on how the administrator configures the response group. Agents can either be formal, which means that they must sign in to the group before they can accept calls routed to the group, or informal, which means that they do not sign into and out of the group to accept calls.

Note:

Only on-premises users can be agents. If an agent is moved from on-premises to online, Response Group calls will not be routed to that agent.

Note:

The Response Group application uses an internal service, called Match Making, to queue calls and find available agents. Each computer that runs the Response Group application runs the Match Making service, but only one Match Making service per Lync Server pool is active at a time--the others are passive. If the active Match Making service becomes unavailable during an unplanned outage, one of the passive Match Making services becomes active. The Response Group application does its best to make sure that call routing and queuing continues uninterrupted. However, when a Match Making service transition occurs, any calls that are in transfer at the time are lost. For example, if the transition is due to the Front End Server going down, any calls currently being handled by the active Match Making service on that Front End Server are also lost.

In Lync Server 2013, two management roles are available for managing response groups: Response Group Manager and Response Group Administrator. Response Group Administrators can manage any aspect of any response group. Response Group Managers can manage only certain aspects, and only for the response groups that they own. The new Manager role can help reduce administration costs, because you can delegate limited responsibilities for specific response groups to any user who is enabled for Enterprise Voice.

To accommodate the new Manager role, Lync Server 2013 Response Group application introduces a **Workflow Type** of Managed or Unmanaged. The following table describes Managed and Unmanaged response groups.

Managed and Unmanaged Response Groups

Response group type	Description
Unmanaged	• Unmanaged response groups have no assigned Managers. Only the Response Group Administrator can configure these response groups. • Multiple unmanaged response groups can share a queue or agent group. • When you migrate response groups from a prior version to Lync Server 2013, the type is set to Unmanaged.
Managed	• Response Group Administrators can configure any aspect of managed response groups. • Response Group Managers cannot view or modify response groups that are not explicitly assigned to them. • Response Group Managers can configure only some settings for the response groups that are explicitly

	assigned to them. - Managed response groups can't share any queues or agent groups with any other response group, managed or unmanaged.

The following table describes the actions that Response Group Managers can and cannot perform for the response groups assigned to them.

Response Group Manager Capabilities

Can configure:	Can create, delete, or configure:	Cannot:
- Agents - Welcome message - Response Group name - Description - Display number - Business hours - Music on hold - Status (active/ inactive) - Hunt group workflows or Interactive voice response (IVR) workflows	- Agent Groups - Queues - Holiday sets	- Create or delete any type of workflow - Modify core response group settings, such as: **SIP URI**, **Telephone Number**, or **Workflow Type**.

Response Group Managers can use the following tools to manage their designated response groups.

- Lync Server Control Panel

✎**Note:**
Response Group Managers can only manage Response Group settings with this tool. Other Lync Server settings are not available to Managers.

- Response Group Configuration Tool
- Lync Server Management Shell

Response Group scales well to departmental or workgroup environments (for details, see Capacity Planning for Response Group) and can be deployed in entirely new telephony installations. It supports incoming calls from the Enterprise Voice deployment and from the local carrier network. Agents can use Lync 2013, Lync 2010, Lync 2010 Attendant, or Lync Phone Edition to take the calls routed to them.

The Response Group application is a component of Enterprise Voice. When you deploy Enterprise Voice, the Response Group application is installed and activated automatically.

1.3.10.13.3.2 Components Used by Response Group

Components Used by Response Group

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Response Groups >

Topic Last Modified: *2012-09-11*

The Response Group application is automatically enabled when you deploy Enterprise Voice. This section describes the components that support the Response Group application.

Response Group Components

The following Microsoft Lync Server 2013 components support the Response Group application:

- **Application service** Application service provides a platform for deploying, hosting, and managing unified communications applications, such as Response Group. The Application service is automatically installed on every Front End Server in a Front End pool and on every Standard Edition server.
- **Response Group application** The Response Group application is one of the unified communications applications that are hosted by Application service. It is included automatically when you deploy Response Group. The Response Group application routes and queues incoming calls to groups of agents.
- **Language pack** A language pack is required to support text-to-speech and speech recognition. These speech technologies are used when you configure messages, such as the welcome message and other prompts, and interactive voice response (IVR) questions and answers. By default, the 26 supported language packs are installed when you deploy Lync Server 2013.
- **Audio files** Audio files are used for messages and on-hold music.
- **File Store** Response Group uses File store to store audio files. Multiple Response Group pools can use the same instance of File store.
- **Response Group Configuration Tool** The Response Group Configuration Tool is a web-based tool that is used to create and configure response groups. The Response Group Configuration Tool is included when you install Web Services.
- **Microsoft Lync Server 2013 Control Panel** You can use Lync Server Control Panel to setup and configure agent groups and queues for response groups.
- **Lync Server Management Shell** All Response Group settings can be configured by using Lync Server Management Shell cmdlets.
- **Microsoft Lync 2013** Formal agents (agents who are required to sign in to the group before they can accept calls for the group) use Lync 2013 to sign in to and sign out from the group. If an agent group is configured for formal agents, the agents click a menu item in Lync 2013 to open Internet Explorer and display a webpage console for signing in and out of the group.
- **Web Services** Web Services is required for Response Group Configuration Tool, the agents' sign-in and sign-out console, Lync Server Control Panel, and Response Group client web service.
- **Response Group Client Web Service** Response Group application provides a client web service, which can be used by third-party applications to retrieve information about agents, agent group membership, agent sign-in status, call status for groups, and the groups that support anonymous calls. Lync 2013 and Lync 2010 Attendant use Response Group Client Web service to retrieve the list of response groups that agents can use to make anonymous calls. The client web service is included when you install Web Services.

1.3.10.13.3.3 Technical Requirements for Response Groups

Technical Requirements for Response Groups

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Response Groups >

Topic Last Modified: *2012-09-12*

This section describes the following technical requirements for the Response Group application:

- Hardware requirements
- Software requirements
- Port requirements
- Audio file requirements
- Response Group configuration tool requirements

Hardware Requirements

The Response Group application has the same hardware requirements as Front End Servers. For details about hardware requirements, see Server Hardware Platforms in the Supportability documentation.

Software Requirements

The Response Group application has the same operating system requirements and software prerequisites as Front End Servers. For details about software requirements, see Server and Tools Operating System Support in the Supportability documentation.

If you use Windows Media Audio (.wma) files for Response Group music and announcements, all Front End Servers or Standard Editions servers that run the Response Group application must have the Windows Media Format Runtime installed for servers running Windows Server 2008 R2, or Microsoft Media Foundation for servers running Windows Server 2012. For Windows Server 2008 R2, Windows Media Format Runtime is installed as part of Windows Desktop Experience.

For more details about audio requirements, see "Audio File Requirements" later in this section.

Port Requirements

The Response Group application uses the following ports:

- **Port 5071** Used for SIP listening requests
- **Port 8404** Used for interserver communications

  Note:

  This port is used for the Match Making service and is required when the Response Group application is deployed in a pool that has more than one Front End Server.

Note:

These ports are default settings that you can change by using the **Set-CsApplicationServer** cmdlet. For details about this cmdlet, see the Lync Server Management Shell documentation.

Audio File Requirements

The Response Group application supports wave (.wav) file format and Windows Media audio (.wma) file format for Response Group messages, on-hold music, or interactive voice response (IVR) questions.

The Windows Media audio file format requires that the Windows Media Format Runtime is installed on Front End Servers running Windows Server 2008 R2 and Windows Server 2008. For more details, see "Software Requirements" earlier in this section.

Supported Wave File Formats

All wave files must meet the following requirements:

- 8-bit or 16-bit file
- Linear pulse code modulation (LPCM), A-Law, or mu-Law format
- Mono or stereo
- 4MB or less

For the best performance of wave files, a 16 kHz, mono, 16-bit Wave file is recommended.

Supported Windows Media Audio File Formats

If you use a Windows Media audio file, consider using low bit rates, and verify the performance of your system under load.

You can use the Microsoft Expression Encoder 4 to convert a file to the Windows Media Audio format. To download Expression Encoder 4, see http://go.microsoft.com/fwlink/p/?linkId=202843.

Response Group Configuration Tool Requirements

The Response Group Configuration Tool supports the combinations of operating systems and web browsers described in the following table.

Note:
32-bit or 64-bit versions of the operating systems are supported. Only 32-bit versions of Internet Explorer are supported.

Supported Operating Systems and Web Browsers

Operating system	**Web browser**
Windows Vista with Service Pack (SP) 2	Internet Explorer 7 Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows 7 Windows 7 with Service Pack 1	Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows Server 2008 with Service Pack 2	Internet Explorer 7 Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows Server 2008 R2 Windows Server 2008 R2 with Service Pack 1	Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)

Response Group Agent Console

The agent console supports the combinations of operating systems and web browsers described in the following table.

Note:
32-bit or 64-bit versions of the operating systems are supported. Only 32-bit versions of Internet Explorer are supported.

Supported Operating Systems and Web Browsers

Operating system	Web browser
Windows Vista with Service Pack (SP) 2	Internet Explorer 7 Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows 7 Windows 7 with Service Pack 1	Internet Explorer 8 (native mode) Internet Explorer 9 (native mode) Firefox 10.0 Chrome 18.0
Windows Server 2008 with Service Pack 2	Internet Explorer 7 Internet Explorer 8 (native mode) Internet Explorer 9 (native mode)
Windows Server 2008 R2 Windows Server 2008 R2 with Service Pack 1	Internet Explorer 8 (native mode) Internet Explorer 9 (native mode) Firefox 10.0 Chrome 18.0

1.3.10.13.3.4 Clients Supported for Response Group

Clients Supported for Response Group

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Response Groups >

Topic Last Modified: *2012-12-04*

The Response Group application supports the following clients:

- Lync 2013
- Lync 2010
- Lync 2010 Attendant
- Office Communications Server 2007 R2 Attendant
- Lync Phone Edition

◆**Important:**

For details about new features, see New Response Group Application Features in the Getting Started documentation.

The specific client that you can use depends on the type of Response Group user that you are:

- **Callers** can call a response group by using any of the clients listed previously, and by using a standard telephone over the public switched telephone network (PSTN).

- **Informal agents** (agents who do not sign into and out of their groups to accept calls) can accept calls by using Attendant, Lync, or Lync Phone Edition. Informal agents are automatically signed into their groups when they sign in to Lync Server 2013 by using one of these clients.
- **Formal agents** (agents who must sign into and out of their groups to accept calls) can accept calls by using Lync 2013 and accessing the agent console from the menu item, or by using Attendant and accessing the agent console directly from Internet Explorer.

1.3.10.13.3.5 Capacity Planning for Response Group

Capacity Planning for Response Group

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Response Groups >

Topic Last Modified: *2012-10-29*

The following table describes the Response Group user model that you can use as the basis for capacity planning requirements.

Note:

The numbers in the following table assume that you use 16 kHz, mono, 16-bit Wave (.wav) files for all response group audio files. If you use other file formats, such as Windows Media Audio (.wma), the numbers may vary.

Important:

Keep in mind that for disaster recovery capacity planning, each pool of a paired pool should be able to handle the workloads for all the response groups in both pools.

Response Group User Model

Metric	Per Enterprise Edition pool (With 8 Front End Servers)	Per Standard Edition server
Incoming calls per second	16	2
Concurrent calls connected to IVR or MoH	480	60
Concurrent anonymous sessions (without IM)	224	28
Concurrent anonymous sessions (with IM)	64	8
Active agents (formal and informal)	1200	1200
Number of hunt groups	400	400
Number of IVR groups (use speech recognition)	200	200

1.3.10.13.3.6 Deployment Process for Response Group

Deployment Process for Response Group

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Response Groups >

Topic Last Modified: *2012-09-27*

This section provides an overview of the phases and steps involved in deploying the Response Group application.

Response Group Deployment Process

Phase	Steps	Permissions	Deployment documentation
Install the Response Group application	The Response Group application is installed and activated by default when you deploy Enterprise Voice.	RTCUniversalServerAdmins	Deploying Enterprise Voice
Install components for Response Group	Lync Server cmdlets, the Lync Server Control Panel, Response Group Configuration Tool, agents' sign-in and sign-out console, and Response Group Client Web service are installed as part of Web Services. Web Services is installed when you deploy an Enterprise Edition pool or a Standard Edition server.	RTCUniversalServerAdmins	Deploying Lync Server 2013
Enable users for Lync 2013 and for Enterprise Voice	Enable users who will be agents for Lync Server and Enterprise Voice. Users must be enabled before you can add them to agent groups. Typically, users are enabled for Lync Server during the Enterprise Edition or Standard Edition server deployment. Users are enabled for Enterprise Voice during the Enterprise Voice deployment.	RTCUniversalUserAdmins CsUserAdministrator CsAdministrator	Disable or Re-Enable User Account for Lync Server Enable Users for Enterprise Voice
Create and configure response groups, which consist of agent groups, queues, and workflows	1. Use the Lync Server Control Panel or Lync Server Management Shell to do the following: 1.a. Create and configure agent groups. 1.b. Create and configure queues. 2. Optionally, use Lync Server Management Shell to create predefined response group business hours and holidays. 3. Use the Response Group Configuration	RTCUniversalServerAdmins CsResponseGroupAdministrator CsVoiceAdministrator CsServerAdministrator CsAdministrator CsResponseGroupManager	Create Response Group Agent Groups Create Response Group Queues (Optional) Define Response Group Business Hours (Optional) Define Response Group Holiday Sets Create or Modify a Workflow

	Tool or Lync Server Management Shell to create workflows (hunt groups or interactive voice response (IVR) call flows), including custom response group business hours and holidays. **Note:** You can access the Response Group Configuration Tool through Lync Server Control Panel.		
(Optional) Customize application-level settings	Use Lync Server Management Shell to customize the default music-on-hold configuration, the default music-on-hold audio file, the agent ringback grace period, and the call context configuration.	RTCUniversalServerAdmins CsResponseGroupAdministrator CsVoiceAdministrator CsServerAdministrator CsAdministrator	Managing Application-Level Response Group Settings
(Optional) Delegate management of response groups	Assign users the CsResponseGroupManager role to delegate configuration of response groups. Response Group Managers can then configure the response groups assigned to them.	RTCUniversalServerAdmins CsResponseGroupAdministrator CsVoiceAdministrator CsServerAdministrator CsAdministrator	Planning for Role-Based Access Control
Verify your Response Group deployment	Test answering calls to your hunt group and interactive voice response workflows to ensure that your configuration works as expected.	-	-

1.3.10.13.4 Planning for Announcements

Planning for Announcements

Planning > Planning for Enterprise Voice > Planning for Call Management Features >

Topic Last Modified: *2012-09-13*

The Lync Server Announcement application lets you configure the handling of incoming phone calls when the dialed number is valid for your organization, but is not assigned to a user or a phone. You can transfer these calls to a predetermined destination (phone number, SIP URI, or voice mail), or play an audio announcement, or both. The Announcement application helps you avoid the situations in which a caller misdials and hears a busy tone or the SIP client receives an error message. This section includes planning information that is specific to the Announcement application.

- Overview of Announcements
- Components Used by Announcements
- Technical Requirements for Announcements
- Deployment Process for Announcements

1.3.10.13.4.1 Overview of Announcements

Overview of Announcements

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Announcements >

Topic Last Modified: *2012-09-13*

When you deploy the Announcement application, you need to configure an unassigned number table that determines the action to be taken when someone dials an unassigned number. The unassigned number table contains ranges of phone numbers that are valid for the organization and specifies which Announcement application handles each range. When a caller dials a telephone number that is valid for your organization but is not assigned to anyone, Lync Server looks up the number in the unassigned number routing table, identifies which range the number falls in, and routes the call to the Announcement application specified for that range. The Announcement application answers the call and plays an audio message (if you configured it to do so) and then either disconnects the call or transfers it to a predetermined destination, such as to an operator. You can use Lync Server Management Shell cmdlets to configure multiple audio messages or to transfer destinations.

How you configure the unassigned number table depends on how you want to use it. If you have specific numbers that are no longer in use and you want to play messages that are tailored for each number, you can enter those specific numbers in the unassigned number table. For example, if you changed the number for your customer service desk, you can enter the old customer service number and associate it with an announcement that gives the new number. If you want to play a general message to anyone who calls a number that is not assigned, such as for employees who have left your organization, you can enter ranges for all the valid extensions in your organization. The unassigned number table is invoked whenever the caller dials a number that is not currently assigned.

In Lync Server 2013, the Announcement application is automatically installed with the Response Group application. The Announcement and Response Group applications are standard components of an Enterprise Voice deployment: When you deploy Enterprise Voice, both of these applications are automatically deployed.

1.3.10.13.4.2 Components Used by Announcements

Components Used by Announcements

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Announcements >

Topic Last Modified: *2012-09-13*

In Lync Server 2013, the Announcement application is a component of the Response Group application. When you deploy Enterprise Voice, the Announcement application is automatically installed and activated along with the Response Group application. This section describes the components that support the Announcement application.

Announcement Application Components

The following Lync Server components support the Announcement application:

- **Application service** Application service provides a platform for deploying, hosting, and managing unified communications applications. Application service is automatically installed on every Front End Server in a Front End pool and on every Standard Edition server.
- **Response Group application** The Response Group application is one of the unified communications applications that are hosted by Application service. When an unassigned phone number range is configured to route to an announcement, the Response Group application is required to route the calls made to the phone number. (Response Group application is not required if all the ranges are configured to route to Exchange Unified Messaging (UM).)
- **Audio files** Audio files are used for the announcements.
- **File Store** The Announcement application uses File Store to store its audio files.
- **Lync Server Control Panel** You can use Lync Server Control Panel to configure the unassigned number table.
- **Lync Server Management Shell** You can use Lync Server Management Shell cmdlets to configure Announcement settings and the unassigned number table.

1.3.10.13.4.3 Technical Requirements for Announcements

Technical Requirements for Announcements

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Announcements >

***Topic Last Modified:** 2012-09-13*

This section describes the following technical requirements for the Announcement application:

- Hardware requirements
- Software requirements
- Port requirements
- Audio file requirements

Hardware Requirements

The Announcement application has the same hardware requirements as Front End Servers. For details about hardware requirements, see Server Hardware Platforms in the Supportability documentation.

Software Requirements

The Announcement application has the same operating system requirements and software prerequisites as Front End Servers. For details about software requirements, see Server and Tools Operating System Support in the Supportability documentation.

All Front End Servers or Standard Edition servers that run the Announcement application must have the Windows Media Format Runtime installed for servers running Windows Server 2008 R2, or Microsoft Media Foundation for servers running Windows Server 2012. For Windows Server 2008 R2, the Windows Media Format Runtime is installed as part of Windows Desktop Experience. Windows Media Format Runtime or Microsoft Media Foundation is required for Windows Media Audio (.wma) files that the Announcement application plays for announcements and music.

Port Requirements

The Announcement application uses the following port:

- **Port 5071** Used for SIP listening requests

Note:

This port is the default setting, which you can change by using the **Set-CsApplicationServer** cmdlet. For details about this cmdlet, see the Lync Server Management Shell documentation.

Audio File Requirements

The Announcement application supports Wave (.wav) file format and Windows Media audio (.wma) file format for music and announcements. Audio file requirements for the Announcement application are the same as for the Response Group application. For details, see Technical Requirements for Response Groups.

1.3.10.13.4.4 Deployment Process for Announcements

Deployment Process for Announcements

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Announcements >

Topic Last Modified: *2012-09-12*

This section provides an overview of the steps involved in deploying the Announcement application. You must deploy Enterprise Voice before you configure announcements. The components required by the Announcement application are installed and enabled when you deploy Enterprise Voice.

Announcement Deployment Process

Phase	Steps	Roles	Deployment documentation
Configure Announcement settings	• Create the announcement by recording and uploading audio files or by using text-to-speech (TTS). • Configure the unassigned number ranges in the unassigned number table and associate them with the	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator CsViewOnlyAdmini	Create an Announcement Configure the Unassigned Number Table

	appropriate announcement.	strator	
Verify your Announcement deployment	Test by listening to announcements to verify that your configuration works as expected.	-	(Optional) Verify Announcement Deployment

1.3.10.14 Planning for Enterprise Voice Resiliency

Planning for Enterprise Voice Resiliency

Microsoft Lync Server 2013 > Planning > Planning for High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-22*

Voice resiliency refers to the ability of users to continue making and receiving calls if a central site that hosts Microsoft Lync Server 2010 becomes unavailable, whether through a wide area network (WAN) failure or another cause. If a central site fails, Enterprise Voice service must continue uninterrupted through seamless failover to a backup site. In the event of WAN failure, branch site calls must be redirected to a local PSTN gateway. This section discusses planning for voice resiliency in the event of central-site or WAN failure.

- Planning for Central Site Voice Resiliency
- Planning for Branch-Site Voice Resiliency

1.3.10.14.1 Planning for Central Site Voice Resiliency

Planning for Central Site Voice Resiliency

See Also

Planning > Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency >

Topic Last Modified: *2012-09-28*

Increasingly, enterprises have multiple sites spread across the globe. Maintaining emergency services, access to help desk, and the ability to conduct critical business tasks when a central site is out of service is essential for any Enterprise Voice resiliency solution. When a central site becomes unavailable, the following conditions must be met:

- Voice failover must be provided.
- Users who ordinarily register with the Front End pool at the central site must be able to register with an alternative Front End pool. This can be done by creating multiple DNS SRV records, each of which resolves to a Director pool or Front End pool in each of your central sites. You can adjust the priority and weights of the SRV records so that users who are served by that central site get the corresponding Director and Front End pool ahead of those in other SRV records.
- Calls to and from users located at other sites must be rerouted to the PSTN.

This topic describes the recommended solution for securing central site voice resiliency.

Architecture and Topology

Planning for voice resiliency at a central site requires a basic understanding of the central role played by the Lync Server 2013 Registrar in enabling voice failover. The Lync Server Registrar is a server role that enables client registration and authentication and provides routing services. It resides along with other components on a Standard Edition server, Front End Server, Director, or Survivable Branch Appliance. A Registrar pool consists of Registrar Services running on the Front End pool and residing at the same site. The Front End pool must be load balanced. DNS load balancing is recommended, but hardware load balancing is acceptable. A Lync client discovers the Front End pool through the following discovery mechanism:

1. DNS SRV record
2. Autodiscovery Web Service (new in Lync Server 2013)
3. DHCP option 120

After the Lync client connects to the Front End pool, it is directed by the load balancer to one of the Front End Servers in the pool. That Front End Server, in turn, redirects the client to a preferred Registrar in the pool.

Each user enabled for Enterprise Voice is assigned to a particular Registrar pool, which becomes that user’s primary Registrar pool. At a given site, hundreds or thousands of users typically share a single primary Registrar pool. To account for the consumption of central site resources by any branch site users that rely on the central site for presence, conferencing, or failover, we recommend that you consider each branch site user as though the user were a user registered with the central site. There are currently no limits on the number of branch site users, including users registered with a Survivable Branch Appliance.

To assure voice resiliency in the event of a central site failure, the primary Registrar pool must have a single designated backup Registrar pool located at another site. The backup can be configured by using Topology Builder resiliency settings. Assuming a resilient WAN link between the two sites, users whose primary Registrar pool is no longer available are automatically directed to the backup Registrar pool.

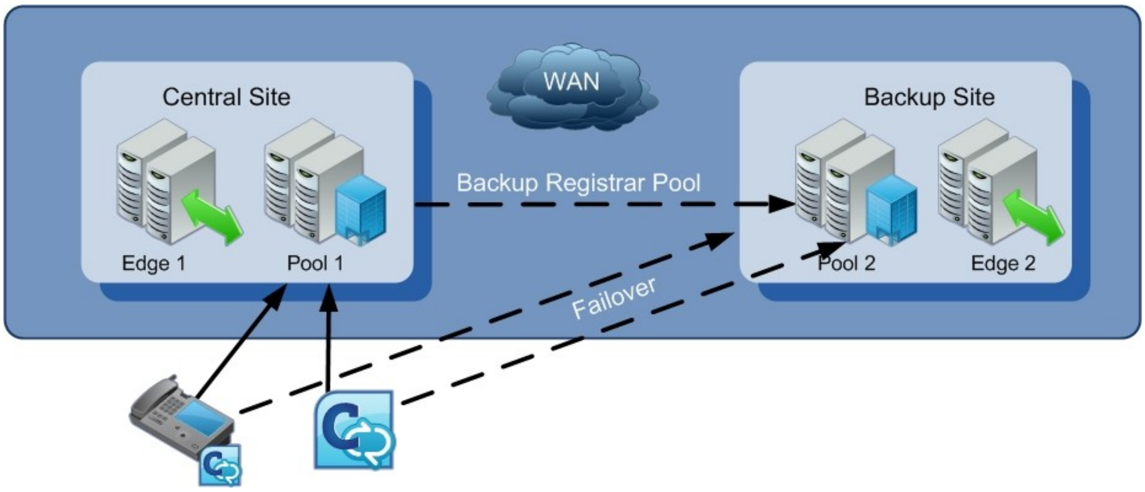
The following steps describe the client discovery and registration process:

1. A client discovers Lync Server through DNS SRV records. In Lync Server 2013, DNS SRV records can be configured to return more than one FQDN to the DNS SRV query. For example, if enterprise Contoso has three central sites (North America, Europe, and Asia-Pacific) and a Director pool at each central site, DNS SRV records can point to the Director pool FQDNs in each of the three locations. As long as the Director pool in one of the locations is available, the client can connect to the first hop Lync Server.

   Note:
   Using a Director pool is optional. A Front End pool can be used instead.

2. The Director pool informs the Lync client about the user’s primary Registrar pool and backup Registrar pool.
3. The Lync client attempts to connect to the user’s primary Registrar pool first. If the primary Registrar pool is available, the Registrar accepts the registration. If the primary Registrar pool is unavailable, the Lync client attempts to connect to the backup Registrar pool. If the backup Registrar pool is available and has determined that the user’s primary Registrar pool is unavailable (by detecting a lack of heartbeat for a specified failover interval) the backup Registrar pool accepts the user’s registration. After the backup Registrar detects that the primary Registrar is again available, the backup Registrar pool will redirect failover Lync clients to their primary pool.

The following figure shows the recommended topology for assuring central site resiliency. The two sites are connected by a resilient WAN link. If the central site becomes unavailable, users who are assigned to that pool are directed to the backup site for registration.



Requirements and Recommendations

The following requirements and recommendations for implementing central site voice resiliency are appropriate for most organizations:

- The sites in which the primary and backup Registrar pools reside should be connected by a resilient WAN link.
- Each central site must contain a Registrar pool consisting of one or more Registrars.
- Each Registrar pool must be load-balanced by using DNS load balancing or hardware load balancing.
- Each user must be assigned to a primary Registrar pool by using either the Lync Server Management Shell **set-CsUser** cmdlet or the Lync Server Control Panel.
- The primary Registrar pool must have a single backup Registrar pool located in a different central site.
- The primary Registrar pool must be configured to fail over to the backup Registrar pool. By default, the primary Registrar is set to fail over to the backup Registrar pool after an interval of 300 seconds. You can change this interval by using the Lync Server 2013 Topology Builder.
- Configure a failover route, as described in the "Configuring a Failover Route" topic in the Planning documentation. When configuring the route, specify a gateway that is located at a different site from the gateway specified in the primary route.
- If the central site contained your primary management server and the site is likely to be down for an extended period, you will need to reinstall your management tools at the backup site; otherwise, you won't be able to change any management settings.

Dependencies

Lync Server depends on the following infrastructure and software components to assure voice resiliency:

Component	**Functional**
DNS	Resolving SRV records and A records for server-server and server-client connectivity
Exchange and Exchange Web Services (EWS)	Contact storage; calendar data

Exchange Unified Messaging and Exchange Web Services	Call logs, voice mail list, voice mail
DHCP Options 120	If DNS SRV is unavailable, the client will attempt to use DHCP Option 120 to discover the Registrar. For this to work, either a DHCP server must be configured or Lync Server 2013 DHCP must be enabled. For details, see Hardware and Software Requirements for Branch-Site Resiliency in Branch-Site Resiliency Requirements section.

Survivable Voice Features

If the preceding requirements and recommendations have been implemented, the following voice features will be provided by the backup Registrar pool:

- Outbound PSTN calls
- Inbound PSTN calls, if the telephony service provider supports the ability to fail over to a backup site
- Enterprise calls between users at both the same site and between two different sites
- Basic call handling, including call hold, retrieval, and transfer
- Two-party instant messaging and sharing audio and video between users at the same site
- Call forwarding, simultaneous ringing of endpoints, call delegation, and team call services, but only if both parties to call delegation, or all team members, are configured at the same site.
- Existing phones and clients continue to work.
- Call detail recording (CDR)
- Authentication and authorization

Depending on how they are configured, the following voice features may or may not work when a primary central site is out of service:

- Voice mail deposit and retrieval
  If you want to make Exchange UM available when the primary central site is out of service, you must do one of the following:
  - Change DNS SRV records so that the Exchange UM servers at the central site point to backup Exchange UM servers at another site.
  - Configure each user’s Exchange UM dial plan to include Exchange UM servers at both the central site and the backup site, but designate the backup Exchange UM servers as disabled. If the primary site becomes unavailable, the Exchange administrator has to mark the Exchange UM servers at the backup site as enabled.

  If neither of the preceding solutions is possible, then Exchange UM will not be available in the event the central site becomes unavailable.
- Conferencing of all types
  A user who has failed over to a backup site can join a conference that is created or hosted by an organizer whose pool is available but cannot create or host a conference on his or her own primary pool, which is no longer available. Similarly, others users cannot join conferences that are hosted on the affected user’s primary pool.

The following voice features do not work when a primary central site is out of service:

- Conference Auto-Attendant
- Presence and DND-based routing
- Updating call forwarding settings
- Response Group service and Call Park

- Provisioning new phones and clients
- Address Book Web Search

⊟See Also

Other Resources

Planning for Branch-Site Voice Resiliency

1.3.10.14.2 Planning for Branch-Site Voice Resiliency

Planning for Branch-Site Voice Resiliency

Planning > Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency >

Topic Last Modified: *2012-09-21*

If you want to provide branch-site resiliency, that is, high-availability Enterprise Voice service, you have three options for doing so:

- Survivable Branch Appliance
- Survivable Branch Server
- A full Lync Server deployment at the branch site

This guide will help you evaluate which resiliency solution is best for your organization and, based on your resiliency solution, which PSTN-connectivity solution to use. It will also help you prepare to deploy the solution that you choose by describing prerequisites and other planning considerations.

- Branch-Site Resiliency Features
- Branch-Site Resiliency Solutions
- Branch-Site Resiliency Requirements

1.3.10.14.2.1 Branch-Site Resiliency Features

Branch-Site Resiliency Features

Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency > Planning for Branch-Site Voice Resiliency >

Topic Last Modified: *2012-10-10*

If you provide branch-site resiliency, if a branch site's WAN connection to a central site fails or if the central site is unreachable, the following voice features should continue to be available:

- Inbound and outbound public switched telephone network (PSTN) calls
- Enterprise calls between users at both the same site and between two different sites
- Basic call handling, including call hold, retrieval, and transfer
- Two-party instant messaging
- Call forwarding, simultaneous ringing of endpoints, call delegation, and team call services, but only if the delegator and delegate (for example, a manager and the manager's administrator), or all team members, are configured at the same site
- Call detail records (CDRs)
- PSTN dial-in conferencing with Conferencing Auto-Attendant
- Voice mail capabilities, if you configure voice mail rerouting settings. (For details, see Branch-Site Resiliency Requirements.)
- User authentication and authorization

The following features will be available only if your resiliency solution is a full-scale Lync Server deployment at the branch site:

- IM, web, and A/V conferencing
- Presence and Do Not Disturb (DND)-based routing (where calls are prevented from ringing on extensions that have DND activated)
- Updating call forwarding settings
- Response Group application and Call Park application
- Provisioning new phones and clients, but only if Active Directory Domain Services (AD DS) is present at the branch site.
- Enhanced 9-1-1 (E9-1-1)
  If E9-1-1 is deployed, and the SIP trunk at the central site is not available because the WAN link is down, then the Survivable Branch Appliance will route E9-1-1 calls to the local branch gateway. To enable this feature, the branch-site users' voice policies should route calls to the local gateway in the event of WAN failure.

1.3.10.14.2.2 Branch-Site Resiliency Solutions

Branch-Site Resiliency Solutions

See Also

Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency > Planning for Branch-Site Voice Resiliency >

Topic Last Modified: *2012-09-23*

There are obvious advantages to providing branch-site resiliency to your organization. Specifically, if you lose the connection to the central site, branch site users will continue to have Enterprise Voice service and voice mail (if you configure voice mail rerouting settings; for details, see Branch-Site Resiliency Requirements). However, for sites with fewer than 25 users, a resiliency solution may not provide a sufficient return on investment.

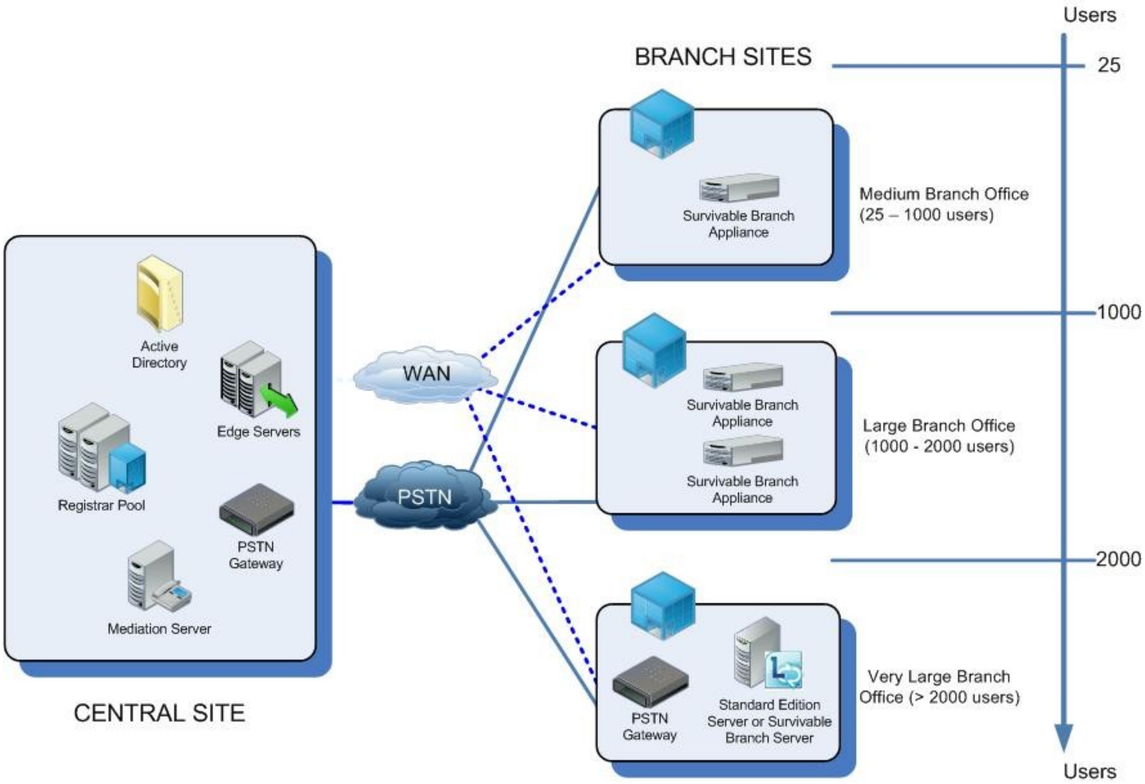
If you decide to provide branch-site resiliency, you have three options. The following table can help you determine the best option for your organization.

If you...	We recommend that you use a...
Host between 25 and 1000 users at your branch site, and if the return on investment does not support a full deployment or where local administrative support is unavailable	Survivable Branch Appliance The Survivable Branch Appliance is an industry-standard blade server with a Lync Server Registrar and Mediation Server running on Windows Server 2008 R2. The Survivable Branch Appliance also contains a public switched telephone network (PSTN) gateway. Qualified third-party devices (developed by Microsoft partners in the Survivable Branch Appliance (SBA) qualification/certification program) provide a continuous PSTN connection in the event of WAN failure, but this approach does not provide resilient presence and conferencing because these features depend on Front End Servers at the central site. For details about Survivable Branch Appliances, see "Survivable Branch Appliance Details," later in this topic.

	Note: If you decide to also use a SIP trunk with your Survivable Branch Appliance, contact your Survivable Branch Appliance vendor to learn about which service provider is best for your organization.
Host between 1000 and 2000 users at your branch site, lack a resilient WAN connection, and have trained Lync Server administrators available	Survivable Branch Server or two Survivable Branch Appliances. The Survivable Branch Server is a Windows Server meeting specified hardware requirements that has Lync Server Registrar and Mediation Server software installed on it. It must connect to either a PSTN gateway or a SIP trunk to a telephone service provider. For details about Survivable Branch Servers, see "Survivable Branch Server Details," later in this topic.
If you require presence and conferencing features in addition to voice features for up to 5000 users, and have trained Lync Server administrators available	Deploy as a central site with a Standard Edition server rather than as a branch site. A full-scale Lync Server deployment provides a continuous PSTN connection and resilient presence and conferencing in the event of WAN failure. For details about preparing for this solution, see Planning Primer: Planning for Your Organization, Determining Your System Requirements, Determining Your Infrastructure Requirements, and other relevant sections of the Planning documentation.

Resiliency Topologies

The following figure shows the recommended topologies for branch-site resiliency.


Users
BRANCH SITES
25
Survivable Branch Appliance
Medium Branch Office (25 – 1000 users)
1000
Survivable Branch Appliance
Survivable Branch Appliance
Large Branch Office (1000 - 2000 users)
2000
PSTN Gateway
Standard Edition Server or Survivable Branch Server
Very Large Branch Office (> 2000 users)
Users
Active Directory
Edge Servers
Registrar Pool
PSTN Gateway
Mediation Server
WAN
PSTN
CENTRAL SITE

Survivable Branch Appliance Details

The Lync Server Survivable Branch Appliance includes the following components:

- A Registrar for user authentication, registration and call routing
- A Mediation Server for handling signaling between the Registrar and a PSTN gateway
- A PSTN gateway for routing calls to the PSTN as a fallback transport in the event of a WAN outage
- SQL Server Express for local user data storage

The Survivable Branch Appliance also includes PSTN trunks, analog ports, and an Ethernet adapter.

If the branch site’s WAN connection to a central site becomes unavailable, internal branch users continue to be registered with the Survivable Branch Appliance Registrar and obtain uninterrupted voice service by using the Survivable Branch Appliance connection to the PSTN. Branch site users who connect from home or other remote locations will be able to register with a Registrar server at a central site if the WAN link to the branch site is unavailable. These users will have full unified communications functionality, with the one exception that inbound calls to the branch site will go to voice mail. When the WAN connection becomes available, full functionality should be restored to branch site users. Neither the failover to the Survivable Branch Appliance nor the restoration of service requires the presence of an IT administrator.

Lync Server supports up to two Survivable Branch Appliance at a branch site.

Survivable Branch Appliance Deployment Overview

The Survivable Branch Appliance is manufactured by original equipment manufacturers in partnership with Microsoft and deployed on their behalf by value-added retailers. This deployment should occur only after Lync Server has been deployed at the central site, a WAN connection to the branch site is in place, and branch site users are enabled for Enterprise Voice.

For details about these phases, see Deploying a Survivable Branch Appliance or Server in the Deployment documentation.

Phase	Steps	User Rights
Set up Active Directory Domain Services for the Survivable Branch Appliance	**At the central site:** 1. Create a domain user account (or enterprise identity) for the technician who will install and activate the Survivable Branch Appliance at the branch site. 2. Create a computer account (with the applicable fully qualified domain name (FQDN)) for Survivable Branch Appliance in Active Directory Domain Services. 3. In Topology Builder, create and publish the Survivable Branch Appliance.	The technician user account must be a member of RTCUniversalSBATechnicians. The Survivable Branch Appliance must belong to the RTCSBAUniversalServices group, which happens automatically when you use Topology Builder.
Install, and activate the Survivable Branch Appliance.	**At the branch site:** 1. Connect the Survivable Branch Appliance to an Ethernet port and PSTN port. 2. Start the Survivable Branch Appliance. 3. Join the Survivable Branch Appliance to the domain, using the domain user account created for the Survivable Branch Appliance at the central site. Set the FQDN and IP address to match the FQDN created in the computer account. 4. Configure the Survivable Branch Appliance using the OEM user interface. 5. Test PSTN connectivity.	The technician user account must be a member of RTCUniversalSBATechnicians.

Survivable Branch Server Details

In Topology Builder create the branch site, add the Survivable Branch Server to that site, and then run the Lync Server Deployment Wizard on the computer where you want to install the role.

⊟See Also

Other Resources

Deploying Lync Server 2013

1.3.10.14.2.3 Branch-Site Resiliency Requirements

Branch-Site Resiliency Requirements

Planning for High Availability and Disaster Recovery > Planning for Enterprise Voice Resiliency > Planning for Branch-Site Voice Resiliency >

Topic Last Modified: *2012-10-18*

This topic will help you to prepare users for branch-site resiliency and voice mail survivability, and also specifies the relevant hardware and software requirements.

Preparing Branch Users for Branch-Site Resiliency

Prepare users for branch-site resiliency by setting their Registrar pool as the Survivable Branch Appliance (SBA) or Survivable Branch Server.

Registrar Assignments for Branch Users

Regardless of which branch-site resiliency solution you choose, you will need to assign a primary Registrar to each user. Branch site users should always register with the Registrar at the branch site, regardless of whether that Registrar resides in the Survivable Branch Appliance, Survivable Branch Server, or stand-alone Lync Server 2013 Standard or Enterprise Edition server. A domain name system (DNS) service (SRV) resource record is required so that a client can discover its Registrar pool. If the Survivable Branch Appliance becomes unavailable, this is how branch site clients will automatically discover the backup Registrar.

If a branch site does not have a DNS server, there are two alternative ways to configure discovery of the Survivable Branch Appliance or Survivable Branch Server:

- Configure DHCP option 120 on the branch site’s Dynamic Host Configuration Protocol (DHCP) server to point to the fully qualified domain name (FQDN) of the Survivable Branch Appliance or Survivable Branch Server.
- Configure the Survivable Branch Appliance or Survivable Branch Server to respond to DHCP 120 queries.

Voice Routing for Branch Users

We recommend that you create a separate user-level Voice over Internet Protocol (VoIP) policy for users in a branch site. This policy should include a primary route that uses the Survivable Branch Appliance or branch server gateway, and one or more backup routes that use a trunk with a public switched telephone network (PSTN) gateway at the central site. If the primary route is unavailable, the backup route that uses one or more central site gateways is used instead. This way, regardless of where a user is registered—on the branch site Registrar or the backup Registrar pool at the central site—the user’s VoIP policy is always in effect. This is an important consideration for failover scenarios. For example, if you need to rename the Survivable Branch Appliance or reconfigure the Survivable Branch Appliance to connect to a backup Registrar pool at the central site, then you must move branch site users to the central site for the duration. (For details about renaming or reconfiguring a Survivable Branch Appliance, see Appendix B: Managing a Survivable Branch Appliance in the Deployment documentation.) If those users do not have user-level VoIP policies or user-level dial plans, when the users are moved to another site, the site-level VoIP policies and site-level dial plans of the central site apply to the users by default, instead of the branch site site-level VoIP policies and dial plans,. In this scenario, unless the site-level VoIP policies and site-level dial plans used by the backup Registrar pool can also apply to the branch site users, their calls will fail. For example, if users from a branch site located in Japan are moved to a central site in Redmond, then a dial plan with normalization rules that prepend +1425 to all 7-digit calls is unlikely to appropriately translate calls for those users.

Important:

When you create a branch office backup route, we recommend that you add two PSTN phone usage records to the branch office user policy and assign separate routes to each one. The first, or primary, route would direct calls to the gateway associated with the Survivable Branch Appliance (SBA) or branch server; the second, or backup, route would direct calls to the gateway at the central site. In directing calls, the SBA or branch server will attempt all routes assigned to the first PSTN usage record before attempting the second usage record.

To help ensure that inbound calls to branch site users will reach those users when the branch gateway or the Windows component of the Survivable Branch Appliance site is unavailable (which would happen, for example, if the Survivable Branch Appliance or branch gateway were down for maintenance), create a failover route on the gateway (or work with your Direct Inward Dialing (DID) provider) to redirect incoming calls to the backup Registrar pool at the central site. From there, the calls will be routed over the WAN link to branch users. Be sure that the route translates numbers to comply with the PSTN gateway or other trunk peer's accepted phone number formats. For details about creating a failover route, see Configuring a Failover Route. Also create service-level dial plans for the trunk associated with the gateway at the branch site to normalize incoming calls. If you have two Survivable Branch Appliances at a branch site, you can create a site-level dial plan for both unless a separate service-level plan for each is necessary.

Note:

To account for the consumption of central site resources by any branch site users that rely on the central site for presence, conferencing, or failover, we recommend that you consider each branch site user as if the user were registered with the central site. There are currently no limits on the number of branch site users, including users registered with a Survivable Branch Appliance.

We also recommend that you create a user-level dial plan and voice policy, and then assign it to branch site users. For details, see Create a Dial Plan and Create the VoIP Routing Policy for Branch Users in the Deployment documentation.

Routing Extension Numbers

When preparing dial plans and voice policies for branch site users, be sure to include normalization rules and translation rules that match the strings and number format used in the msRTCSIP-line (or Line URI) attribute, so that Lync 2013 calls enabled between branch site users and central site users will be routed correctly—particularly when calls must be rerouted over the PSTN because the WAN link is unavailable. Additionally, there are special considerations for dialed numbers that include extension numbers, rather just phone numbers.

Normalization rules and translations rules that match Line URIs that contain an extension number, whether exclusively or in addition to a full E.164 phone number, have additional requirements. This section describes several example scenarios to route calls for Line URIs with an extension number.

If your organization does not have Direct Inward Dial (DID) phone numbers configured for individual users and the Line URI of each user is configured with *only* an extension number, internal users can call one another by dialing only an extension number. However, you must configure normalization rules that can apply to calls from a branch site user to a central site user, that match the extension numbers.

In a scenario where the WAN link between a branch site and a central site is available, calls from branch site users to central site users do not require the matching normalization rule to translate the number because the call is not routed over the PSTN. For example:

Rule name	Description	Number pattern	Translation	Example

5digitExtensions	Does not translate 5-digit numbers	^(\d{5})$	$1	10001 is not translated

You must also accommodate extension numbers for specific scenarios, such as when the WAN link between a branch site and central site is unavailable and a call from a branch site must be routed over the PSTN. During a WAN outage, if a branch site user calls a central site user only by dialing the central site user's extension, you must have an outbound translation rule that adds the central site user's full phone number. If a user's Line URI contains your organization's full phone number and the user's unique extension number instead of a full phone number that is unique to the user, then you must have an outbound translation rule that adds your organization's full phone number instead. For example:

Description	Matching pattern	Translation	Example
Translates 5-digit numbers to a user's phone number and extension	^(\d{5})$	+14255550123;ext=$1	10001 is translated to +14255550123;ext=10001
Translates 5-digit numbers to your organization's phone number and a user's extension	^(\d{5})$	+14255550100;ext=$1	10001 is translated to +14255550100;ext=10001

In this scenario, if the trunk peer that handles rerouting to the PSTN does not support extension numbers, then the outbound translation rule must also remove the extension number. For example:

Description	Matching pattern	Translation	Example
Removes extension from phone numbers with extensions	^\+(\d*);ext=(\d*)$	+$1	+14255550123;ext=10001 is translated to +14255550123

Whether or not a WAN link is available, if your organization does not have DID numbers configured for individual users and the Line URI for a user contains your organization's phone number and the user's unique extension number, then you must configure your organization's phone number Line URI with a number that is reachable by the trunk peer or PSTN gateway at the branch site. You must also configure your organization's phone number Line URI to include its own unique extension for calls to be routed to that number.

For details about calls from a central site user to a branch site user when the WAN link between the sites is unavailable, see "Preparing for Voice Mail Survivability" later in this topic. For details about dial plans and normalization rules, including other sample rules, see Dial Plans and Normalization Rules in the Planning documentation and Configuring Dial Plans in the Deployment documentation. For details about outbound translation rules, see Translation Rules in the Planning documentation and Defining Translation Rules in the Deployment documentation.

Preparing for Voice Mail Survivability

Exchange Unified Messaging (UM) is usually installed only at a central site and not at branch sites. A caller should be able to leave a voice mail message, even if the WAN link between branch site and central site is unavailable. As a result, configuring the Line URI for the Exchange UM Auto Attendant phone number that provides voice mail for branch site users requires special considerations, in addition to the voice policy, dial plan, and normalization rules applicable to that voice mail number.

Survivable Branch Appliances (SBAs) and Survivable Branch Servers provide voice mail survivability for branch users during a WAN outage. Specifically, if you are using a Survivable Branch Appliance or Survivable Branch Server and the WAN becomes unavailable, the SBA or Survivable Branch Server reroutes unanswered calls over the PSTN to Exchange UM at the central site. With a SBA or Survivable Branch Server, users can also retrieve voice mail messages through the PSTN during a WAN outage. Finally, during a WAN outage the Survivable Branch Appliance or Survivable Branch Server queues missed-call notifications and then uploads them to the Exchange UM server when the WAN is restored. To help ensure that voice mail rerouting is resilient, be sure that you add an entry for the central site pool’s FQDN and an entry for the Edge Server FQDN to the hosts file on the Survivable Branch Server. Otherwise, DNS resolution can time out if you do not have a DNS server at the branch site.

We recommend the following configurations for voice mail survivability for branch site users:

- An Microsoft Exchange administrator should configure Exchange UM Auto Attendant (AA) to accept messages only. This configuration disables all other generic functionality, such as transfer to a user or transfer to an operator, and limits the AA to only accepting messages. Alternatively, the Exchange administrator can use a generic AA or an AA customized to route the call to an operator.
- The Lync Server administrator should take the AA phone number and use that phone number as the **exchange um auto attendant** number in the voice mail rerouting settings for the Survivable Branch Appliance or branch server.
- The Lync Server administrator should get the Exchange UM subscriber access phone number and use that number as the **subscriber access** number in the voice mail rerouting settings for the Survivable Branch Appliance or Survivable Branch Server.
- The Lync Server administrator should configure Exchange UM so that only one dial plan is associated with all branch users who need access to voice mail during a WAN outage.
- When the WAN link is unavailable, calls to branch site users can be routed to the user’s Exchange Unified Messaging (UM) voice mailbox, but only if the voice policy applied to the call specifies a voice mail phone number that is unique and does not include an extension number.

Hardware and Software Requirements for Branch-Site Resiliency

The hardware and software requirements vary, depending on your resiliency solution.

Requirements for Survivable Branch Appliances

Required hardware and software is built into the Survivable Branch Appliance. However, we also recommend that each branch site deploy a DHCP server to obtain client IP addresses; otherwise, when the DHCP lease expires, clients will not have IP connectivity.

If the enterprise DNS servers are located only in central sites, branch site users will be unable to access them during a WAN outage, and therefore Lync Server discovery that uses DNS SRV (service (SRV) resource record) will fail. To assure prompt rerouting during a WAN outage, DNS records must be cached at the branch site. If the branch router supports it, turn on DNS caching. Or, you can deploy a DNS server at the branch. This can be a stand-alone server or a version of the Survivable Branch Appliance that supports DNS capabilities. For details, contact your Survivable Branch Appliance provider.

Note:

It is not necessary to have a domain controller at a branch site. The Survivable Branch Appliance authenticates clients by using a special certificate that it sends the client in response to the client’s certificate request when it signs in.

Lync clients can discover the Lync Server by using DHCP Option 120 (SIP Registrar Option). This can be configured in one of two ways:

- Configure the DHCP server at the branch site to reply to DHCP 120 queries, which return the FQDN of the Registrar on the Survivable Branch Appliance or Survivable Branch Server.
- Turn on Lync Server DHCP. When this is turned on, the Lync Server Registrar responds to DHCP Option 120 queries. Note that the Registrar does not respond to any DHCP queries other than DHCP Options 120.

Additionally, for larger branch sites that have multiple subnets, DHCP relay agents should be enabled to forward DHCP Option 120 queries to the DHCP Server (configuration 1) or to the Registrar (configuration 2).

Finally, branch site users must be configured for Enterprise Voice and provisioned with an appropriate unified communications endpoint.

Requirements for Survivable Branch Servers

The requirements for Survivable Branch Servers are the same as the requirements for any Lync Server server role. For details, see Determining Your Infrastructure Requirements in the Planning documentation.

Requirements for Full-Scale Lync Server Branch-Site Deployments

For details, see Determining Your Infrastructure Requirements in the Planning documentation.

Configuring a Failover Route

Planning for Enterprise Voice Resiliency > Planning for Branch-Site Voice Resiliency > Branch-Site Resiliency Requirements >

Topic Last Modified: *2012-09-21*

The following example shows how an administrator can define a failover route for use if the Dallas-GW1 is down for maintenance or is otherwise unavailable. The following tables illustrate the required configuration change.

Table 1. User Policy

User policy	Phone usage
Default Calling Policy	Local GlobalPSTNHopoff
Redmond Local Policy	RedmondLocal
Dallas Calling Policy	DallasUsers GlobalPSTNHopoff

Table 2. Routes

Route name	Number pattern	Phone usage	Trunk	Gateway
Redmond Local Route	^\+1(425|206|253)(\d{7})$	Local RedmondLocal	Trunk1 Trunk2	Red-GW1 Red-GW2

Dallas Local Route	^\+1(972|214|469)(\d{7})$	Local	Trunk3	Dallas-GW1
Universal Route	^\+?(\d*)$	GlobalPSTNHopoff	Trunk1 Trunk2 Trunk3	Red-GW1 Red-GW2 Dallas-GW1
Dallas Users Route	^\+?(\d*)$	DallasUsers	Trunk3	Dallas-GW1

In Table 1, a phone usage of GlobalPSTNHopoff is added after the DallasUsers phone usage in the Dallas Calling Policy. This enables calls with the Dallas Calling policy to use routes that are configured for the GlobalPSTNHopoff phone usage if a route for the DallasUsers phone usage is unavailable.

1.3.10.15 Deployment Guidelines for Enterprise Voice

Deployment Guidelines for Enterprise Voice

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-09-21*

This topic describes prerequisites and other guidelines to consider when you are planning to deploy Lync Server 2013 and the Enterprise Voice workload.

Deployment Prerequisites

For an optimum experience when deploying Enterprise Voice, make sure that your IT infrastructure, network, and systems meet the following prerequisites:

- Lync Server 2013 Standard Edition or Enterprise Edition is installed and operational on your network.
- All Edge Servers are deployed and operational in your perimeter network, including Edge Servers with Access Edge service, A/V Edge service, Web Conferencing Edge service, and a reverse proxy.
- One or more users have been created and enabled for Lync Server.
- Microsoft Exchange Server 2007 Service Pack 1 (SP1) or latest service pack, or Microsoft Exchange Server 2010 is installed. One of these is required for integrating Exchange Unified Messaging (UM) with Lync Server and to provide rich notifications and call log information to client endpoints.
- A unique primary phone number has been designated, normalized, and copied to the **msRTCSIP-line** attribute for each user who is to be enabled for Enterprise Voice.

> **Note:**
>
> Lync Server supports E.164 numbers and non-Direct Inward Dialing (DID) numbers. Non-DID numbers can be represented in the format **<E.164>;ext=<extension>** or as a string of digits, with the requirement that the private extension is unique across the enterprise. For example, a private number of 1001 can be represented as **+1425550100;ext=1001**, or as **1001**. When represented as **1001**, the expectation is that this private number is unique across the enterprise.

- Administrators who deploy Enterprise Voice should be members of the RTCUniversalServerAdmins group.

- At a minimum, Office Communicator 2007 is successfully deployed. To use features new to this release, Lync 2013 is deployed.
- Managed key infrastructure (MKI) is deployed and configured, using either a Microsoft or a third-party certification authority (CA) infrastructure.
- Each computer on which you install Mediation Server must be:
  - A member server of a domain, and prepared for Active Directory Domain Services (AD DS). For Active Directory Domain Services (AD DS) preparation procedures, see Preparing Active Directory Domain Services for Lync Server 2013 in the Deployment documentation.
  - Running one of the following operating systems:
    - The 64-bit edition of the Windows Server 2008 Standard operating system
    - The 64-bit edition of the Windows Server 2008 Enterprise operating system
- If the connection to the public switched telephone network (PSTN) or private branch exchange (PBX) is by means of a Time Division Multiplexing (TDM) connection, one or more PSTN gateways are available for deployment. (If the connection is by means of a SIP trunk, a PSTN gateway is not required.)

Power, Network, or Telephone Service Outages

If there is an outage, disruption, or other degradation of the power, network, or telephone services at your location, the voice, instant messaging, presence, and other features of Lync Server and any device connected to Lync Server may not work properly.

Enterprise Voice Depends on Server Availability and Voice Client and Hardware Operability

Voice communications with Lync Server depend upon the availability of the server software and the proper functioning of the voice clients or the hardware phone devices connecting to the server software.

Alternative Means of Accessing Emergency Services

For those locations where you install a voice client (for example, a PC running Lync client or an Lync Phone Edition device), we recommend that you maintain a backup option for users to call emergency services (for example, 911 or 999) in case of a power failure, network connectivity degradation, telephone service outage, or other issue that may inhibit operation of Lync Server, Lync, or Lync Phone Edition devices. Such alternative options could include a telephone connected to a standard public switched telephone network line or a cell phone.

Emergency Calls and Multi-Line Telephone Systems

The use of a multiline telephone system (MLTS) may be subject to U.S state or federal laws or the laws of other countries/regions that require the MLTS to provide a caller's telephone number, extension, and/or physical location to applicable emergency services when a caller is placed to emergency services (for example, when dialing an emergency access number such as 911 or 999). In this release, Lync Server can be configured to provide a caller's physical location to an emergency services provider, as described in Planning for Emergency Services (E9-1-1). Compliance with MLTS laws is the sole responsibility of the purchaser of Lync Server, Lync client, and Lync Phone Edition devices.

1.3.10.16 Deployment Process Overview for Enterprise Voice

Deployment Process Overview for Enterprise Voice

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-09-22*

The deployment and configuration steps that you need to follow are dependent on the Enterprise Voice feature or functionality you are adding to your Lync Server 2013 environment.

Feature Deployment Overviews

For an overview of deploying PSTN connectivity, see the following:

- SIP Trunk Deployment Checklist
- Direct SIP Deployment Options
- Planning Outbound Voice Routing

For an overview of deploying Exchange Unified Messaging (UM), see the following:

- Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013

For an overview of deploying call admission control, see the following topics:

- Deployment Checklist for Call Admission Control

For an overview of the deployment process for Emergency Services, see the following:

- Defining Your Requirements for Emergency Calls
- Choosing an E9-1-1 Service Provider
- Deployment Checklist for E9-1-1

For an overview of deploying private telephone lines, see the "Private Telephone Lines in Mixed Deployments" section of Planning for Private Telephone Lines.

For an overview of the deployment of call handling features (call parking, announcement application, and response groups), see the following:

- Deployment Process for Call Park
- Deployment Process for Announcements

1.3.10.17 Moving Users to Enterprise Voice

Moving Users to Enterprise Voice

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-10-18*

If you are moving users from an existing PBX telephony infrastructure to Enterprise Voice, the deployment process includes some steps that are not part of the planning process already described in Planning for Enterprise Voice. For information about migrating users from an earlier Enterprise Voice deployment, see the migration documents that were included with your installation media.

The process of moving users from an existing telephony infrastructure to Enterprise Voice consists of the following steps:

1. Designate primary phone numbers.
2. Enable users for Enterprise Voice.
3. Prepare dial plans for users.
4. Plan user voice policies.
5. Plan call routes.
6. Configure PBX or SIP Trunk to reroute calls for users enabled for Enterprise Voice.
7. Move users to Exchange Unified Messaging (UM) (recommended).

This topic describes the planning that is necessary for each of these steps.

Step 1. Designate primary phone numbers

Enterprise Voice integrates voice with other messaging media, such that when an incoming call arrives at the server, the server maps the number to the user's SIP-URI and then forks the call to all the client endpoints associated with that SIP-URI. This process requires that each user be associated with a primary phone number.

A primary phone number must be:

- Globally unique or, in the case of internal extensions, unique in the enterprise.
- Owned by and routable in the enterprise. Personal numbers should not be used.

Enterprise users can have two or more telephone numbers listed for them in Active Directory Domain Services (AD DS). All the telephone numbers associated with a particular user can be viewed or changed on the property sheet for that user in the Active Directory Users and Computers snap-in.

The **Telephone number** box on the **General** tab of the **User Properties** dialog box should contain the user's main work number. This number will usually be designated as the user's Primary Phone Number.

Some users may have special requirements (for example, an executive who wants all incoming calls routed through an administrative assistant), but such exceptions should be limited only to those where the need is clear and critical.

After a primary number is chosen, it must be:

- Normalized to E.164 format, wherever possible.
- Copied to the Active Directory **msRTCSIP-line** attribute.

Note:

Coexisting with remote call control (RCC)

RCC is the ability to use Lync Server to monitor and control a desktop PBX phone. Control is routed through the server, which acts as a gateway to the PBX. Although you cannot configure a user for both RCC and Enterprise Voice, the Line URI setting designates a user's primary phone number in either case.

If you have an existing PBX infrastructure that you want selected users to continue using, you can introduce Enterprise Voice incrementally into your organization. For details about this deployment scenario, see Direct SIP Deployment Options in the Planning documentation.

In previous releases, you could enable both RCC and Enterprise Voice for a user, but only if you also configured the user for dual forking, a feature in which an incoming call will ring a user's PBX phone and Communicator simultaneously. In Lync Server 2010, dual-forking is not supported.

There are three methods for populating the **msRTCSIP-line** attribute:

- Microsoft Identity Integration Server (recommended)
- The **Users** page in the Lync Server Control Panel

Where many phone numbers must be processed, a script custom developed by your organization is the better choice. Depending on how your organization represents telephone numbers in Active Directory Domain Services, the script may have to normalize primary phone numbers to E.164 format before copying them to the **msRTCSIP-line** attribute.

- If your organization maintains all telephone numbers in Active Directory Domain Services in a single format, and if that format is E.164, your script only needs to write each Primary Telephone Number to the **msRTCSIP-line** attribute.
- If your organization maintains all telephone numbers in Active Directory Domain Services in a single format, but that format is not E.164, your script should define an appropriate normalization rule to convert Primary Telephone Numbers from their existing format to E.164 before writing them to the **msRTCSIP-line** attribute.
- If your organization does not enforce a standard format for telephone numbers in Active Directory Domain Services, your script should define appropriate normalization rules to convert Primary Phone Numbers from their various formats to E.164 compliance before writing the Primary Telephone Numbers to the **msRTCSIP-line** attribute.

Your script will also have to insert the prefix **Tel:** before each primary number before writing it to the **msRTCSIP-line** attribute.

The expected format of the number specified in this attribute is:

- Tel:+14255550100;ext=50100.
- Tel:5550100 (for unique enterprise wide extensions)

Important:

The normalization performed by the Address Book Service (ABS) does not replace or otherwise eliminate the need to normalize each user's primary phone number in Active Directory Domain Services because ABS does not have access to Active Directory Domain Services and therefore cannot copy primary numbers to the **msRTCSIP-line** attribute.

Step 2. Enable users for Enterprise Voice

Other than identifying which users are to be enabled, no special planning is required to complete this step.

Step 3. Prepare dial plans for users.

Users who are enabled for Enterprise Voice will not be able to make calls to the PSTN without dial plans in place. A dial plan is a named set of normalization rules that translates phone numbers for a named location, individual user, or contact object into a single standard (E.164) format for purposes of phone authorization and call routing. Normalization rules define how phone numbers expressed in various formats are to be routed for each specified location, user, or contact object.

For information about preparing dial plans, see Dial Plans and Normalization Rules.

Step 4. Plan user voice policies

User class-of-service settings on a legacy PBX, such as the right to make long-distance or international calls from company phones, must be reconfigured as VoIP policies for users moved to Enterprise Voice. For details about planning and creating policies for Enterprise Voice, see Voice Policies.

Step 5. Plan outbound call routes

Call routes specify how Lync Server handles outbound calls placed by Enterprise Voice users. When a user dials a number, the server, if necessary, normalizes the dial string to E.164 format and attempts to match it to a SIP URI. If the server is unable to make the match, it applies outgoing call routing logic based on the number. The final step in defining that logic is creating a separate named call route for each set of destination phone numbers that are listed in each dial plan.

For details about planning call routes, see Voice Routes.

Step 6. Configure PBX or SIP Trunk to reroute calls for Enterprise Voice users

Users who formerly were hosted on a traditional PBX or on a SIP Trunk connection to an Internet Telephony Service Provider (ITSP) retain their phone numbers after the move. The only requirement is that after the move, the PBX or SIP Trunk must be reconfigured to route incoming calls for Enterprise Voice users to the Mediation Server.

Step 7. Move users to Exchange Unified Messaging (recommended)

Moving users to Exchange Unified Messaging consists of the following tasks:

- Configure Exchange Unified Messaging and Lync Server to work together.
- Enable users for Exchange Unified Messaging call answering and Outlook Voice Access. This task is performed on the Exchange Unified Messaging server. For details, see the Exchange Server 2010 TechNet Library at http://go.microsoft.com/fwlink/p/?linkID=139372.

1.3.11 Planning for Monitoring

Planning for Monitoring

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-05*

The monitoring service in Microsoft Lync Server 2013 provides a way for administrators to collect usage, trend, and quality of service data for the communication sessions that take place in their organization. Monitoring in Lync Server 2013 no longer requires a separate server role; instead, the monitoring service is built into each Front End server. However, by default monitoring is not enabled in Lync Server 2013. This document will help you determine whether or not monitoring should be enabled in your organization.

- Overview of Monitoring
- Defining Your Organizations's Requirements for Monitoring
- Enabling Monitoring

- Accessing Monitoring Data
- Components and Topologies for Monitoring
- Deployment Checklist for Monitoring

1.3.11.1 Overview of Monitoring

Overview of Monitoring

Microsoft Lync Server 2013 > Planning > Planning for Monitoring >

Topic Last Modified: *2012-09-05*

In Microsoft Lync Server 2013, monitoring is used to collect usage information and Quality of Experience (QoE) data about the communication sessions that your users are involved in. A session is a generic term that covers a user’s connection to a:

- Conference
- Conferencing modality (such as Audio/Video or Application Sharing)
- Another user via a peer-to-peer conversation such as instant messaging or an audio call

Note:

Lync Server 2013 keeps track of information about each session: who called who; which endpoints were used in the session; how long did the session last; what was the perceived quality of the session; and so on. However, Lync Server does not record and store the actual call itself. That includes instant messaging sessions as well: although Lync Server records information about instant messaging sessions, it does not maintain a record of each instant message that was sent during the session.

The call detail information collected by Lync Server can be employed for any number of uses, including:

- **Return on Investment (ROI)**. Administrators can compare the usage data collected by Monitoring Server to similar data collected for their previous telephony system in order to show cost savings and help justify the deployment of Lync Server.
- **Device Inventory Management**. Asset management information helps administrators identify old devices still in use that need to be replaced, as well as identify expensive devices that do not appear to be getting used at all.
- Help Desk. Troubleshooting data enables support engineers to determine why a user’s call failed, and to do so without having to collect server or client side logs. This information can be readily accessed and understood by support personnel who do not have a deep technical knowledge of Microsoft Lync 2013 and Lync Server 2013.
- **System Troubleshooting**. Enables administrators to detect major issues that might prevent end users from performing basic tasks like joining a conference, establishing a call, or sending an instant message.

In addition to this basic call information, the Monitoring Server also provides a mechanism that allows SIP endpoints (such as Lync 2013) to provide troubleshooting information that the server would not otherwise have access to:

- **Media Metrics that Impact Quality**. These metrics deal with the actual transmission of the call itself; that is, they provide a sort of travel log as the call journeys across the network. These metrics (which include such things as packet loss, jitter, and round trip times) provide information on what happened to the call from the time it left your endpoint to the time it arrived at the other person's endpoint.
- **Issues Reported to the End User**. These metrics include poor quality notifications that Lync 2013 presents to end users in cases where they are too far from a microphone, speaking too softly, have a poor network connection, or are experiencing poor quality because another program on the

computer is consuming the available resources.

- **Environment Information**. These metrics detail call quality factors such as the type of microphone and speakers being used, whether the user is connected through a VPN connection, and whether the user is on a wireless connection.

At the end of each call, SIP-compliant endpoints automatically transmit this information to the Front End server that facilitated the call. You don't have to do anything to get endpoints to transmit that information; that behavior is built into the SIP protocol. However, if you want to collect and store that information, then you need to install and enable monitoring. If you do install and enable monitoring, then call information is gathered by agents running on the Front End server and relayed to a pair of SQL Server databases.

Note that the process of installing and configuring monitoring has been simplified in Lync Server 2013. In prior versions of the software, monitoring required a separate Monitoring Server role, which typically meant a separate computer set aside for use as the Monitoring Server. In Lync Server 2013, however, the Monitoring Server role has been eliminated. Instead, the monitoring service (in the form of "unified data collection agents") has been collocated into all Front End servers. This has at least two major benefits. Collocation of the monitoring service:

- Decreases the number of server roles required when implementing Lync Server 2013. Decrementing the Monitoring Server role also helps reduce costs by eliminating the need to maintain dedicated servers for monitoring.
- Reduces the complexity of Lync Server 2013 setup and administration. By collocating the monitoring services on each Front End server you no longer have to install, configure, and manage the Monitoring Server role.

For more information see the topic Deploying Monitoring in the Lync Server 2013 2013 deployment guide.

1.3.11.2 Defining Your Organizations's Requirements for Monitoring

Defining Your Organizations's Requirements for Monitoring

Microsoft Lync Server 2013 > Planning > Planning for Monitoring >

Topic Last Modified: *2012-09-05*

Streamlining the deployment and installation of monitoring in Microsoft Lync Server 2013 has also streamlined the processes involved in defining your organization's requirements for monitoring. Nevertheless, there are still several key issues that should be addressed before you begin to install and configure Lync Server 2013:

What type of data do you want to monitor? Lync Server 2013 enables you to monitor two different types of data: call detailing recording (CDR) data and Quality of Experience (QoE) data. Call detail recording provides a way for you to track the usage of Lync Server features such as Voice over IP (VoIP) phone calls; instant messaging (IM); file transfers; audio/video (A/V) conferencing; and application sharing sessions. This information helps you know which Lync Server features are being used (and which ones are not) and also provides information as to when these features are being used. Quality of Experience data allows you to maintain a record of the quality of audio and video calls made in your organization, including such things as the number of network packets lost, background noise, and the amount of "jitter" (differences in packet delay).

If you choose to enable monitoring in Lync Server 2013 you can enable both CDR monitoring and QoE monitoring, or you can choose to enable one type of monitoring while leaving the other type disabled. For example, suppose your users only use instant messaging and file transfers, and do not make audio or video calls. In that case, there might be little reason to enable QoE monitoring. Likewise, Lync Server makes it easy to enable and disable monitoring after monitoring has been deployed. For example, you might choose to deploy monitoring but initially leave QoE monitoring disabled. If your users begin to experience problems with audio or video calls you could then enable QoE monitoring and use that data to help you troubleshoot and resolve those problems.

There is no particular advantage (or disadvantage) to installing monitoring at the same time you install Lync Server vs. installing monitoring after Lync Server has been installed. The one point to keep in mind is that, before you install monitoring, you must select a computer to host the backend monitoring store, and a supported version of SQL Server must be installing and configured on that computer before that computer can be used for monitoring. If you have already installed SQL Server on a computer and that computer is ready for use then you can install monitoring at the same time you install Lync Server. If you do not have a backend computer ready then you can proceed to install Lync Server by itself, then install monitoring whenever the backend computer is ready for use.

When do you want to install monitoring? Monitoring can be installed and configured at the same time you install and configured Lync Server 2013; the Lync Server Deployment Wizard will provide you with the opportunity to associate your Front End pools with a monitoring database during setup. Alternatively, you can install monitoring after Lync Server itself has been installed; this can be done by using Topology Builder to associate your Front End pools and servers with a monitoring database, and then publishing the revised topology.

How many backend monitoring databases do you need? A single monitoring database can support tens of thousands of users (for Microsoft Lync Server 2010, it was estimated that a collocated database for both monitoring and archiving could support 240,000 users). In addition, a single monitoring database can be used by multiple Front End pools; if you have three Front End pools in your organization then you could associate all three of those pools with the same backend store.

This simply means that, for many organizations, database capacity will not be the deciding factor when determining the number of backend monitoring databases that will be required. Instead, a more important consideration could be network speed. Suppose you have three Front End pools, but one of those pools is located across a slow network connection. In that case, you might want to use two monitoring databases: one database to service the two pools with the good network connection, and a separate database to service the pool with the slower network connection.

When planning your monitoring infrastructure you should also take into account that Lync Server 2013 supports the use of mirror databases. "Database mirroring" provides a way for you to simultaneously maintain two copies of a database, with each database residing on a different server. Any time data is written to a primary database that same data is also written to the mirror database. If the primary database should fail or otherwise become unavailable, you can "fail over" to the mirror database by using a simple Lync Server PowerShell command. For example:

```
Invoke-CsDatabaseFailover -PoolFqdn atl-cs-001.litwareinc.com -DatabaseType "Moni
```

This is important for planning purposes simply because mirroring will require you to double your required number of databases: in addition to each primary database you will need a second database to act as the mirror.

Do your Lync Server sites need their own custom monitoring configurations? When you install Lync Server 2013 you also install global collections of CDR and QoE configuration settings; these global collections give you the ability to apply the same CDR and QoE settings to your entire organization. In many cases, this will be sufficient: often-times you will want, say, to have CDR monitoring enabled for all of your users.

However, there might also be times when you want to apply different settings to different sites. For example, perhaps you want to use both CDR and QoE monitoring in your Redmond site, but only use CDR monitoring in your Dublin site. Likewise, you might want to retain monitoring data for 60 days in the Redmond site but only need to maintain this type of data for 30 days in the Dublin site. Lync Server 2013 allows you to create separate collections of CDR and QoE configuration settings at the site scope; that enables you to manage each site differently. (This includes both enabling and disabling monitoring as well as configuring management settings such as how long data is to be retained.)

Note that you can make this decision before you deploy monitoring or after you deploy monitoring. For example, you can deploy monitoring and then manage the entire organization by using the global settings. If you later change your mind, you can create a separate collection of settings for, say, the Redmond site, and then use those settings to manage monitoring for Redmond. (Settings applied at the site scope always take precedence over settings applied at the global scope.) If you change your mind again, you can simply delete the configuration settings applied to the Redmond site. When a collection of site settings is removed then the global collection of settings will automatically be applied to that site.

1.3.11.3 Enabling Monitoring

Enabling Monitoring

Microsoft Lync Server 2013 > Planning > Planning for Monitoring >

Topic Last Modified: *2012-10-17*

Although the unified data collection agents are automatically installed and activated on each Front End server, that does not mean that you will automatically begin to collect monitoring data the moment you finish installing Microsoft Lync Server 2013. Instead, you must do two things: you must associate your Front End servers/Front End pools with a monitoring database, and you must enable call detail recording (CDR) and/or Quality of Experience (QoE) monitoring at the global scope and/or the site scope.

For step-by-step instructions on associating Front End servers or Front End pools with a monitoring database, see the topic Associating a Monitoring Store with a Front End Pool in the Deployment guide. After these associations have been made, and after your new Lync Server topology has been published, you will still not be able to collect monitoring data. That's because, by default, both CDR and QoE data collection is disabled when you install Lync Server 2013.

In order to begin data collection you will need to enable CDR and/or QoE monitoring. (Note that you do not have to enable both CDR and QoE monitoring; if you prefer, you can enable one type of monitoring while leaving the other type disabled.) To enable CDR monitoring at the global scope run the following command from within the Lync Server Management Shell:

```
Set-CsCdrConfiguration -Identity "global" -EnableCDR $True
```

Alternatively, you can enable CDR monitoring from within the Lync Server 2013 Control Panel. From within the Lync Server Control Panel, complete the following procedure:

1. Click **Monitoring**.
2. On the **Call Detail Recording** tab, double-click the **Global** setting.
3. In the **Edit Call Detail Recording (CDR) Setting** pane, select **Enable monitoring of CDRs** and then click **Commit**.

To enable QoE monitoring at the global scope, run this command from within the Lync Server Management Shell:

```
Set-CsQoEConfiguration -Identity "global" -EnableQoE $True
```

If you prefer, you can also enable QoE monitoring from within the Lync Server Control Panel. From within the Control Panel, complete the following procedure:

1. Click **Monitoring**.
2. On the **Quality of Experience Data** tab, double-click the **Global** setting.
3. In the **Edit Quality of Experience (QoE) Setting** pane, select **Enable monitoring of QoE data** and then click **Commit**.

As noted, the preceding examples enable monitoring at the global scope; that is, they enable CDR and QoE monitoring throughout your organization. Alternatively, you can create separate CDR and QoE configuration settings at the site scope, and then selectively enable or disable monitoring for each site. For example, you could enable CDR monitoring for your Redmond site, yet disable CDR monitoring for your Dublin site. For more information on managing your monitoring configuration settings, see the Deployment guide topic Configuring Call Detail Recording and Quality of Experience Settings.

1.3.11.4 Accessing Monitoring Data

Accessing Monitoring Data

Microsoft Lync Server 2013 > Planning > Planning for Monitoring >

Topic Last Modified: *2012-09-05*

Monitoring data is stored in a pair of SQL Server databases: LcsCdr for call detail recording data, and QoEMetrics for Quality of Experience data. There is nothing special about these two databases; that means that the data stored in those databases can be accessed using any of the tools you typically use for accessing and analyzing SQL Server data.

One tool you should consider for accessing and analyzing monitoring data is the Lync Server Monitoring Reports. Monitoring Reports are a set of standard reports that are published by Microsoft SQL Server Reporting Service. These reports, which are accessible by using a web browser, provide usage, call diagnostic information, and media quality information, all based on call detail recording (CDR) and Quality of Experience (QoE) records stored in the CDR and QoE databases. Monitoring Reports ship with Lync Server 2013 and can be installed from the Lync Server Deployment Wizard after Lync Server has been installed and monitoring has been configured.

As noted, Monitoring Reports requires the use of SQL Server Reporting Service. SQL Server Reporting Service can be installed at the same time you install SQL Server or can be installed any time after SQL Server itself has been installed.

For more information, see the topic Installing Lync Server 2013 Monitoring Reports in the Lync Server 2013 deployment guide.

1.3.11.5 Components and Topologies for Monitoring

Components and Topologies for Monitoring

See Also

Microsoft Lync Server 2013 > Planning > Planning for Monitoring >

Topic Last Modified: *2012-09-05*

Because the unified data collection agents are automatically installed and activated on each Front End server you do not need to configure a server to act as the Monitoring server; each Front End server already functions as a Monitoring server. However, you will need to install and configure a database to act as the backend data store for your monitoring data. Microsoft Lync Server 2013 can use any of the following databases as the backend store for monitoring:

- Microsoft SQL Server 2008 R2 Enterprise Edition
- Microsoft SQL Server 2008 R2 Standard Edition
- Microsoft SQL Server 2012 Enterprise Edition
- Microsoft SQL Server 2012 Standard Edition

Note that you must use the 64-bit editions of these databases; 32-bit versions of SQL Server cannot be used as the backend store for monitoring. Likewise, Lync Server 2013 does not support the Express Editions of SQL Server 2008 or SQL Server 2012. For more information on database requirements for Lync Server 2013 see the topic Database Software Support in the Lync Server 2013 Supportability guide.

Keep in mind that SQL Server must be installed and configured before you deploy and configure monitoring. However, you only need to deploy SQL Server itself; you do not have to setup the monitoring databases in advance. Instead, those databases will automatically be created for you when you publish your Lync Server topology.

Monitoring data can share a SQL Server instance with other types of data. Typically, the call detail recording database (LcsCdr) and the Quality of Experience database (QoEMetrics) share the same SQL instance; it is also common for the two monitoring databases to be in the same SQL instance as the archiving database (LcsLog). About the only real requirement with SQL Server instances is that any one instance of SQL Server is limited to the following:

- One instance of the Lync Server 2013 backend database. (As a general rule, it is not recommended that your monitoring database be collocated in the same SQL instance, or even on the same computer, as the backend database. Although technically possible, you run the risk of the monitoring database using up disk space needed by the backend database.)
- One instance of the call detail recording database.
- One instance of the Quality of Experience database.
- One instance of the archiving database.

In other words, you cannot have two instances of the LcsCdr database in the same instance of SQL Server. If you need multiple instances of the LcsCdr database then you will need to configure multiple instances of SQL Server.

Other Resources

Deploying Monitoring

1.3.11.6 Deployment Checklist for Monitoring

Deployment Checklist for Monitoring

Microsoft Lync Server 2013 > Planning > Planning for Monitoring >

Topic Last Modified: *2012-09-05*

Although monitoring is already installed and activated on each Front End server, there are still several steps that you must undertake before you can actually being to collect monitoring data for Microsoft Lync Server 2013. These steps are outlined in the following checklist:

Phase	Steps	Role and group	Documentation

		membership	
Install prerequisite hardware and software	Install a supported version of Microsoft SQL Server on the computer that will act as the backend data store for monitoring.	Domain user who is also a member of the local administrators group.	Supported Hardware in the Supportability guide Server Software and Infrastructure Support in the Supportability Guide
Create the appropriate internal topology to support monitoring	Use Lync Server 2013 Topology Builder to add monitoring databases to the topology, then published the updated topology.	To define a topology, a user who is a member of the local users group. To publish the topology, a user who is a member if the domain administrators group and the RTCUniversalServerAdmins group.	Associating a Monitoring Store with a Front End Pool in the Deployment guide
Enable the appropriate monitoring settings	Enable call detail recording (CDR) and/or Quality of Experience (QoE) monitoring at the global and/or the site scopes.	A user who is a member of the RTCUniversalServerAdmins group or who has been assigned an RBAC role that provides access to the CsCdrConfiguration and CsQoEConfiguration cmdlets.	Configuring Call Detail Recording and Quality of Experience Settings in the Operations guide

1.3.12 Planning for Archiving

Planning for Archiving

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-28*

Corporations and other organizations are subject to an increasing number of industry and government regulations that require the retention of specific types of communications. If your organization has such requirements, you can use Archiving in Lync Server 2013 to archive instant messaging (IM) and conferencing (meeting) communications sent through Lync Server to help support some of your compliance requirements.

- Overview of Archiving
- How Archiving Works
- Defining Your Organization's Requirements for Archiving
- Components and Topologies for Archiving
- Technical Requirements for Archiving
- Deployment Checklist for Archiving

1.3.12.1 Overview of Archiving

Overview of Archiving

Microsoft Lync Server 2013 > Planning > Planning for Archiving >

Topic Last Modified: *2012-10-10*

Archiving in Lync Server 2013 provides a way for you to archive communications that are sent through Lync Server 2013.

You can implement Archiving as part of your initial Lync Server 2013 deployment, or you can add it to an existing deployment. To use Lync Server 2013 Archiving databases (SQL Server databases) for storage of archiving data, you use Topology Builder to add the databases to your topology, and then publish the topology again. If all your users are homed on Exchange 2013 and have their mailboxes put on In-Place Hold, you do not have to update your topology, but only need to enable Microsoft Exchange integration to store archived data in Exchange 2013.

When you implement Archiving, you configure it to specify what is archived. By default, nothing is archived. You configure and manage Archiving by using Lync Server 2013 Control Panel. You can implement Archiving for internal communications, external communications, or both. You can configure archiving settings your entire organization and, optionally, for specific sites, specific pools, and specific users and user groups. For details about determining the appropriate options for your organization, see Defining Your Organization's Requirements for Archiving in the Planning documentation. For details about how Archiving policies and configurations are implemented, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

1.3.12.2 How Archiving Works

How Archiving Works

Microsoft Lync Server 2013 > Planning > Planning for Archiving >

Topic Last Modified: *2013-01-22*

Lync Server 2013 Archiving provides options to help you meet your compliance needs. To implement and maintain it in a way that most effectively meets your organization’s requirements, you should understand:

- What information can be archived.
- How to enable and disable Archiving in your deployment.
- The archiving options that you can configure to control how Archiving is implemented.

What Information Can Be Archived?

The following types of content can be archived:

- Peer-to-peer instant messages
- Conferences (meetings), which are multiparty instant messages
- Conference content, including uploaded content (for example, handouts) and event-related content (for example, joining, leaving, uploading sharing, and changes in visibility)
- Whiteboards and polls shared during a conference

The following types of content are not archived:

- Peer-to-peer file transfers
- Audio/video for peer-to-peer instant messages and conferences

- Desktop and application sharing for peer-to-peer instant messages and conferences

Lync Server also does not archive Persistent Chat conversations. To archive Persistent Chat conversations, you must enable and configure the compliance service, which is a component that can be deployed with Microsoft Lync Server 2013, Persistent Chat Server. For details, see Planning for Persistent Chat Server in the Planning documentation.

How Do I Start Using Archiving?

Archiving is automatically installed on each Front End Server when you deploy the server, but Archiving is not enabled until you configure it. How you configure it is determined by how you deploy Archiving:

- **Archiving using Microsoft Exchange integration.** If you have users who are homed on Exchange 2013 and their mailboxes have been put on In-Place Hold, you can select the option to integrate Lync Server 2013 storage with Exchange storage. If you choose the Microsoft Exchange integration option, you use Exchange 2013 policies and configurations to control the archiving of Lync Server 2013 data for those users.
- **Archiving using Lync Server Archiving databases.** If you have users who are not homed on Exchange 2013 or who have not had their mailboxes put on In-Place Hold, or if you don’t want to use Microsoft Exchange integration for any or all users in your deployment, you can deploy Lync Server Archiving databases using SQL Server to store Archiving data for those users. In this case, Lync Server 2013 Archiving policies and configurations determine whether Archiving is enabled and how it is implemented. To use Lync Server 2013, you must add the appropriate SQL Server databases to your topology and publish the topology.

Archiving Setup When Using Microsoft Exchange Integration

If your users are homed on Exchange 2013 and their mailboxes have been put on In-Place Hold, you can choose the **Microsoft Exchange integration** option (as described later in this section) to archive Lync Server 2013 for those users, and then you control archiving for those users by specifying Exchange In-Place Hold policies and settings, as well as Lync Server configurations to control the following:

- Whether to archive IM, conferencing, or both.
- Whether to implement critical mode for your Lync Server deployment.
- Selection of the Microsoft Exchange integration option to use Exchange 2013 for storage of archived data.

These Lync Server 2013 Archiving configuration options are described later in this section. For information about how to configure Exchange In-Place Hold policies and settings to support archiving, see the Exchange 2013 product documentation.

Archiving Setup When Using Lync Server Archiving Database Storage

If you want to use Lync Server Archiving databases (using SQL Server databases) to archive data for any users in your deployment, you can configure Lync Server Archiving policies to control whether Archiving is enabled for those users. In each Archiving policy, you can enable or disable Archiving for either or both of the following:

- Internal communications
- External communications

By default, archiving is not enabled for internal communications or external communications in any Lync Server Archiving policy. You enable and disable communications using Lync Server 2013 Control Panel or using cmdlets in the Lync Server 2013 Management Shell.

Lync Server 2013 Archiving policies include the following:

- **Global Archiving policy**. This is the default Archiving policy and applies to your entire deployment. It is created when you deploy Lync Server 2013 and, by default, disables Archiving for both internal and external communications. You cannot delete this policy. If you choose the delete option, the global policy is reset to the default settings.
- **Site Archiving policy**. Optionally, you can enable or disable Archiving for one or more specific sites by creating and configuring a site-level Archiving policy for the site. When you create a site-level Archiving policy, by default, archiving is not enabled. You can delete any site-level Archiving policy that you create. A site-level Archiving policy overrides the global policy, but only for the site specified in the policy. For example, if you enable Archiving for internal and external communications in your global policy and create a site policy in which you disable Archiving for external communications, only internal communications would be archived for that site.
- **User Archiving policy**. Optionally, you can enable or disable Archiving for one or more specific users and group of users by creating, configuring, and applying a user-level Archiving policy for the specified users and user groups. When you create a user-level Archiving policy, by default, archiving is not enabled. You can delete any user-level Archiving policy that you create, and you can change which users and group of users the Archiving policy applies to. A user-level Archiving policy overrides the global policy and any site policies, but only for the users and user groups to whom the policy is applied. For example, if you disable Archiving for internal and external communications in your global policy, create a site-level policy in which you enable Archiving for internal and external communications, and then create a user-level policy in which you disable Archiving for external communications, the communications would be archived for both external and internal communications for all site users except that, for the users to whom you apply the user-level policy, only internal communications would be archived.

For details about how to set up initial Archiving policies when you deploy Archiving, see Configuring and Assigning Archiving Policies in the Deployment documentation. For details about using Archiving policies to enable and disable communications after deployment, see Managing the Archiving of Internal and External Communications in the Operations documentation.

Note:

If you implement both Lync Server 2013 Archiving databases and enable Microsoft Exchange integration, Exchange 2013 policies override Lync Server Archiving policies, but only for users who are homed on Exchange 2013 and have had had their mailboxes put on In-Place Hold. Lync Archiving depends on Microsoft Exchange In-Place Hold policy only.

What Options Do I Have for Configuring Archiving?

In addition to using policies and to enable and disable Archiving, you have other Archiving options that can be configure for your entire deployment and, optionally, for specific sites and pools. You control most Archiving options by using one or more Archiving configurations, which are available in Lync Server 2013 Control Panel, but also have another option that is only available for configuration using Lync Server 2013 Management Shell.

Archiving Configuration Options Available in Lync Server 2013 Control Panel

Each archiving configuration provides the following options:

The global-level configuration is created automatically when you deploy archiving and can be configured, but not deleted. If you select the option to delete the global configuration, the settings are reset to the default values. You can create multiple site and pool configurations that, together with the global configuration, control archiving settings. For the global configuration and each site and pool configuration, you have the following options:

- Disable archiving, enable archiving only for instant messaging (IM), or enable archiving of both IM and conferencing.
- Configure critical mode to block IM and conferencing sessions in the event of a Lync Server failure. Failures include the following:
  - **IM**. A problem with the Lync Server storage service. In this case, IM is blocked for users who are enabled for Archiving.
  - **Conferencing**. A failure could be an unavailable file share or a problem with the storage service. In this case, all active conferences hosted in the pool at the time of failure are switched to restricted mode and new conferences cannot be activated.

  Both IM and conferencing automatically recover after the failures are corrected.
- Specify the use of Microsoft Exchange Server 2013 integration to use Exchange 2013 for storage of archived data, instead of setting up separate SQL Server databases for storage of Lync Server 2013 archiving data.
- Configure purging options for archived data. This includes specifying when to purge archived data, which can be either of the following:
  - After a specific number of days that you specify
  - After the archiving data has been exported (which includes data that has been uploaded to Exchange, if you enable Microsoft Exchange integration).

  Note:

  If you enable Microsoft Exchange integration, purging for users homed on Exchange 2013 and with their mailboxes put on In-Place Hold is controlled by Exchange. The only qualification is for conferencing files, which are stored on the Lync Server file share. These files are purged from the file share only after the files have been exported (uploaded to Exchange), if you select the option to purge data after the archiving data has been exported, or after the specified maximum number of days, if you specify a maximum number of days for retention.

By default, no archiving options are enabled. You can manage Archiving configurations using Lync Server 2013 Control Panel.

You can specify the following Archiving configurations:

- **Global Archiving configuration**. This is the default Archiving configuration and applies to your entire deployment. It is created when you deploy Lync Server 2013 and, by default, does not enable archiving functionality. You can modify the global configuration, but you cannot delete it. If you choose the delete option for the configuration, the global configuration is reset to the default settings.
- **Site Archiving configuration**. Optionally, you can configure Archiving for one or more specific sites by creating and configuring a site-level Archiving configuration for an individual site. A site-level Archiving configuration exists only if you create it. You can modify or delete any site-level Archiving configuration. A site-level Archiving configuration overrides the global configuration, but only for the site specified in the site-level configuration. For example, if you enable Archiving for only IM in your global configuration and create a site configuration in which you enable Archiving for both IM and conferencing, conferencing would only be archived for the site, not for the remainder of your organization.
- **Pool Archiving configuration**. Optionally, you can specify Archiving settings for one or more specific pools by creating and configuring a pool-level configuration for the individual pool. A pool-level Archiving configuration exists only if you create it. You can modify and delete any pool-level Archiving configuration. A pool-level Archiving configuration overrides the global configuration and any site archiving configuration you may have created. For example, if you enable Archiving for only IM in your global configuration, create a site-level configuration in which you enable Archiving for both IM and conferencing for the site, and then create a pool-level configuration in which

you enable Archiving only for IM, the communications would be archived for both IM and conferencing for all users of the site except the users homed in the pool specified in the pool-level configuration. For all other users in your organization, Archiving would be enabled only for IM.

For details about how to set up initial Archiving configurations when you deploy Archiving, see Configuring Archiving Options in the Deployment documentation. For details about using Archiving policies to enable and disable communications after deployment, see Managing Archiving Configuration Options for Your Organization, Sites, and Pools in the Operations documentation.

Archiving Options Available Only in Windows PowerShell

Using Lync Server 2013 Management Shell, you can use cmdlets to implement options that are not available in Lync Server 2013 Control Panel. These options include the following:

- **Archive duplicate messages**. For details, see New-CsArchivingConfiguration and Set-CsArchivingConfiguration in the Operations documentation.
- **Export archived data**. For details, see Export-CsArchivingData

How Do I Access Archived Data?

Access to archived data is dependent on where the data is stored:

- **Microsoft Exchange storage**. If you choose the SharePoint integration option, Lync Server deposits the archiving content in the Exchange 2013 store for all users who are homed on Exchange 2013, and who have had their mailboxes put on In-Place Hold. Archived data is stored in user mailboxes Recoverable items folder, which is generally invisible to users, and can only be searched by users with an Exchange **Discovery Management** role. Exchange enables federated search and discovery, along with SharePoint, if it is deployed. For more details about storage, retention, and discovery of data stored in Exchange, see the Exchange 2013 and SharePoint documentation.
- **Lync Server storage**. If you set up Lync Server 2013 Archiving databases for storage of Lync Server data, Lync Server deposits archiving content in the Lync Server Archiving databases (SQL Server databases) for any users not homed on Exchange 2013, and who have not had their mailboxes put on In-Place Hold. This data is not searchable, but it can be exported to formats that are searchable using other tools. For details about exporting data stored in Archiving databases, see Exporting Archived Data in the Operations documentation.

For more details about how Lync Server 2013 and Exchange 2013 work together, see Exchange Server and SharePoint Integration Support in the Supportability documentation.

1.3.12.3 Defining Your Organization's Requirements for Archiving

Defining Your Organization's Requirements for Archiving

Microsoft Lync Server 2013 > Planning > Planning for Archiving >

***Topic Last Modified:** 2012-10-09*

If your organization must follow compliance regulations, you can deploy Archiving to enable archiving support for Lync Server 2013 instant messaging (IM) and conferencing (meetings). For details about the type of content that can be archived, see Overview of Archiving in the Planning documentation.

To implement Archiving, you need to first decide how to meet your organization’s requirements for Archiving. This requires determining the following:

- **When to deploy Archiving**. You can deploy Archiving as part of your initial Lync Server 2013 deployment, or you can add it to an existing deployment. You deploy Archiving by using Topology Builder to add it to your topology, and then publishing the topology.
- **Whether to archive internal or external communications**. You can enable archiving for internal communications (communications between internal users), external communications (communications that include at least one user outside your internal network), or both. You can specify these options for your entire organization, or you can specify them for specific sites and pools. By default, neither option is enabled.

  Note:

  If you use Microsoft Exchange integration to store archived data, your Exchange settings control whether Lync communications are archived. If your deployment includes multiple forests, you must synchronize the settings between Lync Server and Exchange. Controlling archiving for internal or external communications is only available for Lync Policy. For Exchange-integrated archiving, both of them will be archived or not archived.
- **Why enable Archiving**. You can enable and disable Archiving for your entire deployment at a global level, and you can enable and disable Archiving for specific sites and users. At each of these levels, you specify whether to enable archiving of IM sessions (peer-to-peer), conferences (meetings, which are multiparty sessions), or both. By default, Archiving is disabled.
- **How critical Archiving is to users in your organization**. If archiving is mission-critical in your organization, you can specify that Lync Server 2013 run in critical mode, which blocks IM and conferencing sessions if archiving fails. For example:
  - If the Archiving service is temporarily unable to send a message to the database queue or insert a message into the database), both IM and conferencing functionality are blocked in the deployment until archiving support is restored.
  - If a conferencing user uploads a file, but the file cannot be copied to the archiving file store, conferencing functionality is blocked in the deployment until the problem is resolved, but IM functionality is not blocked.

  You can configure this option at the global level, site level, and pool level. By default, critical mode is not enabled.
- **Whether to use Microsoft Exchange integration**. This option integrates Archiving storage with your Exchange 2013 storage, so that your Lync Server archived data and Exchange 2013 archived data are stored together in Exchange. You can use Microsoft Exchange integration for storage of archiving data for users who are homed on Exchange 2013, if their mailboxes have been put on In-Place Hold. If you do not have an Exchange 2013 deployment, or if you prefer not to integrate with it, or if you have any Lync users who are not homed on Exchange 2013, you can deploy separate Archiving databases by using SQL Server to store archived data from Lync communications. You can configure the Microsoft Exchange integration option at the global level, site level, and pool level. By default, Microsoft Exchange integration is not enabled.
- **How archived data is to be managed**. The archiving database is not intended for long-term retention and Lync Server 2013 does not provide an e-discovery (search) solution for archived data, so data needs to be moved to other storage. Lync Server does provide a session export tool that you can use to export archived data, and which creates searchable transcripts of the archived data. For the global policy, and for each site and user policy that you create, you can enable data purging and specify one of the following options:
  - Purge both exported archiving data and stored archiving data after a specific number of days. The minimum number of days that you can specify is one day. The maximum number of days that you can specify is 2562 days.
  - Purge exported archiving data only. This option purges all records that have been exported and marked as safe to delete by the session export tool.

  You can configure this option at the global level, site level, and pool level. By default, purging is not enabled.

You control Archiving by using the following methods:

- **Archiving policies**. You use one or more Archiving policies to enable and disable archiving of internal and external communications. By default, no archiving is enabled. You enable or disable Archiving for internal communications, external communications, or both in your deployment by using the default global policy. You cannot delete the global policy. You can specify one or more optional site policies to enable or disable Archiving for internal and external communications for specific sites. You can also specify one or more user policies to enable or disable Archiving for specific users and user groups. User-level policies override site policies. Site-level policies override the global-level policies. User-level policies are implemented only for the specific users who are configured to use the policy. Group instant messages and conferences are archived only if a policy for at least one of the participants is configured to enable archiving.

  Note:
  If you use Microsoft Exchange integration, Exchange 2013 policies override Lync Server Archiving policies for all users homed on the Exchange 2013 servers.

- **Archiving configurations**. You use one or more Archiving configurations to specify most of the Archiving options that are described previously in this topic, except for enabling archiving of internal and external communications (configured using Archiving policies, as described in the previous bullet). Archiving configurations include the default global configuration and optional site and pool configurations. You cannot delete the global configuration. Pool-level configurations override site-level configurations. Site-level configurations override the global-level configuration.

As part of your requirements analysis, you need to determine how to configure the global Archiving configuration and global Archiving policy. You also need to determine your requirements for any site-level Archiving configurations, pool-level Archiving configurations, site-level Archiving policies, and user-level Archiving policies.

If you deploy Archiving for one Front End pool or Standard Edition server, you should then enable it for all other Front End pools and Standard Edition servers in your deployment. You need to do this because users whose communications are required to be archived can be invited to a group IM conversation or meetings hosted on a different pool. If archiving is not enabled on the pool where the conversation or meeting is hosted, all conference data may not be archived. Archiving will still work for archiving enabled users and all IM messages, but conferencing content and events may not be archived.

Note:
To enable delegation of administrative tasks while maintaining your organization's security standards, Lync Server 2013 uses role-based access control (RBAC). With RBAC, administrative privilege is granted by assigning users to predefined administrative roles. To configure Lync Archiving policies and Archiving configurations, the user must be assigned to the CsArchivingAdministrator role (unless the configuration is done directly on the server where Archiving is deployed, instead of remotely from another computer). For details about RBAC, see Planning for Role-Based Access Control in the Planning documentation. For a list of the user rights, permissions, and roles required for archiving deployment, see Deployment Checklist for Archiving, which is available in both the Planning documentation and the Deployment documentation.
If you use Microsoft Exchange integration, configuration of Exchange policies requires appropriate administrator rights and permissions. For details, see the Exchange 2013 documentation.

1.3.12.4 Components and Topologies for Archiving

Components and Topologies for Archiving

Microsoft Lync Server 2013 > Planning > Planning for Archiving >

Topic Last Modified: *2012-10-09*

If you want to archive Lync Server 2013 IM and conferencing content, you can implement Archiving in Lync Server.

Archiving Components

The Archiving feature includes the following components:

- **Archiving agents**. Archiving agents (also known as unified data collection agents) are installed and activated automatically on every Front End pool and Standard Edition server. Although archiving agents are activated automatically, no messages are actually captured until Archiving is enabled and appropriately configured.
- **Archiving data storage**. Data storage for Lync Server 2013 can be either of the following:
  - Exchange 2013 storage. If you enable the Microsoft Exchange integration option, user mailboxes homed on the Exchange 2013 server use Exchange 2013 storage for archived data, but only if the mailboxes have been put on In-Place Hold.
  - SQL Server storage. If you have users in your deployment who are homed on Lync Server 2013, you can set up Archiving databases that run a supported version of SQL Server to enable archiving for those users.

Archiving also requires file storage, but Archiving uses the same file storage as the Front End Servers or Standard Edition server.

For a list of hardware and software requirements for Archiving, see Supported Hardware and Server Software and Infrastructure Support in the Supportability documentation.

Supported Topologies

You deploy Archiving in each pool that has users that require archiving support. Archiving runs on Front End Servers in Enterprise Edition pools and on Standard Edition servers. Archiving data storage can be the following:

- Integrated with Exchange 2013 storage
- Deployed using separate SQL Server databases

If your Exchange 2013 deployment does not include all users in your Lync Server deployment, you must use Microsoft Exchange integration for the users whose mailboxes are home on Exchange 2013 servers, and you must deploy separate SQL Server databases for all other Lync users to use for archiving.

Supported Collocation

Lync Server 2013 supports a variety of collocation scenarios, allowing you flexibility to save hardware costs by running multiple components on one server (if you have a small organization), or to run individual components on different servers (if you have a larger organization that needs scalability and performance). Scalability factors should certainly be considered before you decide whether to collocate components.

Archiving is deployed on the Front End Servers of a pool or Standard Edition servers. For details about components that can be collocated there, see Supported Server Collocation in the Supportability documentation.

If you use separate SQL Server databases for Archiving, instead of or in addition to integrating storage with Exchange 2013 storage, you can collocate the Archiving database with any of the following:

- Monitoring database
- Back-end database of an Enterprise Edition Front End pool

Note:

The server hosting the Archiving database can host other databases. However, when you consider collocating the Archiving database with other databases, be aware that if you are archiving the messages of more than a few users, the disk space needed by the Archiving database can grow very large. For this reason, we do not recommend collocating the Archiving database with the back-end database.

If you collocate the Archiving database with the Monitoring database, back-end database, or both of these databases, you can either use a single SQL instance for any or all of the databases, or you can use a separate SQL instance for each database, with the following limitation:

- Each SQL instance can contain only a single back-end database, single Monitoring database, and single Archiving database.

For details about collocation of all server roles and databases, see Supported Server Collocation in the Supportability documentation.

1.3.12.5 Technical Requirements for Archiving

Technical Requirements for Archiving

Microsoft Lync Server 2013 > Planning > Planning for Archiving >

Topic Last Modified: *2012-10-09*

Lync Server 2013 technical requirements include the following:

- Infrastructure requirements.
- Prerequisite software that must be installed for Archiving.
- Data storage requirements for Archiving.
- Scaling requirements and considerations for your Archiving deployment.
- Performance requirements and considerations for your Archiving databases.

Note:

Scaling and performance information is not available in this Lync Server 2013 release.

Infrastructure Requirements

Lync Server 2013 Archiving infrastructure requirements are the same as for deployment of Lync Server 2013. For details, see Determining Your Infrastructure Requirements in the Planning documentation.

Archiving Prerequisites

Lync Server 2013 streamlines prerequisites for Archiving because of the following:

- Archiving Server is no longer a server role. Instead, Unified Data Collection

Agents run on the Front End Servers in a pool and Standard Edition servers to capture data for Archiving, so you do not set up separate system platforms for Archiving.

- Archiving uses the Lync Server 2013 file storage for temporary storage of meeting content files, so you do not set up a separate file store for archiving.
- In Lync Server 2013, Message Queuing is not required.

Data Storage Requirements for Archiving

Additionally, you need to set up the infrastructure for Archiving storage. This includes one or both of the following:

- **Microsoft Exchange storage**. Meeting content files, such as PowerPoint presentations, are archived as attachments. If you want to use Microsoft Exchange integration so that Lync archive data is stored with Exchange compliance data, you must use Exchange 2013 for your Exchange deployment and ensure that the maximum storage size supports storage of the meeting content files. If you deploy Archiving using the Microsoft Exchange integration option, Lync archive data is stored with Exchange 2013 compliance data only for the users who are homed on your Exchange 2013 servers. You must deploy Exchange 2013 prior to deploying and enabling Archiving using the Microsoft Exchange integration option. If you choose to use Exchange 2013 storage, you do not need to deploy separate SQL Server databases for Archiving, unless you have Lync users who are not homed on your Exchange 2013 servers.
- **SQL Server database storage for Archiving**. To support users who are not homed on Exchange 2013 servers, or if you do not want to use the Microsoft Exchange integration option, you must deploy Archiving storage using a SQL Server database. Lync Server 2013 supports the following 64-bit versions of SQL Server:
  - Microsoft SQL Server 2008 R2 Enterprise
  - Microsoft SQL Server 2008 R2 Standard
  - Microsoft SQL Server 2012 Enterprise
  - Microsoft SQL Server 2012 Standard

  Note:

  Microsoft SQL Server 2008 R2 Express and Microsoft SQL Server 2012 Express are not supported for Archiving. 32-bit versions of SQL Server are not supported. For additional SQL Server requirements and restrictions, see Database Software Support in the Planning documentation or in the Supportability documentation.

  You must set up the SQL Server platforms prior to deploying and enabling Archiving. If the account to be used to publish the topology has the appropriate administrator rights and permissions, you can create the Archiving database (LcsLog) when you publish your topology. You can also create the database later, including as part of the installation procedure. For details about SQL Server, see the SQL Server TechCenter at http://go.microsoft.com/fwlink/p/?linkID=129045.

1.3.12.6 Deployment Checklist for Archiving

Deployment Checklist for Archiving

Microsoft Lync Server 2013 > Planning > Planning for Archiving >

Topic Last Modified: *2012-10-18*

Archiving is automatically installed on each Front End Server in your Lync Server 2013 deployment, but you still need to set it up before you can use it. The steps required to set it up, as summarized in this section, constitute the deployment of Archiving.

Deployment Sequence

How you set up Archiving depends on which storage option you choose:

- If you use Microsoft Exchange integration for all users in your deployment, you don’t need to configure Lync Server 2013 Archiving policies for your users. Instead, configure your Exchange In-Place Hold policies to support archiving for users homed on Exchange 2013, with their mailboxes put on In-Place Hold. For details about configuring these policies, see the Exchange 2013 product documentation.
- If you do not use Microsoft Exchange integration for all users in your deployment, you need to add Lync Server Archiving databases (SQL Server databases) to your topology and then publish it, as well as configure policies and settings for your users, before you can archive data for those users. You can deploy Archiving databases at the same time that you deploy your initial topology or after you have deployed at least one Front End pool or Standard Edition server. This document describes how to deploy Archiving databases by adding them to an existing deployment.

If you enable archiving in one Front End pool or Standard Edition server, you should enable it for all other Front End pools and Standard Edition servers in your deployment. This is because users whose communications are required to be archived can be invited to a group IM conversation or meetings hosted on a different pool. If archiving is not enabled on the pool where the conversation or meeting is hosted, the complete session may not be archived. In these cases, IMs with archiving-enabled users still can be archived, but not for conferencing content files, and conference join or leave events.

Important:

If archiving is critical in your organization for compliance reasons, be sure to deploy Archiving, configure policies and other options at the appropriate level, and enable it for all appropriate users, before you enable those users for Lync Server 2013.

Archiving Deployment Process

The following table provides an overview of the steps required to deploy archiving in an existing topology.

Phase	Steps	Roles and group memberships	Documentation
Install prerequisite hardware and software	• To use Microsoft Exchange integration (using Exchange 2013 for archiving storage for some or all users), you need an existing Exchange 2013 deployment. • To use separate Archiving databases (using SQL Server databases) for archiving storage for some or all users, SQL Server on the server that will store archiving data.	Domain user who is a member of the local administrators group.	Supported Hardware in the Supportability documentation. Server Software and Infrastructure Support in the Supportability documentation. Technical Requirements for Archiving in the Planning documentation. Setting Up

	Note: Archiving runs on Front End Servers of an Enterprise pool and Standard Edition servers. It has no additional hardware or software requirements beyond what is required to install those servers.		Systems and the Infrastructure for Archiving in the Deployment documentation. Exchange Server and SharePoint Integration Support in the Supportability documentation.
Create the appropriate internal topology to support archiving (only if not using Microsoft Exchange integration for all users in your deployment)	Run Topology Builder to add Lync Server 2013 Archiving databases (SQL Server databases) to the topology, and then publish the topology.	To define a topology to incorporate Archiving databases, an account that is a member of the local users group. To publish the topology, an account that is a member of the domain admins group and RTCUniversalServerAdmins group, and that has full control permissions (read/write/modify) on the file share to be used for the Lync Server 2013 file store (so that Topology Builder can configure the required DACLs).	Adding Archiving Databases to an Existing Lync Server 2013 Deployment in the Deployment documentation.
Configure server-to-server authentication (only if using Microsoft Exchange integration)	Configure servers to enable authentication between Lync Server 2013 and Exchange 2013. We recommend running **Test-CsExchangeStorageConnectivity testuser_sipUri –Folder Dumpster** to validate Exchange Archiving storage connectivity before enabling archiving.	An account with the appropriate permissions for managing certificates on the servers.	Managing Server-to-Server Authentication (Oauth) and Partner Applications in the Deployment documentation or the Operations documentation.
Configure archiving policies and configurations	Configure archiving, including whether to use Microsoft Exchange integration, the global policy and any site and user policies (when not using Microsoft Exchange integration	RTCUniversalServerAdmins group (Windows PowerShell only) or assign users to	Configuring Support for Archiving in the Deployment documentation.

	for all data storage), and specific archiving options, such as critical mode and data export and purging. If using Microsoft Exchange integration, configure Exchange In-Place Hold policies as appropriate.	the CSArchivingAdministrator or CSAdministrator role.	Exchange product documentation (if using Microsoft Exchange integration).

Deploying Lync Server and Microsoft Exchange in Different Forests

If Microsoft Exchange Server is not deployed in the same forest as Lync Server, you must make sure that the following Exchange Active Directory attributes are synchronized to the forest where Lync Server is deployed:

1. msExchUserHoldPolicies
2. proxyAddresses

This is a multi-value attribute. When synchronizing this attribute, you need to merge the values, not replace them to ensure the existing values are not lost.

1.3.13 Planning for Persistent Chat Server

Planning for Persistent Chat Server

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-10-11*

You can use Lync Server 2013, Persistent Chat Server to enable multiple users to participate in conversations in which they post and access content about specific topics, including text, links, and files. Although users can communicate in real time during a session, the content of each session is persistent, which means it continues to be available after a session ends.

This section describes planning considerations in a Lync Server 2013, Persistent Chat Server deployment, including defining requirements, identifying components and supported topologies, and deployment recommendations.

- Overview of Persistent Chat Server
- How Persistent Chat Server Works
- Defining Your Organization's Requirements for Persistent Chat Server
- Components and Topologies for Persistent Chat Server
- Technical Requirements for Persistent Chat Server
- Setting Up Systems and the Infrastructure for Persistent Chat Server
- Deployment Checklist for Persistent Chat Server

1.3.13.1 Overview of Persistent Chat Server

Overview of Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-10-29*

Lync Server 2013, Persistent Chat Server enables users to participate in multiparty, topic-based conversations that persist over time. Persistent Chat Server can help your organization do the following:

- Improve communication between geographically dispersed and cross-functional teams. By using Persistent Chat, teams can efficiently share information, ideas, and decisions with one another. The messages posted to chat rooms (discussion forums) can persist (that is, can be available over time), so that people from different locations and departments can participate, even when they are not simultaneously online. When a user connects to a chat room, backchat (a configurable number of chat-history messages) is automatically loaded in the chat room to give the user a context for the conversation.
- Improve information awareness. By using client-side filters, users can define conditions—such as keywords in message content, or the value of the "from" field in a message—to receive notification when those conditions are met in Persistent Chat instant messages or chat room messages. This way, users can stay up-to-date with the content that interests them most.
- Improve communication with their extended organization. By making it easy to collaborate over long-running topics with others in the organization, and by providing a persistent place to share information, Persistent Chat helps improve communication.
- Reduce information overload. Users can follow chat rooms and messages of most interest by using client-side filters, and can add chat rooms they want to follow to their contact list.
- Increase dispersion of important knowledge and information. Documents and links can be included within conversations for access by all the team. By posting questions to a broader team, users can benefit from responses by subject matter experts. Integration with other information systems enables important organizational data to be easily communicated to large groups.

To enable chat rooms in Lync Server 2013, deploy Lync Server 2013 Persistent Chat. For information about enabling chat rooms, see the Persistent Chat Help at http://go.microsoft.com/fwlink/p/?linkid=270945. If users are enabled for Lync Server, and Lync Server support is deployed, users can install and use Lync 2013 Persistent Chat to provide chat room support.

If your organization is required to follow compliance regulations, you can optionally deploy Persistent Chat Compliance service.

1.3.13.2 How Persistent Chat Server Works

How Persistent Chat Server Works

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-11-21*

Lync Server 2013, Persistent Chat Server enables you to participate in multiparty, topic-based conversations that persist over time. Persistent Chat Server can help your organization do the following:

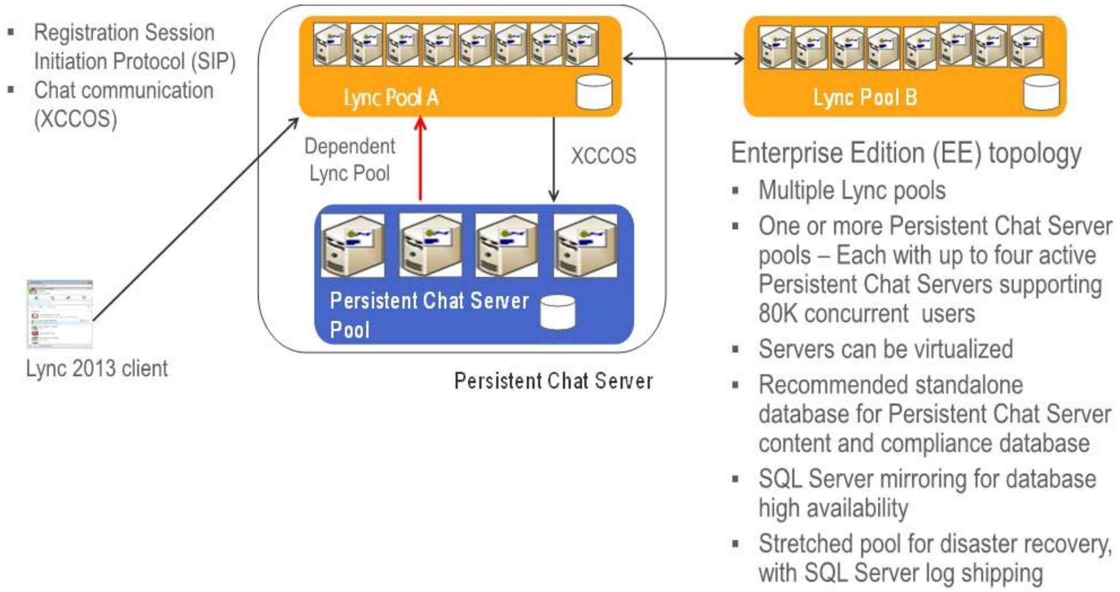
- Improve communication between geographically dispersed and cross-functional teams
- Broaden information awareness and participation
- Improve communication with your extended organization

- Reduce information overload
- Improve information awareness
- Increase dispersion of important knowledge and information

You can deploy Persistent Chat Server as an optional role with Lync Server 2013. Persistent Chat services run on a dedicated pool, and a Persistent Chat Server pool depends on a Lync Server pool to route messages to it. Clients use eXtensible Chat Communication Over SIP (XCCOS). The Lync Server Front End Servers are configured to route the traffic to a Persistent Chat Server pool.

High-Level Architecture

The following diagrams provide high-level perspectives of the Persistent Chat Server architecture and services.

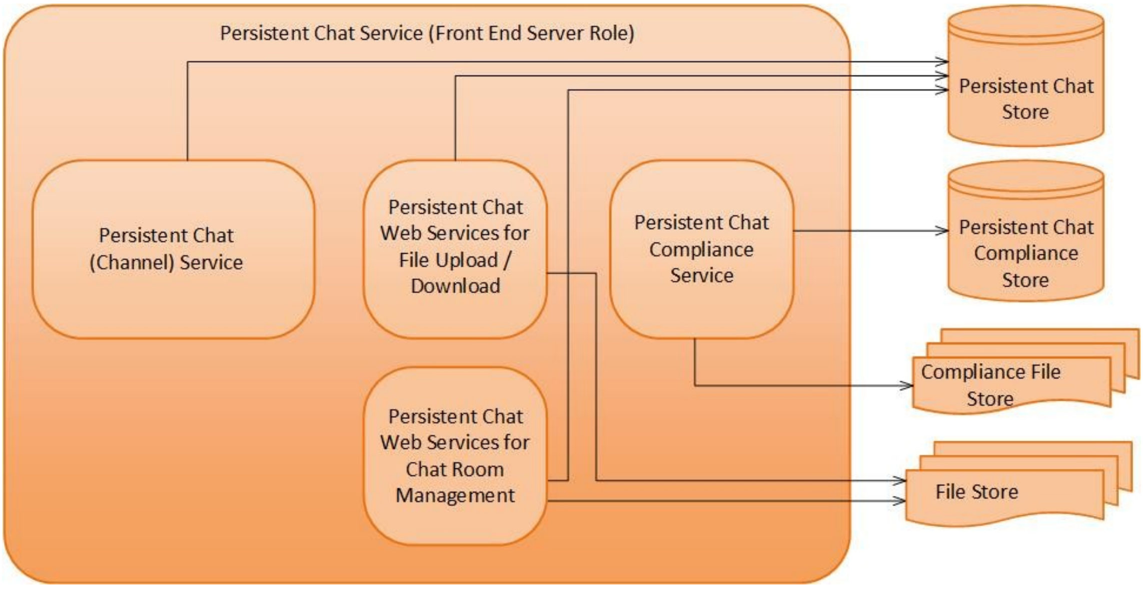


- Registration Session Initiation Protocol (SIP)
- Chat communication (XCCOS)

Enterprise Edition (EE) topology

- Multiple Lync pools
- One or more Persistent Chat Server pools – Each with up to four active Persistent Chat Servers supporting 80K concurrent users
- Servers can be virtualized
- Recommended standalone database for Persistent Chat Server content and compliance database
- SQL Server mirroring for database high availability
- Stretched pool for disaster recovery, with SQL Server log shipping

Lync Pool A
Lync Pool B
Dependent Lync Pool
XCCOS
Persistent Chat Server Pool
Persistent Chat Server
Lync 2013 client



Persistent Chat Service (Front End Server Role)
Persistent Chat (Channel) Service
Persistent Chat Web Services for File Upload / Download
Persistent Chat Compliance Service
Persistent Chat Web Services for Chat Room Management
Persistent Chat Store
Persistent Chat Compliance Store
Compliance File Store
File Store

Two services run on the Persistent Chat Server Front End Servers:

- Persistent Chat (Channel)
- Compliance

Persistent Chat (Channel) Service

The Persistent Chat (Channel) service is the core service responsible for Persistent Chat Server. This service provides the following functions:

- Accepts incoming messages
- Registers and lists online participants within a Persistent Chat room
- Retransmits messages to other channel subscribers
- Implements logic for channel management, chat room invitation, search, and new content notifications

The Persistent Chat (Channel) service stores and accesses chat room content and other system metadata (authorization rules, and so on) by using the Persistent Chat Store. This service stores files that are uploaded into chat rooms in the Persistent Chat File Store.

Compliance Service

The Compliance service is an optional component of Persistent Chat Server and is responsible for archiving chat content and events to the Persistent Chat Compliance Store. If your organization has regulations that require Persistent Chat activity to be archived, you can deploy the optional Persistent Chat Compliance service. The Compliance service is installed on each Persistent Chat Server in a Persistent Chat pool. When configured, Persistent Chat Server compliance records user activity such as joining and leaving rooms, and posting and reading of messages. The Compliance service stores files that need to be archived in the Persistent Chat Compliance File Store.

Persistent Chat Web Services

On the Lync Server Front End Servers, two services run that depend on Internet Information Services (IIS), and are implemented as web components:

- **Persistent Chat Web Services for File Upload/Download** Responsible for posting and retrieving files from chat rooms.
- **Persistent Chat Web Services for Chat Room Management** Responsible for providing users the ability to manage their chat rooms, and create new chat rooms.

How Do I Start Using Persistent Chat Server?

Persistent Chat Server is an optional server role within the Lync Server 2013 infrastructure. If you install the Persistent Chat Server role, any users who have been enabled through policy by an administrator can use Persistent Chat with the Lync 2013 client.

For details about how to deploy Persistent Chat Server and enable users to leverage the capabilities by policy, see Deploying Persistent Chat Server.

For details about how to configure settings on your Persistent Chat Server deployment, see Deploying Persistent Chat Server and Managing Lync Server 2013, Persistent Chat Server.

For details about how to enable users by policy such that they can leverage Persistent Chat functionality in Lync 2013 client, see Deploying Persistent Chat Server and Managing Lync Server 2013, Persistent Chat Server.

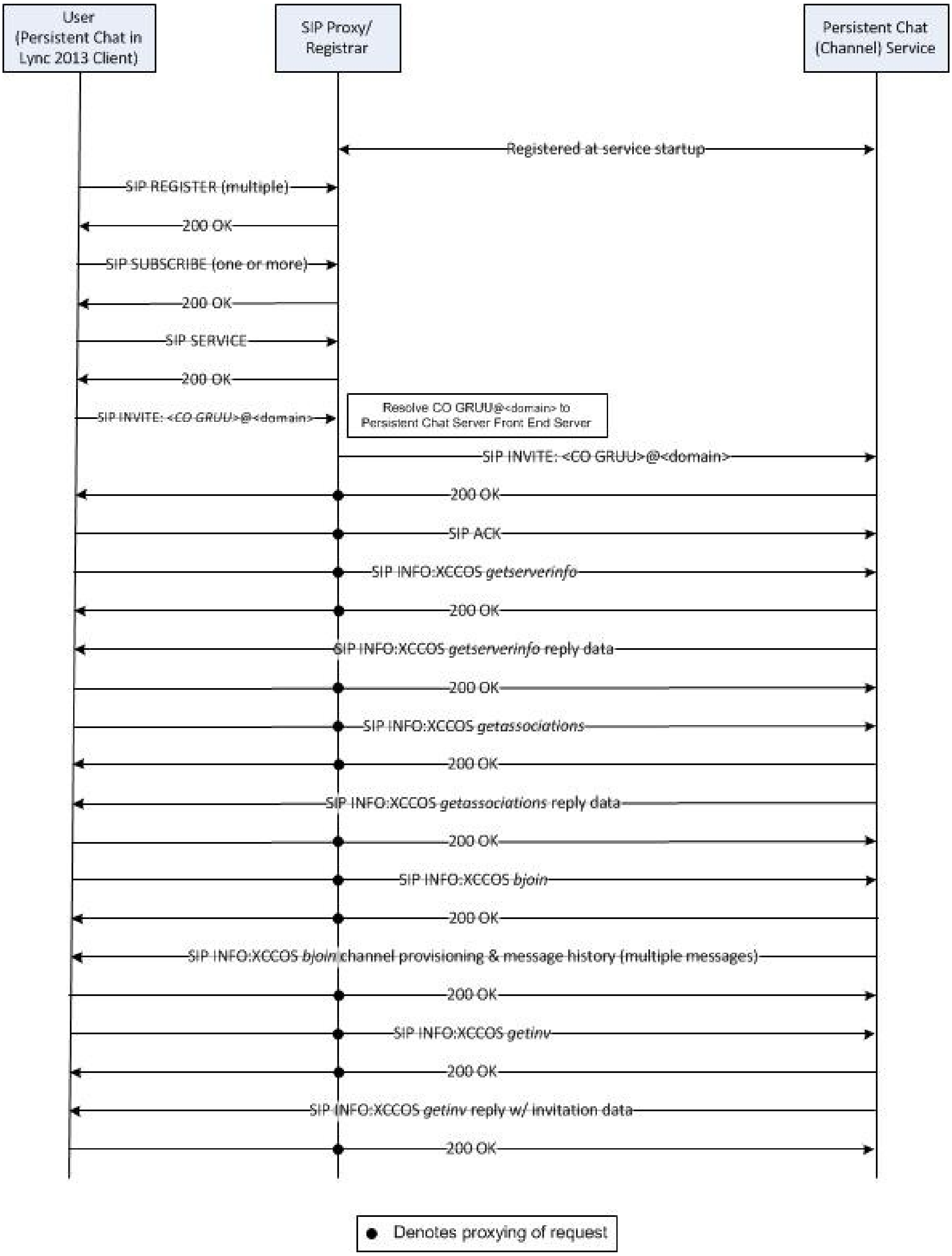
If you deployed Persistent Chat compliance, see Managing Lync Server 2013, Persistent Chat Server for details about how to configure settings for compliance.

Persistent Chat Call Flows

The Persistent Chat client communicates with the Persistent Chat service by using XCCOS. The following sequences describe the sign-in process and a typical room subscription and message post scenario.

Sign-in

The following call flow diagram and steps describe the sign-in process.


User (Persistent Chat in Lync 2013 Client)
SIP Proxy/ Registrar
Persistent Chat (Channel) Service
Registered at service startup
SIP REGISTER (multiple)
200 OK
SIP SUBSCRIBE (one or more)
200 OK
SIP SERVICE
200 OK
SIP INVITE: <CO GRUU>@<domain>
Resolve CO GRUU@<domain> to Persistent Chat Server Front End Server
SIP INVITE: <CO GRUU>@<domain>
200 OK
SIP ACK
SIP INFO:XCCOS getserverinfo
200 OK
SIP INFO:XCCOS getserverinfo reply data
200 OK
SIP INFO:XCCOS getassociations
200 OK
SIP INFO:XCCOS getassociations reply data
200 OK
SIP INFO:XCCOS bjoin
200 OK
SIP INFO:XCCOS bjoin channel provisioning & message history (multiple messages)
200 OK
SIP INFO:XCCOS getinv
200 OK
SIP INFO:XCCOS getinv reply w/ invitation data
200 OK
● Denotes proxying of request

1. The Persistent Chat client first sends a SIP SUBSCRIBE to retrieve the in-band provisioning document from the server. This document indicates if Persistent Chat is enabled or disabled for the user and the list of SIP URIs for the Persistent Chat Server pool.
2. The Persistent Chat client sends a SIP INVITE message to the SIP URI of the Persistent Chat Server that it obtained in the previous step. The INVITE sequence is followed by 200 OK and ACK, and the Persistent Chat client has

now opened a SIP session with a Persistent Chat Server endpoint. Consequently, the Persistent Chat client communicates with Persistent Chat Server by sending SIP INFO messages that contain either chat messages or commands requesting the server to take an action. All of these messages are acknowledged with either 200 OK or 503 Service Unavailable (that is, in the event of heavy server load). If the client receives a 503 response, it will retry the message. (This example does not include a 503 response.) If the server accepts the message or command and sends 200 OK, it provides a response to the client in the form of a separate SIP INFO message. This response includes a reference to the originating command.

3. The Persistent Chat client sends a SIP INFO message that contains the XCCOS **getserverinfo** command. Persistent Chat Server replies with a new SIP INFO message that contains information about the Persistent Chat service configuration.
4. The Persistent Chat client sends a SIP INFO message that contains the XCCOS **getassociations** command. Persistent Chat Server replies with a new SIP INFO message that contains the list of rooms of which the user is a member. The Persistent Chat client repeats the command to retrieve the list of rooms of which the user is a manager.
5. The Persistent Chat client gets the list of followed rooms from the "presence" document, where each followed room is represented by a "roomSetting" category. All followed rooms are joined by a single SIP INFO message that contains the XCCOS **bjoin** command that contains the list of room URIs. Because the list of followed rooms is kept on the server, any client on any computer has the same list of followed rooms for the specified user URI. The Persistent Chat client also keeps the list of opened rooms (if this option is enabled by the user) in the local computer registry, and joins each of these rooms at sign-in by sending a SIP INFO message that contains the XCCOS **join** command for each opened room. Because this list is kept in the registry, it can be different on two Persistent Chat clients running on different computers.
6. For each room joined, the Persistent Chat client sends a SIP INFO message that contains the XCCOS **bccontext** command. Persistent Chat Server replies with a new SIP INFO message that contains the most recent chat message in the room.
7. The Persistent Chat client sends a SIP INFO message that contains a XCCOS **getinv** (that is, get invitation) command to request any new room invitations that the client has not yet seen. In a separate SIP INFO message, Persistent Chat Server returns a list of those rooms.

Subscribe to a Room and Post a Message

The following call flow diagram and steps describe a typical room subscription and message post scenario.

1. From the Persistent Chat client, User1 clicks **Join a Chat Room**, clicks **Search**, and then enters some search criteria. The Persistent Chat client sends a SIP INFO message that contains the XCCOS **chansrch** (room search) command, along with the search criteria. Persistent Chat Server queries the back-end database and replies in a new SIP INFO message that contains a list of available rooms that meet the search criteria.
2. User1 selects the chat room that he or she wants to join, and then clicks **Follow this room**. The Persistent Chat client sends Persistent Chat Server a SIP INFO message that contains the XCCOS **join** command and the room ID of the chat room that the user selected. Persistent Chat Server replies with a SIP INFO message that contains the provisioning data.
3. The Persistent Chat client sends Persistent Chat Server a SIP INFO message that contains the XCCOS **bccontext** (backchat context) command. Persistent Chat Server retrieves the chat history, and returns it to the Persistent Chat client in a separate SIP INFO message. At this point, the user enters the chat

room and is ready to participate.
4. User1 enters a new message, and then clicks **Send**. The Persistent Chat client posts the message to the chat room in a SIP INFO XCCOS **grpchat** command. Persistent Chat Server stores a copy of this new message in the Persistent Chat back-end database.
5. Persistent Chat Server sends a separate copy of the SIP INFO XCCOS **grpchat** message to User2, who has already entered the chat room.

Persistent Chat Compliance Call Flows

Persistent Chat Server uses Message Queuing (also known as MSMQ) and an additional compliance database (mgccomp) to process compliance data. As an example of how compliance events are processed, the following sequence of events describes how a message post event is processed.

1. A user posts a message to a room.
2. Persistent Chat Server places information pertaining to the event in a private Message Queuing queue.
3. Persistent Chat Compliance server reads this event from the queue, and places it into the mgccomp database for processing later.
4. Periodically, the Persistent Chat Compliance server processes a set of events in the database, and sends them to the Persistent Chat Compliance adapter for processing.
5. If the adapter successfully processes the data, Persistent Chat Compliance server deletes the events from the mgccomp database.

1.3.13.3 Defining Your Organization's Requirements for Persistent Chat Server

Defining Your Organization's Requirements for Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

***Topic Last Modified:** 2012-09-30*

Before you deploy Persistent Chat Server for your organization, it’s essential to consider the following key questions to optimize your deployment:

- Who (user profile) should be enabled for Persistent Chat Server? Persistent Chat Server is enabled by a policy that can be set at a Global, Site, Pool or User level.
- How many users (scale) should be enabled for Persistent Chat Server? Persistent Chat Server supports 150,000 provisioned users (enabled by policy), and a maximum of 80,000 concurrent users using Persistent Chat Server. A single Persistent Chat Server can support 20,000 connected users, and a single Persistent Chat Server pool can have up to 4 active servers for a total of 80,000 concurrently connected users.
- Are you migrating from a previous version of Group Chat Server, or are you deploying Persistent Chat Server for the first time?
- Are there compliance requirements? Persistent Chat Server supports compliance. The compliance service runs collocated on the Persistent Chat Server Front End Server, as opposed to the requirement for a separate computer in previous Group Chat Server deployments. Compliance is optional, and if chosen, requires a compliance database that must be configured to store compliance data and events. You may want to also configure an adapter to take the data from the compliance database and convert to another format (such as XML files or Exchange-hosted archives).
- How do you want to control scopes, ethical boundaries, and access? You can define **Categories** to segregate these boundaries, and choose who is allowed to be in rooms that are created in each of these categories.

- How do you want to control who can create rooms? You can configure **Creators**, appropriate to your categories, who can create rooms. Creators can assign other members as **Chat Room Managers** for ongoing management of the rooms (adding or removing additional members), according to the scope for **AllowedMembers/DeniedMembers** configured by the category.
- How do you want to create rooms? Persistent Chat Server provides a web-based feature for room creation and management. This can be launched from the Lync 2013 client. You can choose to define a custom solution (by using the Persistent Chat Server Software Development Kit (SDK)) that implements your business requirements and workflows, and configures Persistent Chat Server to direct users to your custom solution.
- What kind of add-ins do you want to provision? **Add-ins** enhance the in-room experience by leveraging the extensibility pane in the Lync 2013 client to provide context that is relevant to the room. You can choose what general add-ins might be most useful (for example, your company website, internal collaboration documents, and so on). Chat room managers can choose one of the registered add-ins and associate it with their rooms, if desired.
- What kind of high availability and disaster recovery requirements do you have? Persistent Chat Server supports SQL Server mirroring for high availability and supports up to 8 servers (4 active and 4 standby) in a stretched pool with SQL Server log shipping for disaster recovery.
- Are there regulatory requirements? If your company is in a country/region where data needs to be kept globally, you may need to deploy multiple Persistent Chat Server pools, each local to a specific geography. A room, category, or add-in does not span pools—it belongs to only one Persistent Chat Server pool. Users can be configured to have access to rooms in one or more pools, depending on how you design your categories.

Important:
Having multiple Persistent Chat Server pools does not give you more scale (you can still have only 80,000 concurrently connected users across all your Persistent Chat Server pools).

1.3.13.4 User Roles in Persistent Chat Server

User Roles in Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-10-05*

Persistent Chat Server provides the concept of Allowed/Denied members, which applies to Persistent Chat categories and controls who can access rooms in a particular category.

Important:
Allowed/Denied members in a Category is not the same as a **Member** role, which applies to a Persistent Chat room. Searches display all open and closed chat rooms for which the user performing the search is in the Allowed/Denied member list. Secret rooms are not displayed unless the user who performs the search is a member of the secret room. The user can search only for rooms that he or she is already a member of, or those for which they can request membership.

The primary rationale for the concept of Allowed/Denied Members is ethical walls. For example, it is common in banking and financial institutions to have ethical boundaries that prevent traders and analysts from sharing communications while implementing policies and conventions. To address this requirement, an administrator can create categories so that one category allows rooms to be created and used by traders, and another category allows rooms to be created and used by analysts. With this constraint is designed into the system prohibits adding a user as a member of the room if the parent category prevents it.

Following are the four user roles Persistent Chat Server:

- **Creator:** Users who have permissions to create chat rooms. These users are in the Creators list of certain categories: they can create chat rooms in that category, and they can also assign membership according to the category, and assign managers to manage the chat room. The user who creates a chat room is automatically added as a manager of the room.

  Note:

  Being a Creator simply provides rights for creating chat rooms. It is the automatic promotion to Manager that enables the Creator to further refine memberships, managers, and so on, on the created chat services.

  This role exists to give you the option of controlling who creates chat rooms in your organization, particularly if you want to centrally manage creating chat rooms to enforce policies and conventions, and subsequently delegate the chat room management to other users in the organization.
- **Manager:** Users who manage properties of a chat room. Chat room managers can modify the member list (add and remove members), and modify the chat room managers list (add and remove managers). Chat room managers can add themselves to the members or presenters list (for auditorium rooms) so they can participate in the chat room. Chat room managers can also disable chat rooms (administrators can query for disabled chat rooms and can permanently delete them). Managers can change all the properties of a chat room, except the category of the chat room. Only the Persistent Chat Administrator can change the category after the chat room has been created.

  Important:

  If the manager is also a Creator in another category, he or she can change the category to one where they are authorized to create rooms.
- **Member:** Users who are members of a chat room. These users can see the chat rooms in the directory (even if the chat room is secret), as well as subscribe to the chat room (including metadata options such as unread messages, ego filters, and keyword filters), and participate in the chat room (can post, unless the room is an auditorium room where only presenters can post, get content, and search). Users who aren't members of the chat room can search for the chat room if they are in the Allowed Members list of the category, but need to request access to join these chat rooms to access content. (There is no request access or approvals built into the system; these are done externally by email, phone, or other forms of contact.)
- **Presenter:** Users who can post to an auditorium room.

The following roles are administrator roles for Persistent Chat Server:

- **Persistent Chat Administrator (CsPersistentChatAdministrator):** This is a new Role-Based Access Control (RBAC) role to administer and manage Persistent Chat Server. Users or security groups designated as CsPersistentChatAdministrator are able administer Persistent Chat Server by using Windows PowerShell cmdlets remotely (that is, from a computer other than the Persistent Chat Server). Persistent Chat Server checks that the Persistent Chat Administrator is member of the RTC Local administrator local group on the Persistent Chat Server Front End Server.
  The CsPersistentChatAdministrator role can manage chat rooms (modify all properties including membership, managers, categories, mark rooms as disabled), as well as create and manage chat room categories that define who can create and access chat rooms. Administrators can also mark chat rooms as disabled and clean up chat rooms that are no longer active. Administrators are not subject to the Creators or Allowed Members restrictions. Administrators can create any kind of chat room and add themselves as a member to any chat room. Administrators can also modify and manage Persistent Chat

configuration (pool properties, global settings, and compliance configuration) and can also plan and implement migration from an older Group Chat Server deployment to Lync Server 2013 Persistent Chat Server.

- **Lync Administrator:** Overall enterprise administrator for Lync Server 2013 responsible for deployment.
- **Operations Manager:** User responsible for managing day-to-day operations.
- **Third-party developers and partners:** Third-party developers extend the system, in particular providing an ethical wall solution for group conversations, compliance support and tools, web/mobile clients, and a framework for Bot development.

1.3.13.5 Components and Topologies for Persistent Chat Server

Components and Topologies for Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-10-05*

Persistent Chat Server supports both single-server configurations and multiple-server configurations. Persistent Chat Server can also run on a Lync Server 2013 Standard Edition server. These configurations consist of the following Persistent Chat Server components and topologies.

Persistent Chat Server Components

Installing the latest version of Persistent Chat Server requires the following components:

- One or more computers running Persistent Chat Server and providing the following services:
  - Persistent Chat service
  - Compliance service, which is turned on if compliance is enabled

  Important:

  In Lync Server 2013, the Persistent Chat Web Services for File Upload/Download is now collocated with Lync Server 2013 Front End Server. The Persistent Chat Web Services for Chat Room Management is also collocated with Lync Server 2013 Front End Server.

- Server(s) (more than one server if mirroring is used) that host the SQL Server back-end database for hosting the Persistent Chat content database where chat room content, rooms, and categories are stored.

  Note:

  The back-end database stores chat history data, including information about categories and Persistent Chat rooms that are created.

- If compliance was enabled, a server(s) (more than one server if mirroring is used) that host the SQL Server back-end database for hosting the Persistent Chat Compliance database, where compliance events and chat content for the purpose of compliance are stored.

To administer Persistent Chat Server from a separate computer (such as an administrative console), use the Lync Server Control Panel on the computer. This computer must then be deployed in an Active Directory Domain Services (AD DS) domain, with at least one global catalog server in the forest root.

For details about hardware and software requirements for Persistent Chat Server, see Technical Requirements for Persistent Chat Server, Supported Hardware, and Server Software and Infrastructure Support in the Supportability documentation.

Supported Collocation

Lync Server 2013 supports a variety of collocation scenarios, providing you the flexibility to save hardware costs by running multiple components on one server (if you have a small organization), or to run individual components on different servers (if you have a larger organization that needs scalability and performance). Scalability factors should certainly be considered before you decide whether to collocate components.

The Persistent Chat Compliance service, if compliance is enabled, is collocated with the Lync Server 2013 Front End Server.

Persistent Chat Server can be deployed on the Standard Edition server. The Persistent Chat Server Back End Server and the Persistent Chat Compliance database can be collocated on the Standard Edition server on the local SQL Server Express Back End Server. For details about components that can be collocated there, see Supported Server Collocation in the Supportability documentation.

For Lync Server 2013 Enterprise Edition, Persistent Chat Servers cannot be collocated on the Enterprise Edition server. The SQL Server database for Persistent Chat Server can be collocated with the Back End Server database of an Enterprise Edition Front End pool. The SQL Server database for Persistent Chat compliance can also be collocated with the Back End Server database of an Enterprise Edition pool.

Important:

The server hosting the Persistent Chat database can host other databases. However, when you consider collocating the Persistent Chat database with other databases, be aware that if you are storing the messages of more than a few users, the disk space needed by the Persistent Chat database can grow very large. For this reason, we do not recommend collocating the Persistent Chat database with the back-end database.

If you collocate the Persistent Chat database with the back-end database, you can either use a single instance of SQL Server for any or all of the databases, or you can use a separate instance of SQL Server for each database, with the following limitation:

- Each instance of SQL Server can contain only a single back-end database and a single Persistent Chat database.

For details about collocation of all server roles and databases, see Supported Server Collocation in the Supportability documentation.

Persistent Chat Server Topologies

Persistent Chat Server supports the following topologies:

- Lync Server 2013 Enterprise Edition single server Persistent Chat Server Front End Server
- Lync Server 2013 Enterprise Edition multiple server Persistent Chat Server Front End Server
- Lync Server 2013 Standard Edition server using SQL Server Express
- Lync Server 2013 Standard Edition server and Persistent Chat Server on a separate server using Standard Edition server as the next hop server.

You can add Persistent Chat Server to your Lync Server 2013 deployment by using Topology Builder. You can add a single server or a multiple server Persistent Chat Server pool to your topology.

Important:

After you create a Persistent Chat Server pool with a single server by using Topology Builder, you cannot add additional servers to the pool.

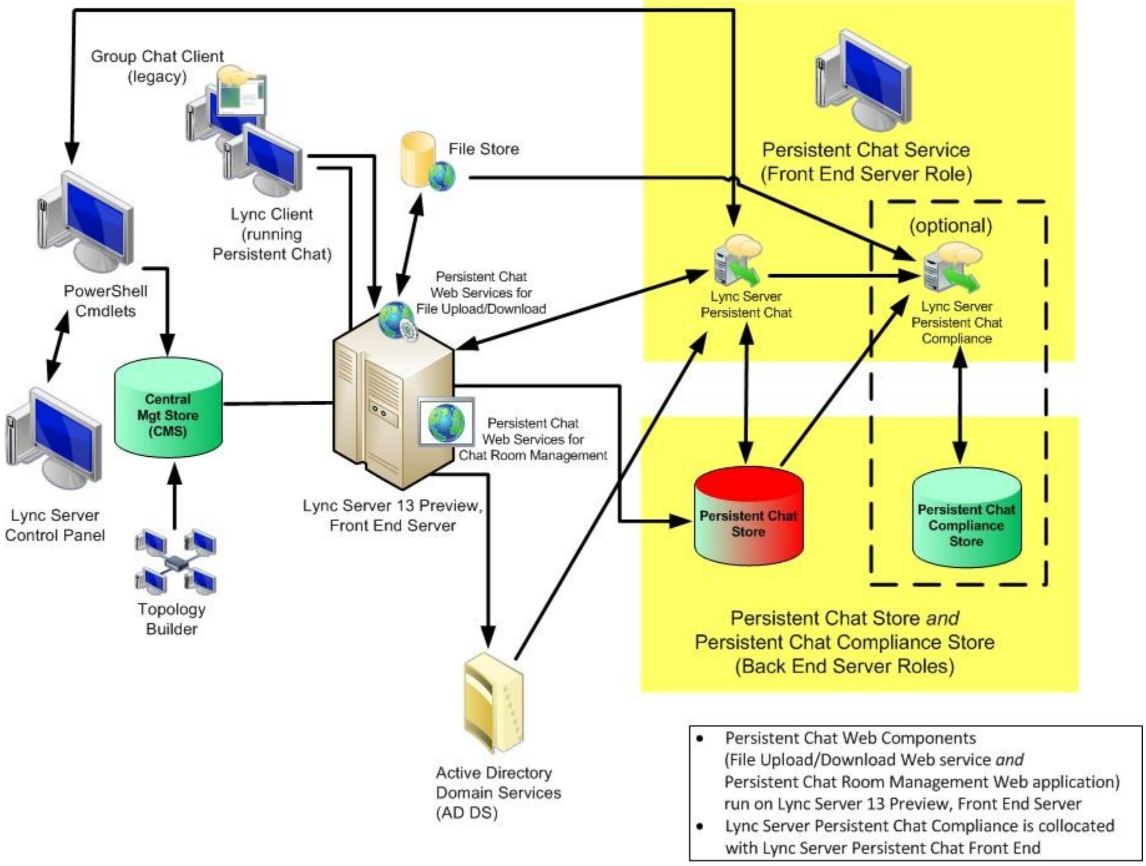
Single-Server Topology

The minimum configuration and simplest deployment for Persistent Chat Server is a single Persistent Chat Server Front End Server topology. This deployment requires a single server that runs Persistent Chat Server (which optionally runs the Compliance service, if compliance is enabled), a server that hosts both the SQL Server database, and if compliance is required, the SQL Server database to store the compliance data.

Important:

You cannot add additional servers to a Persistent Chat Server pool that is started as a single-server deployment in Topology Builder. We recommend using the multiple-server pool topology, even if you're using a single server, so that you can add more servers later, if needed..

The following figure shows all required and optional components of a topology for a single Persistent Chat Server Front End Server with compliance.

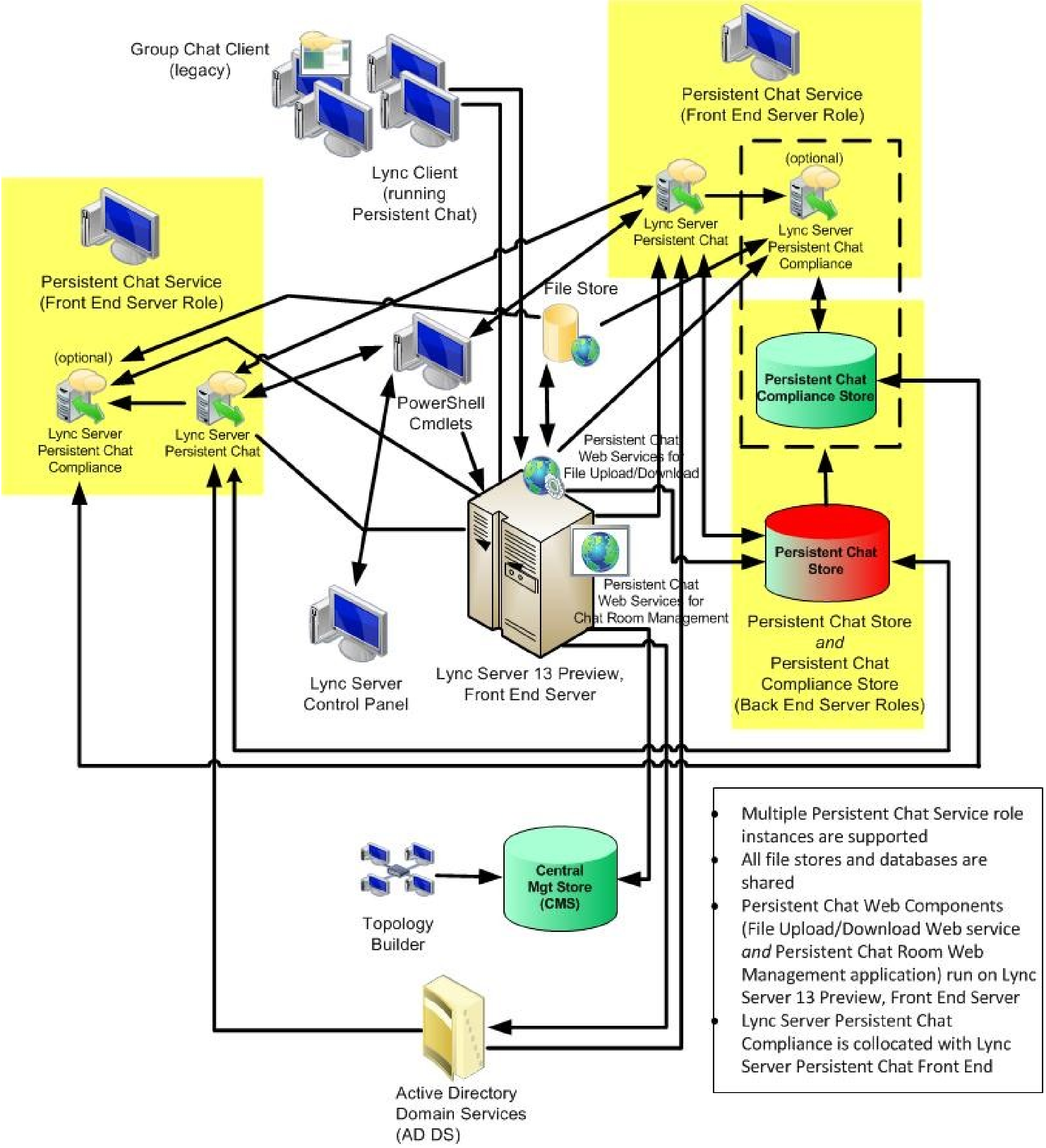


- Persistent Chat Web Components (File Upload/Download Web service *and* Persistent Chat Room Management Web application) run on Lync Server 13 Preview, Front End Server
- Lync Server Persistent Chat Compliance is collocated with Lync Server Persistent Chat Front End

Multiple-Server Topology

To provide greater capacity and reliability, you can deploy a multiple-server topology, as described in Planning for Persistent Chat Server. The multiple-server topology can include as many as four active computers running Persistent Chat Server (high availability and disaster recovery configurations will allow up to eight, but only four can be active and the remaining four on standby). Each server can support as many as 20,000 concurrent users, for a total of 80,000 concurrent users connected to a Persistent Chat Server pool with 4 servers. A multiple-server topology is the same as the single-server topology except that multiple servers host Persistent Chat Server, and can scale higher. Multiple computers running Persistent Chat Server should reside in the same Active Directory Domain Services (AD DS) domain as Lync Server and the Compliance service.

The following figure shows all the components of a multiple-server topology with multiple computers running Persistent Chat Server, the optional Compliance service, and a separate compliance database.



- Multiple Persistent Chat Service role instances are supported
- All file stores and databases are shared
- Persistent Chat Web Components (File Upload/Download Web service *and* Persistent Chat Room Web Management application) run on Lync Server 13 Preview, Front End Server
- Lync Server Persistent Chat Compliance is collocated with Lync Server Persistent Chat Front End

Multiple-server topologies provide pooling of server functionality. In a server pool, the Persistent Chat services communicate and share data. For example, chat history that was originally posted to one Persistent Chat service is available from any Persistent Chat service in the system. A file that is uploaded through one Persistent Chat service can be accessed by any Persistent Chat service. Users can be connected to different Persistent Chat Server Front End Servers and can be chatting and communicating with each other.

The default port of TCP 8011 connects a server to a server pool, and is used by the Persistent Chat service to communicate between themselves, or for administrative purposes.

1.3.13.6 Technical Requirements for Persistent Chat Server

Technical Requirements for Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2013-01-06*

Each computer that hosts Persistent Chat Server must have access to an existing Lync Server 2013 topology with the following components:

- **Lync Server 2013, Front End Server.** The Front End Server is the foundation for Session Initiation Protocol (SIP) routing, which makes communication between computers running Persistent Chat Server and the Persistent Chat functionality possible. Before you begin to deploy Persistent Chat Server, verify the deployment of Lync Server 2013, Standard Edition, or a Lync Server Front End pool and any other internal computers running Lync Server, as appropriate to your organization.

The following sections describe the specific requirements for the Persistent Chat Server and the database that stores the Persistent Chat data.

Persistent Chat Server Requirements

For details about the recommended hardware for deploying Lync Server and the latest version of Persistent Chat Server, see Server Hardware Platforms in the Supportability documentation.

For details about the server and tools operating system support for Lync Server and Persistent Chat Server, see Server and Tools Operating System Support in the Supportability documentation.

For details about additional software required for deploying Persistent Chat Server, see the following table.

Persistent Chat Server Software Prerequisites

Software	Description
Message Queuing	Used by the Persistent Chat Server and Persistent Chat Compliance service, if deployed.

Persistent Chat Server Database Requirements

Persistent Chat Server uses the Persistent Chat database to store chat history, configuration, and user provisioning data. Optionally, it uses the Persistent Chat compliance database to store compliance data.

◆**Important:**
The Persistent Chat database (mgc) and the compliance database (mgccomp) can be located in the same instance of SQL Server or on different SQL Servers.

To prepare a database server platform, be sure that each computer meets the hardware requirements, and then install the prerequisite software.

The server platform for the Persistent Chat database servers requires the same hardware as the Lync Server back-end database server. For details, see Server Hardware Platforms in the Supportability documentation.

On the database server, be sure that one of the following software applications is installed:

- Microsoft SQL Server 2012. For details about how to install Microsoft SQL Server 2012, see "Install SQL Server 2012" at http://go.microsoft.com/fwlink/p/?LinkID=248559.
- Microsoft SQL Server 2008 R2. For details about how to install Microsoft SQL Server 2008 R2, see "SQL Server Installation (SQL Server 2008 R2)" at http://go.microsoft.com/fwlink/?LinkId=275702.

Persistent Chat Server Certificate Requirements

For details about acquiring certificates, creating the SQL Server database, and creating file stores, see Deploying Lync Server 2013 in the Deployment documentation.

1.3.13.7 Setting Up Systems and the Infrastructure for Persistent Chat Server

Setting Up Systems and the Infrastructure for Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-03-23*

Before deploying Lync Server 2013, Persistent Chat Server, you need to deploy the appropriate hardware and software for all Persistent Chat Server components.

In This Section

- Set Up System Platforms
- Install Lync Server 2013 Prerequisite Software

1.3.13.8 Deployment Checklist for Persistent Chat Server

Deployment Checklist for Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-10-16*

Deployment of Lync Server 2013, Persistent Chat Server requires that you deploy it in the correct sequence and that you complete all required deployment steps.

Deployment Sequence

You can deploy Persistent Chat Server after you deploy your initial topology, including at least one Lync Server 2013, Front End pool or one Lync Server 2013, Standard Edition server. This topic describes how to deploy Persistent Chat Server by adding it to an existing deployment.

Deployment Process

The following table lists the basic steps to deploy Persistent Chat Server and provides links for more details.

Persistent Chat Server Deployment Process

Task	Steps	Required roles and group memberships	Related topics
Install prerequisite hardware and software	On hardware that meets system requirements, install the following: • On the Persistent Chat Server Front End Servers: • An operating system that meets system requirements • Software prerequisites for computers running Lync Server 2013 • SQL Server on the server that will host Persistent Chat Server database If Persistent Chat Server compliance is required: • SQL Server on the server that will host Persistent Chat Server compliance database	Any user who is a member of the local Administrators group.	Supported Hardware in the Supportability documentation Server Software and Infrastructure Support in the Supportability documentation Determining Your System Requirements Technical Requirements for Persistent Chat Server
Create the appropriate internal topology to support Persistent Chat Server (and optionally, Persistent Chat compliance)	Run Topology Builder to add a Persistent Chat Server pool to your topology: • Add Persistent Chat Server components to the topology • Create a SQL Server database for the Persistent Chat Server store (and a backup SQL Server for disaster recovery) • Define a new Lync File Store or use an existing Lync File Store for Persistent Chat Server files • Associate the Lync	To define a topology, an account that is a member of the local Users group. To publish the topology, an account that is a member of the Domain Admins group and RTCUniversalServerAdmins group, and the user should also have full control permissions (read/	Adding Persistent Chat Server to Your Deployment in the Deployment documentation

	Server 2013 pool that can route requests to this Persistent Chat Server pool If Persistent Chat compliance is required: • Add Persistent Chat Compliance Store • Click the Persistent Chat Server pool definition check box for enabling compliance • Publish the topology If you install Persistent Chat Server on Standard Edition, the fully qualified domain name (FQDN) of the Persistent Chat Server pool must match the Standard Edition server, and the SQL Server databases are collocated on the SQL Server Express instance on the Standard Edition server	write/modify) on the Lync File Store for Persistent Chat Server files (so that Topology Builder can configure the required DACLs).	
Deploy Persistent Chat Server	Run the Lync Server setup on all the computers running Persistent Chat Server. The Persistent Chat Server setup is integrated into the Lync Server 2013 Deployment wizard that provides the following instructions: • Deploy local management store • Install Persistent Chat Server services • Request and assign certificates • Run and start the services	Any user who is a member of the local Administrators group.	Deploying Persistent Chat Server in the Deployment documentation
Create a Persistent Chat administrator	Add users to the CsPersistentChatAdministrator security group.	Any user who is a member of domain administrators.	Adding a Persistent Chat Administrator in the Deployment documentation
Configure Persistent Chat Server	Configure users: • User has to be enabled by policy to access Persistent Chat Server. By default, the policy is turned off for all users and can be defined at global/ site/pool/user	User must be a member of CsPersistentChatAdministrator. To change policy, user must be in CsUserAdministrator, at a minimum.	Configuring Persistent Chat Server in the Deployment documentation

	scopes. - Configure settings		

Important:
You can deploy one or more Persistent Chat Server pools. We support multiple Persistent Chat Server pools for regulatory reasons whereby data generated in a given region is required to stay in that region. For example, if you deploy a Persistent Chat Server pool in Chicago, and another in Zurich to comply with regulations for data in Switzerland, users can connect to rooms in both the Persistent Chat Server pools, provided they have access.

1.3.13.9 Capacity Planning for Persistent Chat Server

Capacity Planning for Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-10-05*

Persistent Chat Server can perform multi-user real-time chat that can persist for future retrieval and search. Unlike group instant messaging (IM) that is saved in a user's mailbox if conversation history is configured, a Persistent Chat Server session stays open longer, and the content is saved on a server, along with the messages, files, URLs, and other data that are part of an ongoing conversation.

Capacity planning is an important part of preparing to deploy Persistent Chat Server. This topic provides details about supported Persistent Chat Server topologies and capacity planning tables that you can use to determine the best configuration for your deployment. It also describes how to best manage Persistent Chat Server deployments that require greater capacity at peak times.

To download Persistent Chat Server, see "Microsoft Lync Server 13 Persistent Chat Server" at http://go.microsoft.com/fwlink/p/?linkId=209539.

For details about installing Persistent Chat Server, see Installing Persistent Chat Server and Configuring Persistent Chat Server in the Deployment documentation.

Support tools, such as Lync Server Planning Tool, can further assist you with capacity planning. For details about the Planning Tool, see Beginning the Planning Process in the Planning documentation.

Persistent Chat Server Supported Topologies

You can deploy Persistent Chat Server in single-server or multiple-server pools, and with single-pool or multiple-pool topology.

We now also support Persistent Chat Server on Standard Edition server for new Lync Server 2013 deployments. However, performance and scale will be affected, and because there is no high availability option for this new deployment, we expect you to use this primarily for the purposes of proof of concept, evaluation, and so on.

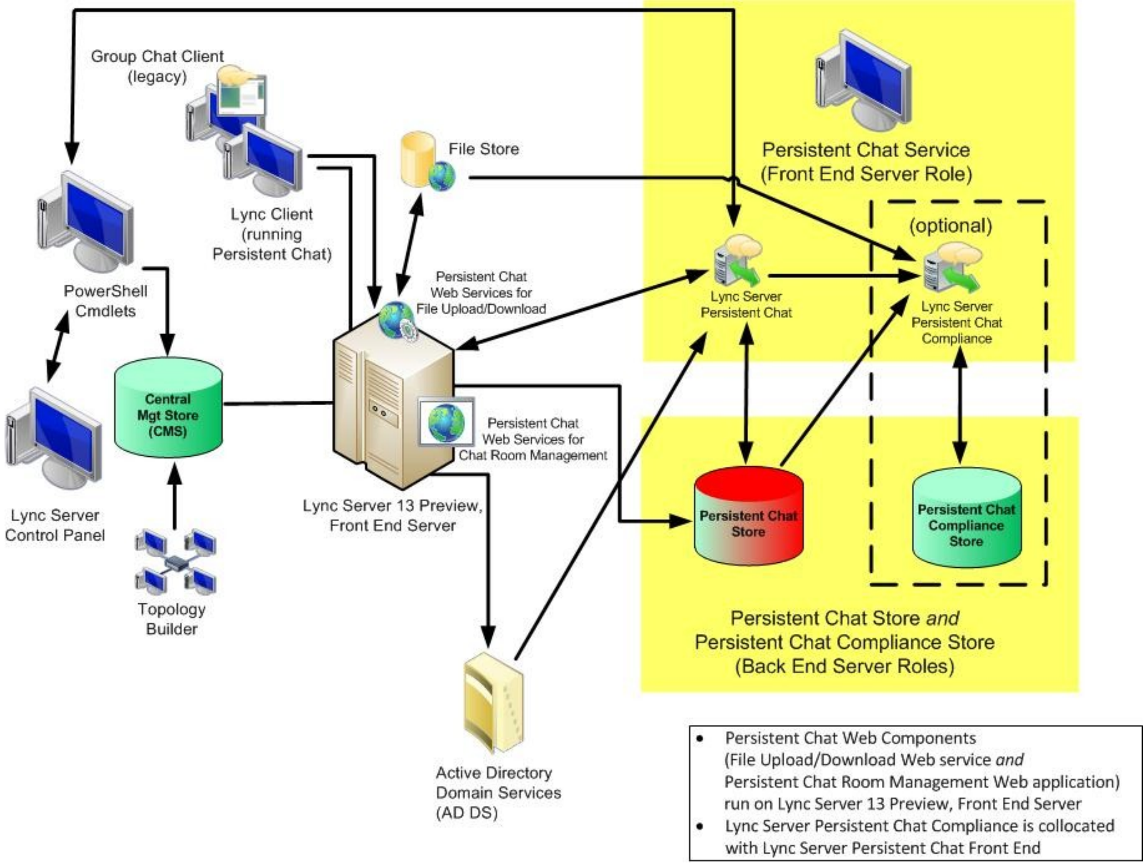
Note:
For additional details about both topologies, see Planning for Persistent Chat Server in this documentation set and Deploying Persistent Chat Server in the Deployment documentation.

Single-Server Topology

The minimum configuration and simplest deployment for Persistent Chat Server is a single Persistent Chat Server Front End Server topology. This deployment requires a single server that runs Persistent Chat Server (which optionally runs the Compliance service, if compliance is enabled), a server that hosts both the SQL Server database, and if compliance is required, the SQL Server database to store the compliance data.

> **Important:**
>
> You cannot add additional servers to a Persistent Chat Server pool that is started as a single-server deployment in Topology Builder. We recommend using the multiple-server pool topology, even if you're using a single server, so that you'll be able to add more servers later, if needed.

The following figure shows all required and optional components of a topology for a single Persistent Chat Server Front End Server with compliance.

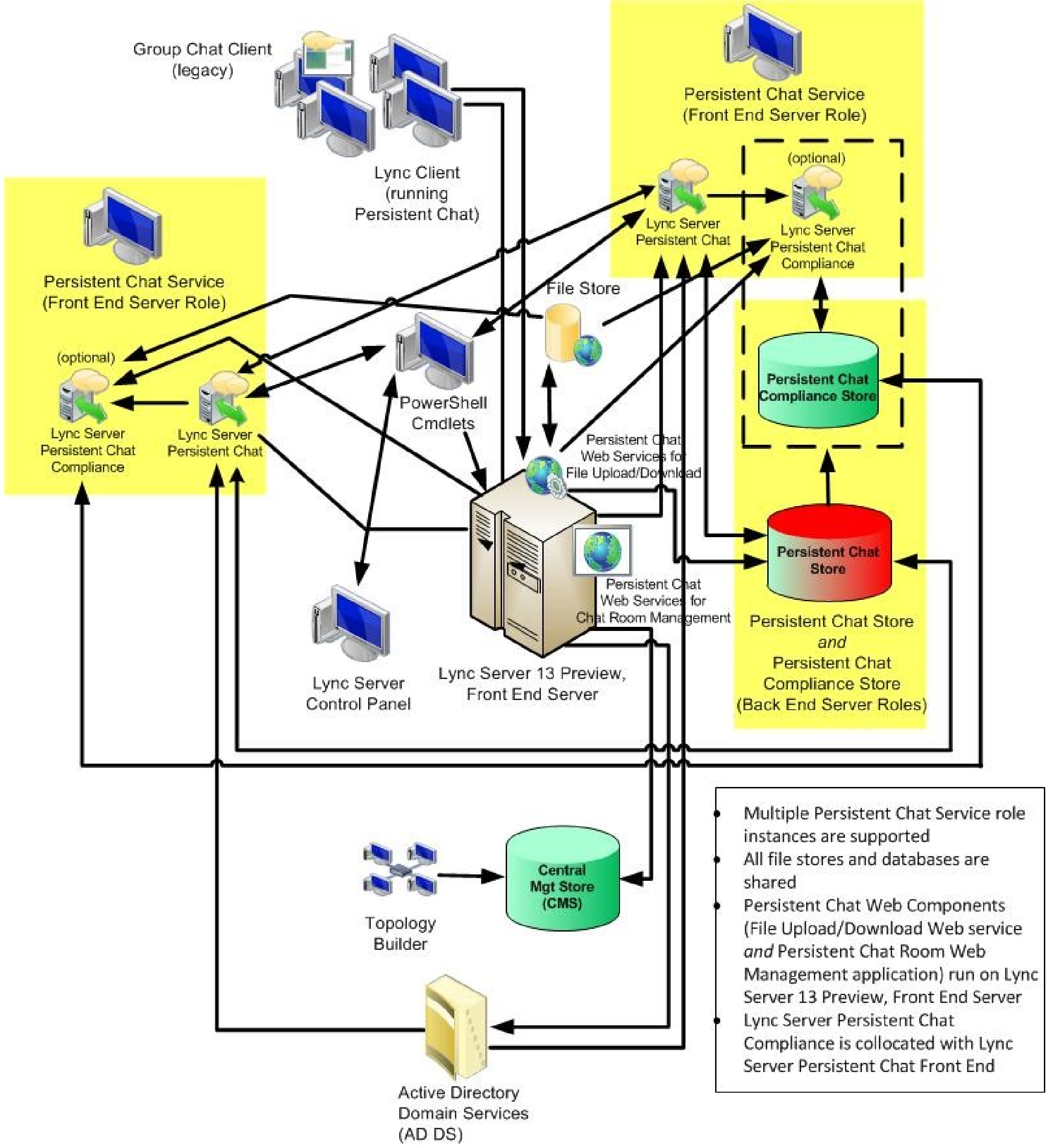

Group Chat Client (legacy)
Lync Client (running Persistent Chat)
File Store
Persistent Chat Service (Front End Server Role)
(optional)
PowerShell Cmdlets
Persistent Chat Web Services for File Upload/Download
Lync Server Persistent Chat
Lync Server Persistent Chat Compliance
Central Mgt Store (CMS)
Persistent Chat Web Services for Chat Room Management
Lync Server Control Panel
Lync Server 13 Preview, Front End Server
Persistent Chat Store
Persistent Chat Compliance Store
Topology Builder
Persistent Chat Store *and* Persistent Chat Compliance Store (Back End Server Roles)
Active Directory Domain Services (AD DS)

- Persistent Chat Web Components (File Upload/Download Web service *and* Persistent Chat Room Management Web application) run on Lync Server 13 Preview, Front End Server
- Lync Server Persistent Chat Compliance is collocated with Lync Server Persistent Chat Front End

Multiple-Server Topology

To provide greater capacity and reliability, you can deploy a multiple-server topology, as described in Planning for Persistent Chat Server. The multiple-server topology can include as many as four active computers running Persistent Chat Server (high availability and disaster recovery configurations will allow up to eight, but only four can be active and the remaining four on standby). Each server can support as many as 20,000 concurrent users, for a total of 80,000 concurrent users connected to a Persistent Chat Server pool with 4 servers. A multiple-server topology is the same as the single-server topology except that multiple servers host Persistent Chat Server, and can scale higher. Multiple computers running Persistent Chat Server should reside in the same Active Directory Domain Services (AD DS) domain as Lync Server and the Compliance service.

The following figure shows all the components of a multiple-server topology with multiple computers running Persistent Chat Server, the optional Compliance service, and a separate compliance database.


Group Chat Client (legacy)
Lync Client (running Persistent Chat)
Persistent Chat Service (Front End Server Role)
(optional)
Lync Server Persistent Chat
Lync Server Persistent Chat Compliance
Persistent Chat Service (Front End Server Role)
(optional)
Lync Server Persistent Chat Compliance
Lync Server Persistent Chat
File Store
PowerShell Cmdlets
Persistent Chat Web Services for File Upload/Download
Persistent Chat Compliance Store
Persistent Chat Store
Persistent Chat Web Services for Chat Room Management
Lync Server Control Panel
Lync Server 13 Preview, Front End Server
Persistent Chat Store *and* Persistent Chat Compliance Store (Back End Server Roles)
Central Mgt Store (CMS)
Topology Builder
Active Directory Domain Services (AD DS)

- Multiple Persistent Chat Service role instances are supported
- All file stores and databases are shared
- Persistent Chat Web Components (File Upload/Download Web service *and* Persistent Chat Room Web Management application) run on Lync Server 13 Preview, Front End Server
- Lync Server Persistent Chat Compliance is collocated with Lync Server Persistent Chat Front End

In a four-server Persistent Chat Server deployment, where 80,000 users can be simultaneously signed in to and using Persistent Chat, the load is distributed evenly at 20,000 users per server. If one server becomes unavailable, the users who are connected to that server will lose their access to Persistent Chat Server. The disconnected users will be automatically transferred to the remaining servers until the unavailable server is restored. Depending on the amount of Persistent Chat traffic on the network, this transfer can take a few minutes or longer. Because each of the remaining servers might be hosting as many as 30,000 users, we recommend that you restore the unavailable server as quickly as possible to avoid performance issues. Otherwise, you can make another

Persistent Chat Server available by using the Topology Builder or the Windows PowerShell cmdlet, **set-CsPersistentChatActiveServer**.

Persistent Chat Server Capacity Planning

The following tables can help you with capacity planning for Persistent Chat Server. They model how changing various Persistent Chat Server settings affect capacity capabilities.

Planning Your Maximum Capacity for Persistent Chat Server

Use the following sample table to determine the number of users you will be able to support.

Persistent Chat Server pool Maximum Capacity Sample

Active Persistent Chat service instances	*4*
Persistent Chat service instances	*8 (4 must be inactive; only a maximum of 4 can be active)*
Active users connected	*80,000*
Total provisioned users	150,000
Number of endpoints	120,000

In the preceding sample, the plan is to support the maximum number of users that Persistent Chat Server allows: four servers/instances of the Persistent Chat service (can have four more passive servers running Persistent Chat Server for high availability and disaster recovery) and 20,000 users per server, for a total of 80,000 active users.

Capacity Planning for Managing Persistent Chat Room Access

The following sample table can help you plan for managing Persistent Chat room access in a Persistent Chat Server pool.

Managing Chat Room Access Sample

	Small Chat Rooms	**Medium Chat Rooms**	**Large Chat Rooms**	**Total**
Size of chat rooms (number of users connected)	30 per room	150 per room	16,000 per room	
Chat rooms	32,000	1,067	10	33,077
% of rooms that are auditorium	1%	1%	50%	
% of rooms that are open	3%	3%	50%	
Open rooms (no explicit membership)	960	32	5	997
Non-open rooms (regular rooms with explicit membership)	31,040	1.035	5	32,080

Auditorium rooms (additional presenters entry)	0	32	5	
Rooms managed by direct membership	50%	10%	0%	
Rooms managed by user groups	50%	90%	100%	
User groups in each chat room's membership list for open rooms (not specified explicitly)	0	0	0	
Users in each chat room's membership list for non-open rooms	30	150	16,000	
User groups in each chat room's membership list for non-open rooms	3	5	10	
Users and user groups in each chat room's manager list (for open and non-open rooms)	6	6	6	
Users and user groups in each auditorium chat room's presenters list (for open and non-open rooms)	6	6	6	
User-based membership entities across all non-open rooms	465,600	15,520	-	
User-group-based membership entities across all non-open rooms	46,560	4656	50	
Users and user groups based entities across all auditorium chat rooms	0	192	50	

Users and user groups based manager entities across all chat rooms manager lists	192,000	6,400	60	
Active users per chat room	*30*	*150*	*16,000*	
Chat rooms per user	*12*	*2*	*2*	*16*
User groups in each chat room's membership list	*10*	*10*	*15*	
Rooms managed by user groups	*50%*	*50%*	*50%*	
User-group-based membership entities across all chat rooms	155,200	5173	68	
User-based membership entities across all chat rooms	465,600	77,600	72,000	
Users and user groups in each chat room's manager, presenter, and scope lists	6	6	6	
Users and user groups across all chat rooms' manager, presenter, and scope lists	192,000	6400	60	
Access control entries	704,160	26,768	160	731,088
Maximum access control entries				2,000,000

In the preceding sample, when you deploy the Persistent Chat Servers according to the recommended guidelines, they can handle up to 80,000 active users across a four-server pool with compliance enabled.

This sample shows chat rooms categorized as small (30 active users at any given time), medium (150 active users), and large (16,000 active users). The number of chat rooms of a certain size is computed based on the total number of:

- Active users in the system
- Active users in chat rooms of the given size
- Chat rooms of the given size that a single user joins

For each chat room, the preceding capacity planning table specifies the number of access control entries that are associated with the chat room, including entries that are assigned directly to the chat room. You can control access to individual chat rooms by using access control lists (ACLs). You can also control access at the category level. In an ACL, an individual access control entry can be either a user group—for example, a security group, a distribution list, or a single user. You can define access control entries for chat room managers, presenters, and members.

Important:

In planning your strategy for managing chat rooms, keep in mind that the total number of allowed access control entries is 2 million. If the calculated access control entries exceed 2 million, server performance could degrade significantly. To avoid this issue, whenever possible, be sure that your access control entries are user groups instead of individual users.

Capacity Planning for Managing Chat Room Access by Invitation

You can use the following capacity planning table to understand the number of invitations that Persistent Chat Server creates and stores in the Persistent Chat database when it is configured to send invitations. You manage invitations on the Category by using the **Chat Room Category settings** page in the Lync Server Control Panel, or by using the Windows PowerShell cmdlet, **set-csPersistentChatCategory**. You can manage invitations on a chat room (in line with what the category allows) by using the **Room Management** page launched from the Lync client, or by using a Windows PowerShell cmdlet, **set-csPersistentChatRoom**.

The sample data in the following table assumes that, on the **Chat room settings** page for 50 percent of all chat rooms, the **Invitations** option is set to **Yes**.

Important:

If the calculated value for the number of invitations that is generated by the server exceeds 1 million, server performance could degrade significantly. To avoid this issue, be sure that you minimize the number of chat rooms that are configured to send invitations or restrict the number of users who can join chat rooms that have been configured to send invitations.

Chat Room Access by Invitation Sample

	Small Chat Rooms	**Medium Chat Rooms**	**Large Chat Rooms**	**Total**
Users who can access chat room	30 per room	150 per room	16,000 per room	
Percentage of rooms that have invitations	50%	50%	50%	
Chat rooms configured to send invitations	*16,000*	*533*	*5*	
Users who can access the chat room	*60*	*225*	*16,000*	
Invitations generated by Persistent Chat Server	960,000	120,000	80,000	1,160,000
Maximum allowable				2,000,000

number of invitations				
Model 1 - Start with expected number of messages per room per day				
Chat Rate Per Room (per day)	50	500	100	650
Chat rate (per second) across all rooms	55.56	18.52	0.03	74
Model 2 - Start with number of messages posted per user per day				
Chat rate per user per day	15	5	0.1	20
Chat rate per room (per day)	38	375	800	1,213
Chat rate (per second) across all rooms	41.67	13.89	0.28	56

Persistent Chat Server Performance User Model

The following table describes the user model for Persistent Chat Server. It provides the basis for the capacity planning requirements and represents a typical organization with 80,000 concurrent users on four servers.

Persistent Chat Server Performance User Model

Number of active users connected	80,000
Number of Persistent Chat Server service instances	4
Size of small chat rooms	30 users
Size of medium chat rooms	150 users
Size of large chat rooms	16,000 users
Total number of chat rooms	33,077
Number of small chat rooms	32,000
Number of medium chat rooms	1,067
Number of large chat rooms	10
Total number of chat rooms per user	16
Number of small chat rooms per user	12
Number of medium chat rooms per user	2

Number of large chat rooms per user	2
Number of rooms joined per user	24
Peak join rate	10/second
Total chat rate	24/second
Chat rate for small chat rooms	22.22/second
Chat rate for medium chat rooms	1.67/second
Chat rate for large chat rooms	~0.15/second
Percentage of chat rooms configured for invitations	50%
Percentage of direct memberships	50%
Percentage of group memberships	50%
Average number of ancestor affiliations in Active Directory Domain Services (AD DS)	100 - 200
Number of subscribed contacts per user	80
Average number of endpoints per user	1.5
Average number of visible chat rooms per endpoint	1.5
Average number of visible chat rooms per user	2.25 (50% for 1 room and 50% for 2 rooms); Up to 6 rooms open, one per monitor
Number of participants polled per interval	25 per visible chat room
Length of polling interval	5 minutes
Number of participants polled per second	15,000
Number of presence changes per hour per user	6
Number of presence changes per second	133.33

1.3.14 Planning for Exchange Server Integration

Planning for Exchange Server Integration

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-20*

When you deploy both Exchange and Lync Server in your organization, many features in both products are enhanced. This section contains information about these capabilities.

- Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013
- Planning for Exchange Unified Messaging Integration
- Hosted Exchange Unified Messaging Integration

1.3.14.1 Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Microsoft Lync Server 2013 > Planning > Planning for Exchange Server Integration >

Topic Last Modified: *2012-10-10*

Exchange and Lync Server have a long history of integration and compatibility. This integration is most noticeable within their respective client application. For example, Lync presence information can be reported in Microsoft Outlook; likewise, Lync can use Outlook calendar to automatically update that presence information. (For example, Lync can change your status to Busy any time your calendar shows that you have a meeting scheduled.) Although you do not have to run Exchange in order to run Lync Server (or vice-versa) there's little doubt that using the two products together epitomizes the very definition of the term "better together."

This is especially true with the release of Microsoft Lync Server 2013 and Microsoft Exchange Server 2013. In addition to features, such as unified messaging and IM and presence, that are found in Microsoft Exchange Server 2010 and Microsoft Lync Server 2010, the 2013 releases of the server products include a number of new capabilities. These capabilities include such things as:

- **Lync Archiving Integration**. In Lync Server 2013 administrators still have the option of having instant messaging and Web conferencing transcripts archived to SQL Server (the same way these transcripts were archived in Lync Server 2010). Alternatively, however, administrators can choose to have transcripts archived to Exchange 2013, storing those transcripts in the individual user mailboxes in the same way in which Exchange archives communications. That means a single repository for all your electronic communications (from both Exchange and Lync Server), which makes it much easier to search for and retrieve those archived communications should the need arise.
- **Unified Contact Store**. In Lync Server 2010, users had to maintain separate contact lists in Outlook and Lync; in fact, to ensure that you had the same contacts available in both products you had to maintain duplicate contact lists, one for Outlook and one for Lync. With Lync Server 2013, however, user contacts can be stored in Exchange 2013 and the unified contact store. Using a single contact store enables users to maintain just one set of contacts, with that same set of contacts being available in Lync 2013, Outlook 2013, and Outlook Web Access 2013.
- **High resolution photos**. Lync 2010 could only display small photos of your contacts; that's because those photos were stored in Active Directory, and Active Directory imposes a 48 pixel by 48 pixel size limitation on stored photos. With Lync Server 2013, however, photos can be stored in Microsoft Exchange; that allows for high-resolution photos as large as 648 pixels by 648 pixels. As you might expect, Lync 2013 has been upgraded to allow for the display of these high-resolution photographs.

Keep in mind that these new features require the use of both Lync Server 2013 and Exchange 2013. In addition to that, users who hope to take full advantage of these new capabilities must have accounts on Lync Server 2013 and Exchange 2013, and must be using the latest versions of the client software (e.g., Lync 2013). For example, the unified contact store is not available to users who have been homed on Lync Server 2010; likewise, high-resolution photos cannot be displayed in Lync 2010.

This documentation provides information on integrating Lync Server 2013 and Exchange 2013. including step-by-step information on enabling new features such archiving Integration and the unified contact store. What this documentation does not do is discuss the initial setup and configuration of these two products. For details about deploying Lync

Server 2013 see the Lync Server 2013 Tech Center at http://go.microsoft.com/fwlink/p/?LinkId=246127. For details about deploying Exchange 2013 see the Exchange 2013 Tech Center at http://go.microsoft.com/fwlink/p/?LinkId=268528.

Prerequisites for Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Configuring Partner Applications in Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Configuring Microsoft Lync Server 2013 to Use Microsoft Exchange Server 2013 Archiving

Configuring Microsoft SharePoint Server 2013 to Search for Archived Microsoft Lync Server 2013 Data

Configuring Microsoft Lync Server 2013 to Use the Unified Contact Store

Configuring the Use of High-Resolution Photos in Microsoft Lync Server 2013

Configuring Microsoft Exchange Server 2013 Unified Messaging for Microsoft Lync Server 2013 Voicemail

Integrating Microsoft Lync Server 2013 and Microsoft Outlook Web App 2013

1.3.14.1.1 Prerequisites for Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Prerequisites for Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2012-10-10*

Before you can integrate Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 you must ensure that all the prerequisite steps have been completed. As you might expect, integration cannot take place until both Exchange 2013 and Lync Server 2013 are fully installed and up and running. For details about installing Exchange, see the Exchange 2013 Planning and Deployment documentation at http://go.microsoft.com/fwlink/p/?LinkId=268539. For details about installing Lync Server 2013, see the planning and deployment documentation at http://go.microsoft.com/fwlink/p/?LinkId=254806.

After the servers are up and running you must assign server-to-server authentication certificates to both Lync Server 2013 and Exchange 2013; these certificates allow Lync Server and Exchange to exchange information and to communicate with one another. When you install Exchange 2013, a self-signed certificate with the name Microsoft Exchange Server Auth Certificate is created for you. This certificate, which can be found in the local computer certificate store, should be used for server-to-server authentication on Exchange 2013. For details about assigning certificates in Exchange 2013, see "Configure Mail Flow and Client Access" at http://go.microsoft.com/fwlink/p/?LinkId=268540.

For Lync Server 2013 you can use an existing Lync Server certificate as your server-to-server authentication certificate; for example, your default certificate can also be used as the OAuthTokenIssuer certificate. Lync Server 2013 allows you to use any Web server certificate as the certificate for server-to-server authentication provided that:

- The certificate includes the name of your SIP domain in the Subject field.
- The same certificate is configured as the OAuthTokenIssuer certificate on all of

your Front End Servers.
- The certificate has a length of at least 2048 bits.

For details about server-to-server authentication certificates for Microsoft Lync Server 2013, see Assigning a Server-to-Server Authentication Certificate to Microsoft Lync Server 2013.

After the certificates have been assigned you must then configure the autodiscover service on Exchange 2013. In Exchange 2013, the autodiscover service configures user profiles and provides access to Exchange services when users log on to the system. Users present the autodiscover service with their email address and password; in turn, the services provide the user with information such as:

- Connection information for both internal and external connectivity to Exchange 2013.
- The location of the user’s Mailbox server.
- URLs for Outlook features such as free/busy information, Unified Messaging, and the offline address book.
- Outlook Anywhere server settings.

The autodiscover service must be configured before you can integrate Lync Server 2013 and Exchange 2013. You can verify whether or not the autodiscover service has been configured by running the following command from the Exchange Management Shell and checking the value of the AutoDiscoverServiceInternalUri property:

```
Get-ClientAccessServer
```

If this value is blank, you must assign a URI to the autodiscover service. Typically this URI will look similar to this:

```
https://autodiscover.litwareinc.com/autodiscover/autodiscover.xml
```

You can assign the autodiscover URI by running a command similar to this:

```
Get-ClientAccessServer | Set-ClientAccessServer -AutoDiscoverServiceInternalUri "
```

For details about the autodiscover service, see "Understanding the Autodiscover Service" at http://go.microsoft.com/fwlink/p/?LinkId=268542.

After the autodiscover service has been configured you must then modify the Lync Server OAuth configuration settings; this ensures that that Lync Server knows where to find the autodiscover service. To modify the OAuth configuration settings in Lync Server 2013, run the following command from within the Lync Server Management Shell. When running this command, be sure that you specify the URI to the autodiscover service running on your Exchange server, and that you use **autodiscover.svc** to point to the service location instead of **autodiscover.xml** (which points to the XML file used by the service):

```
Set-CsOAuthConfiguration -Identity global -ExchangeAutodiscoverUrl "https://autod
```

Note:

The Identity parameter in the preceding command is optional; that's because Lync Server only allows you to have a single, global collection of OAuth configuration settings. Among other things, that means that you can configure the autodiscover URL by using this slightly-simpler command:
Set-CsOAuthConfiguration–ExchangeAutodiscoverUrl "https://autodiscover.litwareinc.com/autodiscover/autodiscover.svc"
If you are unfamiliar with the technology, OAuth is a standard authorization protocol used by a number of major websites. With OAuth, user credentials and passwords are not passed from one computer to another. Instead, authentication and authorization is based on the exchange of security tokens; these tokens grant access to a specific set of resources for a specific amount of time.

In addition to configuring the autodiscover service, you must also create a DNS record for the service that points to your Exchange server. For example, if your autodiscover service is located at autodiscover.litwareinc.com you will need to create a DNS record for autodiscover.litwareinc.com that resolves to the fully qualified domain name of your Exchange server (for example, atl-exchange-001.litwareinc.com).

1.3.14.1.2 Configuring Partner Applications in Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Configuring Partner Applications in Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2012-11-12*

Server-to-server authentication typically involves three entities: the two servers that need to communicate with one another, and a third-party security token server. If two servers (for example, Server A and Server B) need to communicate, then both of those servers typically start by contacting a token server and obtain a mutually-trusted security token. Server A then present that security token to Server B (and vice-versa) as a way to guarantee both its authenticity and its trustworthiness.

However, that's a general rule. Lync Server 2013, Microsoft Exchange Server 2013, and Microsoft SharePoint Server 2013 do not need to use a third-party token server when communicating with one another; that's because these server products can create security tokens that can be accepted by one another without the need for a separate token server. (This capability is only available in Lync Server 2013, Exchange 2013, and SharePoint Server 2013. If you need to set up server-to-server authentication with other servers, including other Microsoft server products, then you will need to do so by using a third-party token server.)

In order to set up server-to-server authentication between Lync Server and Exchange you must do two things: 1) you must assign the appropriate certificates to each server; and, 2) you must configure each server to be a partner application of the other server: that means you must configure Lync Server 2013 to be a partner application for Exchange 2013, and you must configure Exchange 2013 to be a partner application for Lync Server 2013.

Configuring Lync Server 2013 to be a Partner Application for Exchange 2013

The easiest way to configure Lync Server 2013 to be a partner application with Exchange 2013 is to run the Configure-EnterprisePartnerApplication.ps1 script, a Windows PowerShell script that ships with Exchange 2013. To run this script, you must provide the URL for the Lync Server authentication metadata document; this will typically be the fully qualified domain name of the Lync Server 2013 pool followed by the suffix /metadata/json/1. For example:

```
https://atl-cs-001.litwareinc.com/metadata/json/1
```

To configure Lync Server as a partner application, open the Exchange Management Shell and run a command similar to this (assuming that Exchange has been installed on drive C: and that it uses the default folder path):

```
"C:\Program Files\Microsoft\Exchange Server\V15\Scripts\Configure-EnterprisePartn
```

After configuring the partner application it is recommended that you stop and restart Internet Information Services (IIS) on your Exchange mailbox and client access servers. You can restart IIS by using a command similar to this, which restarts the service on the computer atl-exchange-001:

```
iisreset atl-exchange-001
```

This command can be run from within the Exchange Management Shell or from any other command window run under administrator privileges.

Configuring Exchange 2013 to be a Partner Application for Lync Server 2013

After you have configured Lync Server 2013 to be a partner application for Exchange 2013, you must then configure Exchange to be a partner application for Lync Server. This can be done by using the Lync Server Management Shell and specifying the authentication metadata document for Exchange; this will typically be the URI of the Exchange autodiscover service followed by the suffix /metadata/json/1. For example:

```
https://autodiscover.litwareinc.com/autodiscover/metadata/json/1
```

In Lync Server, partner applications are configured by using the New-CsPartnerApplication cmdlet. In addition to specifying the metadata URI you should also set the application trust level to Full; this will allow Exchange to represent both itself and any authorized user in the realm. For example:

```
New-CsPartnerApplication -Identity Exchange -ApplicationTrustLevel Full -Metadata
```

Alternatively, you can create a partner application by copying and modifying the script code found in the Lync Server 2013 server-to-server authentication documentation. See the article Managing Server-to-Server Authentication (Oauth) and Partner Applications for more information.

If you have successfully configured partner applications for both Lync Server and Exchange that means that you have also successfully configured server-to-server authentication between the two products. Lync Server 2013 includes a Windows PowerShell cmdlet, Test-CsExStorageConnectivity, that enables you to verify that server-to-server authentication has been correctly configured and that the Lync Server Storage Service can connect to Exchange 2013. The cmdlet does this by connecting to the mailbox of an Exchange 2013 user, writing an item into the Conversation History folder for that user, and then, optionally, deleting that item.

To test the integration of Lync Server 2013 and Exchange 2013, run a command similar to this from within the Lync Server Management Shell:

```
Test-CsExStorageConnectivity -SipUri "sip:kenmyer@litwareinc.com"
```

In the preceding command, the SipUri represents the SIP address of a user with an account on Exchange 2013; your command will fail in this is not a valid user account.

If the test succeeds and connectivity has been established, you can then proceed to configure optional features such as archiving integration and the unified contact store.

Configuring Microsoft Lync Server 2013 to Use Microsoft Exchange Server 2013 Archiving

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2012-10-04*

Microsoft Lync Server 2013 gives administrators the option of having instant messaging and Web conferencing transcripts archived to a user's Microsoft Exchange Server 2013 mailbox rather than a SQL Server database. If you enable this option, transcripts are written to the Purges folder in the user's mailbox. The Purges folder is a hidden folder found in the Recoverable Items folder. Although this folder is not visible to end-users, the folder is indexed by the Exchange search engine and can be discovered by using Exchange mailbox search and/or Microsoft SharePoint Server 2013. Because information is stored in the same folder used by the Exchange In-Place Hold feature (responsible for archiving email and other Exchange communications), administrators can use a single tool to search for all the electronic communications archived for a user.

In order to archive transcripts to Exchange 2013 you must begin by configuring server-to-server authentication between the two servers. After server-to-server authentication is in place you can then carry out the following tasks in Microsoft Lync Server 2013 (note that, depending on your setup and configuration, you might not need to complete all of these tasks):

1. Enable Exchange archiving by modifying your Lync Server archiving configuration settings. This step is required for all deployments.
2. Enable archiving for internal and/or external communications for your users. This step is required for all deployments.
3. Configure the ExchangeArchivingPolicy property for each user. This step is only required in Lync Server and Exchange are located in different forests.

Step 1: Enabling Exchange Archiving

Archiving in Lync Server is primarily managed by using the archiving configuration settings. When you install Lync Server 2013 you are automatically given a single, global collection of these settings. (Administrators can optionally create new collections of archiving settings at the site scope.) By default, archiving is not enabled in the global settings, nor is Exchange archiving enabled in these settings. In order to use Exchange archiving administrators must configure both the EnableArchiving and the EnableExchangeArchiving properties in these configuration settings. The EnableArchiving property can be set to one of three possible values:

- **None**. Archiving is disabled. This is the default value. If EnableArchiving is set to None then nothing will be archived in either your Lync Server archiving database or in Exchange 2013.
- **ImOnly**. Only instant message transcripts are archived. If Exchange archiving is enabled these transcripts will be archived in Exchange 2013. If Exchange archiving is disabled then these transcripts will be archived to Lync Server.
- **ImAndWebConf**. Both instant message transcripts and Web conferencing transcripts are archived. If Exchange archiving is enabled these transcripts will be archived in Exchange 2013. If Exchange archiving is disabled then these transcripts will be archived to Lync Server.

The EnableExchangeArchiving property is a Boolean value: set EnableExchangeArchiving to True ($True) to enable Exchange archiving or set EnableExchangeArchiving to False ($False) to disable Exchange archiving. For example, this command enables the archiving of instant messaging transcripts and also enables Exchange archiving:

```
Set-CsArchivingConfiguration -Identity "global" -EnableArchiving ImOnly -EnableEx
```

To disable Exchange archiving, use a command similar to the following, which enables instant messaging archiving but disables archiving to Exchange (in other words, transcripts will be archived to Lync Server):

```
Set-CsArchivingConfiguration -Identity "global" -EnableArchiving ImOnly -EnableEx
```

Note:

If the EnableArchiving property is set to None then Lync Server will not archive instant messaging and Web conferencing transcripts at all. In that case, the server will simply ignore the value configured for EnableExchangeArchiving.

Exchange archiving can also be enabled (or disabled) by using the Lync Server Control Panel. To do that, complete the following procedure:

1. In Control Panel, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
2. On the **Archiving Configuration** tab, double-click the collection of archiving settings to be modified (for example, the **Global** collection).
3. In the **Edit Archiving Setting** pane, click the **Archiving setting** dropdown list and select either **Archive IM sessions** (to archive just instant messaging sessions) or **Archive IM and web conferencing sessions** (to archive both instant messaging and Web conferencing sessions).
4. After choosing the items to be archived, select the **Exchange Server integration** checkbox to enable Exchange archiving. To disable Exchange archiving, clear this checkbox.

Note:

The **Exchange Server integration** checkbox will not be available if the **Archiving setting** is set to **Disable archiving**. You must enable archiving first and then enable Exchange archiving.

If Lync Server 2013 and Exchange 2013 are located in the same forest then archiving for individual users (or at least for users who have email accounts on Exchange 2013) is managed by using Exchange In-Place Hold policies. If you have users who are homed on a previous version of Exchange then archiving for those users will be managed by using Lync Server archiving policies. Note that only users with accounts on Exchange 2013 can have their Lync transcripts archived to Exchange.

If Lync Server 2013 and Exchange 2013 are located in different forests then archiving for individual users is managed by configuring the ExchangeArchivingPolicy property for each individual user account. See Step 3 for more information.

Step 2: Enabling the Archiving of Internal and/or External Communications

After you have enabled archiving (and Exchange archiving) you must then modify the appropriate archiving policies to ensure that user sessions are actually archived. Note that simply enabling archiving (Step 1) does not cause Lync Server to begin archiving instant messaging and Web conferencing transcripts. Instead, you must use archiving policies to enable internal and/or external archiving. When you install Lync Server 2013 you also install a single, global archiving policy that contains two properties:

- **ArchiveInternal**. When set to True ($True) indicates that internal communication sessions involving only users who have Active Directory accounts in your organization) will be archived.
- **ArchiveExternal**. When set to True ($True) indicates that internal

communication sessions (sessions involving at least one user who does not have an Active Directory account in your organization) will be archived.

By default, both of these property values are set to False, meaning that neither internal nor external communication sessions are archived. To modify the global policy, you can use the Lync Server Management Shell and the Set-CsArchivingPolicy cmdlet. This command enables the archiving of both internal and external communication sessions:

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $True -ArchiveExternal
```

Alternatively, you can use the New-CsArchivingPolicy to create a new policy at either the site scope or the per-user scope. For example, this command creates a new per-user archiving policy named RedmondArchivingPolicy:

```
New-CsArchivingPolicy -Identity "RedmondArchivingPolicy" -ArchiveInternal $True -
```

If you create a per-user policy you will then need to assign that policy to the appropriate users. For example:

```
Grant-CsArchivingPolicy -Identity "Ken Myer" -PolicyName  "RedmondArchivingPolicy
```

Archiving policies can also be managed by using the Lync Server Control Panel. Within the Control Panel, click **Monitoring and Archiving** and then click **Archiving Policy**. To modify an existing policy, double-click the policy (e.g., Global) and then, in the **Edit Archiving Policy** pane, select or clear the **Archive internal communications** and the **Archive external communications** checkboxes as needed. To create a new archiving policy, click **New** and then select either **Site policy** or **User policy**. If you create a new user policy then you must access the appropriate user accounts (from the **Users** tab) and assign those users the new policy.

Step 3: Configuring the ExchangeArchivingPolicy Property

If Lync Server 2013 and Exchange 2013 are located in different forests then it is not enough to simply enable Exchange archiving in the archiving configuration settings; that will not result in instant messaging and Web conferencing transcripts being archived in Exchange. Instead, you must also configure the ExchangeArchivingPolicy property on each of the relevant Lync Server user accounts. This property can be set to one of four possible values:

1. Uninitialized. Indicates that archiving will be based on the In-Place Hold settings configured for the user's Exchange mailbox; if In-Place Hold has not been enabled on the user's mailbox then the user will have his or her messaging and Web conferencing transcripts archived in Lync Server.
2. **UseLyncArchivingPolicy**. Indicates that the user's instant messaging and Web conferencing transcripts should be archived in Lync Server rather than in Exchange.
3. **NoArchiving**. Indicates that the user's instant messaging and Web conferencing transcripts should not be archived at all. Note that this setting overrides any Lync Server archiving policies assigned to the user.
4. **ArchivingToExchange**. Indicates that the user's instant messaging and Web conferencing transcripts should be archived to Exchange regardless of the In-Place Hold settings that have (or have not) been assigned to the user's mailbox.

For example, to configure a user account so that instant messaging and Web conferencing transcripts are always archived to Exchange you can use a command similar to this from the Lync Server Management Shell:

```
Set-CsUser -Identity "Ken Myer" -ExchangeArchivingPolicy ArchivingToExchange
```

If you want to set the same archiving policy for a group of users (for example, all the users homed on a specified Registrar pool) you can use a command similar to this:

```
Get-CsUser -Filter {RegistrarPool -eq "atl-cs-001.litwareinc.com"} | Set-CsUser -
```

Note that you must use the Lync Server Management Shell (and Windows PowerShell) in order to configure value of the ExchangeArchivingPolicy property. This property is not exposed to administrators in the Lync Server Control Panel.

If you would like to view a list of all the users who have been assigned a specific archiving policy then you can use a command similar to the following, which returns the Active Directory display name of all the users who have had the ExchangeArchivingPolicy property set to Uninitialized:

```
Get-CsUser | Where-Object {$_.ExchangeArchivingPolicy -eq "Uninitialized"} | Sele
```

Likewise, this command returns the display name of the users who have not have the ExchangeArchivingPolicy property set to UseLyncArchivingPolicy:

```
Get-CsUser | Where-Object {$_.ExchangeArchivingPolicy -ne "UseLyncArchivingPolicy
```

1.3.14.1.4 Configuring Microsoft SharePoint Server 2013 to Search for Archived Microsoft Lync Server 2013 Data

Configuring Microsoft SharePoint Server 2013 to Search for Archived Microsoft Lync Server 2013 Data

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2013-02-04*

One of the major advantages to storing instant messaging and Web conferencing transcripts in Microsoft Exchange Server 2013 instead of Microsoft Lync Server 2013 is the fact that storing data in the same location enables administrators to use a single tool to search for archived Exchange data and/or archived Lync Server data. Because all the data is stored in the same place (Exchange) any tool that can search for archived Exchange data can also search for archived Lync Server data.

One tool that makes it easy to search for archived data is Microsoft SharePoint Server 2013. If you would like to use SharePoint to search for Lync Server data, you must first complete all the steps involved in configuring Exchange archiving in Lync Server. After Exchange 2013 and Lync Server 2013 have been successfully integrated you must then install the Exchange Web Services Managed API Version 2.0 on your SharePoint Server; the setup program for that API can be downloaded from the Microsoft Downloads Center (http://go.microsoft.com/fwlink/p/?LinkId=258305). The downloaded file (EWSManagedAPI.msi) can be saved to any folder on your SharePoint server.

After the file has been downloaded complete the following procedure on the SharePoint server:

1. Open a command window by clicking **Start**, clicking **All Programs**, clicking **Accessories**, right-clicking **Command Prompt**, and then clicking **Run as administrator**.
2. In the command window, use the **cd** command to change the current directory to the folder where the file EWSManagedAPI.msi has been saved. For example, if you have saved the file to C:\Downloads type the following command in the command window and then press ENTER:

```
cd C:\Downloads
```

3. To install the API, type the following command then press ENTER:

```
msiexec /I EwsManagedApi.msi addlocal="ExchangeWebServicesApi_Feature,
```

4. After the API has been installed, reset IIS by typing the following command and pressing ENTER:

```
iisreset
```

After Exchange Web Services has been installed you must then configure server-to-server authentication between SharePoint Server 2013 and Exchange 2013. To do this, first open the SharePoint 2013 Management Shell and run the following set of command:

```
New-SPTrustedSecurityTokenIssuer -Name "Exchange" -MetadataEndPoint "https://auto
$service = Get-SPSecurityTokenServiceConfig
$service.HybridStsSelectionEnabled = $True
$service.AllowMetadataOverHttp = $False
$service.AllowOAuthOverHttp = $False
$service.Update()
```

Note:

Be sure and use the URI for your autodiscover service. Do not use the sample URI https://autodiscover.litwareinc.com/autodiscover/metadata/json/1.

After you have created the token issuer and configured the token service, run these commands, making sure to substitute the URL of your SharePoint site for the sample URL http://atl-sharepoint-001:

```
$exchange = Get-SPTrustedSecurityTokenIssuer "Exchange"
$app = Get-SPAppPrincipal -Site "https://atl-sharepoint-001" -NameIdentifier $exc
$site = Get-SPSite  "https://atl-sharepoint-001"
Set-SPAppPrincipalPermission -AppPrincipal $app -Site $site.RootWeb -Scope "SiteS
```

To configure server-to-server authentication for Exchange 2013, open the Exchange Management Shell and run a command similar to this (assuming that Exchange has been installed on drive C: and that it uses the default folder path):

```
"C:\Program Files\Microsoft\Exchange Server\V15\Scripts\Configure-EnterprisePartn
```

After configuring the partner application it is recommended that you stop and restart Internet Information Services (IIS) on all your Exchange mailbox and client access servers. You can restart IIS by using a command similar to this, which restarts the service on the computer atl-exchange-001:

```
iisreset atl-exchange-001
```

This command can be run from within the Exchange Management Shell or from any other command window.

Next, run a command similar to the following, which gives the specified user (in this example, kenmyer) the right to do discovery on Exchange:

```
Add-RoleGroupMember "Discovery Management" -Member "kenmyer"
```

After server-to-server authentication has been established between Exchange and SharePoint your next step is to create an eDiscovery site in SharePoint. That can be done by running commands similar to these from the SharePoint Management Shell:

```
$template = Get-SPWebTemplate | Where-Object {$_.Title -eq "eDiscovery Center"}
New-SPSite -Url "https://atl-sharepoint-001/sites/discovery" -OwnerAlias "kenmyer
```

Note:

"eDiscovery" is short for "electronic discovery," and typically refers to the process of looking through electronic archives for items that can be "reasonably calculated to lead to admissible evidence" in a court of law.

When the new site is ready, the next step is to configure Exchange 2013 to act as a result source for SharePoint. You can do that by completing the following procedure from the SharePoint 2013 Central Administration page:

1. On the Central Administration page click **Manage Service Applications** and then click **Search Service Application**.
2. On the Search Service Application: Search Administration page click **Result Sources** and then click **New Result Source**.
3. In the **New Result Source** pane enter a name for the new result source (for example, **Microsoft Exchange**) in the **Name** box. Select **Exchange** as the result source **Protocol**, and then enter the web services source URL for your Exchange server in the **Exchange Source URL** box. The source URL should look similar to this:
   https://atl-exchange-001.litwareinc.com/ews/exchange.asmx
4. Make sure that **Use Autodiscover** is not selected, and then click **OK**.

Finally, create a new eDiscovery case and a new eDiscovery set by completing the following procedure from the SharePoint Discovery site (for example, https://atl-sharepoint-001/sites/discovery):

1. On the Site Contents page click **Create a new case**.
2. On the Site Contents: New SharePoint Site page, enter the user's email alias (for example, **kenmyer**) in the **Title** box, then add that same URL to the **Web Site Address** box. That will result in a URL similar to this:
   https://atl-sharepoint-001/sites/eDiscovery/kenmyer
3. Click **Create**.
4. When the eDiscovery set page appears, click **new item** under **Identity and Preserve: Discovery Sets**.
5. On the New: Discovery Set page, enter the user's email alias in the **Discovery Set Name** box. Enter **eDiscovery Lync*** in the **Filter** box and then click **Add & Manage Sources**.
6. On the Add & Manage Sources page, enter the user's email alias in the first textbox under **Mailboxes**. Click the check mailbox icon located next to the textbook to verify that SharePoint can connect to the specified mailbox.
7. Click **OK**.
8. On the eDiscovery set page, click **Save** to save the new eDiscovery set.

At this point you can search the specified mailbox (kenmyer) and/or enable In-Place holds the same way you would for any other SharePoint content or result source.

1.3.14.1.5 Configuring Microsoft Lync Server 2013 to Use the Unified Contact Store

Configuring Microsoft Lync Server 2013 to Use the Unified Contact Store

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2013-01-16*

The unified contact store enables users to maintain a single contacts list and then have those contacts available in multiple applications, including Microsoft Lync 2013, Microsoft Outlook 2013, and Microsoft Outlook Web App 2013. When you enable the unified contact store for a user that user's contacts are not stored in Microsoft Lync Server 2013 and then retrieved using the SIP protocol. Instead, his or her contacts are stored in Microsoft Exchange Server 2013 and are retrieved by using Exchange Web Services.

Note:

Technically, contact information is stored in a pair of folders found in the user's Exchange 2013 mailbox. The contacts themselves are stored in a folder named Lync Contacts which is visible to end users; metadata about the contacts are stored in a subfolder that is not visible to end users.

Enabling the Unified Contact Store for a User

If you have already configured server-to-server authentication between Lync Server 2013 and Exchange 2013 then you have also enabled the use of the unified contact store; no additional server configuration is required. However, additional user account configuration is required in order to move a user's contacts into the unified contact store. By default, user contacts are kept in Lync Server and not in the unified contact store.

Access to the unified contact store is managed by using Lync Server user services policies. User server policies have only a single property (UcsAllowed); this property is used to determine the location where a user's contacts are stored. If a user is managed by a user services policy where UcsAllowed has been set to True ($True) then the user's contacts will be stored in in the unified contact store. If the user is managed by a user services policy where UcsAllowed has been set to False ($False) then his or her contacts will be stored in Lync Server.

When you install Lync Server 2013 a single user services policy (configured at the global scope) is installed as well. The UcsAllowed value in this policy is set to True, meaning that, by default, user contacts will be stored in the unified contact store (assuming this has been deployed and configured). If you want to migrate all of your user contacts to the unified contact store you do not have to do anything at all.

If you would prefer not to migrate all your contacts to the unified contact store you can disable the unified contact store for all users by setting the UcsAllowed property in the global policy to False:

```
Set-CsUserServicesPolicy -Identity global -UcsAllowed $False
```

After you have disabled the unified contact store in the global policy you can then create a per-user policy that enables the use of the unified contact store; this allows you to have some users keep their contacts in the unified contact store while other users continue to keep their contacts in Lync Server. You can create a per-user user services policy by using a command similar to this:

```
New-CsUserServicesPolicy -Identity "AllowUnifiedContactStore" -UcsAllowed $True
```

After you have created the new policy you must then assign that policy to any user who should have access to the unified contact store. Per-user policies can be assigned to users by using commands similar to this:

```
Grant-CsUserServicesPolicy -Identity "Ken Myer" -PolicyName "AllowUnifiedContactS
```

After the policy has been assigned Lync Server will begin to migrate the user's contacts to the unified contact store. After migration is complete, the user will then have his or her contacts stored in Exchange rather than Lync Server. If the user happens to be logged on to Lync 2013 at the time migration completes, a message box will appear and he or she will be asked to log off of Lync and then log back on in order to finalize the process. Users who have not been assigned this per-user policy will not have their contacts migrated to the unified contact store. That’s because those users are being managed by the global policy, and use of the unified contact store has been disabled in the global policy.

You can verify that a user's contacts have successfully been migrated to the unified contact store by running the Test-CsUnifiedContactStore cmdlet from within the Lync Server Management Shell:

```
Test-CsUnifiedContactStore -UserSipAddress "sip:kenmyer@litwareinc.com" -TargetFq
```

If Test-CsUnifiedContactStore succeeds that means that the contacts for the user sip:kenmyer@litwareinc.com have been migrated to the unified contact store.

Rolling Back the Unified Contact Store

If you need to remove a user's contacts from the unified contact store (for example, if the user needs to be rehomed on Microsoft Lync Server 2010 and thus can no longer use the unified contact store) you must do two things. First, you must assign the user a new user services policy, one that prohibits storing contacts in the unified contact store. (That is, a policy where the UcsAllowed property has been set to $False.) If you do not have such a policy you can create one using a command similar to this:

```
New-CsUserServicesPolicy -Identity NoUnifiedContactStore -UcsAllowed $False
```

You can then assign this new per-user policy (NoUnifiedContactStore) by using a command like this:

```
Grant-CsUserServicesPolicy -Identity "Ken Myer" -PolicyName NoUnifiedContactStore
```

The preceding command assigns the new policy to the user Ken Myer, and also prevents Ken's contacts from being migrated to the unified contact store.

Note:

In some cases you can achieve the same net effect by simply unassigning the user's current user services policy. For example, suppose Ken Myer has a per-user user services policy the enables the unified contact store, but your global policy prohibits the use of the unified contact store. In that case, you could unassign Ken's per-user services policy. When you do that, Ken will automatically be managed by the global policy, and thus will no longer have access to the unified contact store.
To unassign a previously-assigned per-user policy, use the same command as shown before, but this time set the PolicyName parameter to a null value:
Grant-CsUserServicesPolicy –Identity "Ken Myer" –PolicyName $Null

The terminology "prevents Ken's contacts from being migrated to the unified contact store" is important to keep in mind when working with the unified contact store. Simply assigning Ken a new user services policy will not move his contacts out of the unified contact store. When a user logs on to Lync Server 2013, the system checks the user's user services policy to see whether his or her contacts should be kept in the unified contact store. If the answer is yes (that is, if the UcsAllowed property is set to $True) then those contacts will be migrated to the unified contact store (assuming that those contacts are not already in the unified contact store). If the answer is no, then Lync Server simply ignores the user's contacts and moves on to its next task. That means that Lync Server will not automatically move a user's contacts from out of the unified contact store, regardless of the value of the UcsAllowed property.

That also means that, after assigning the user a new user services policy, you must then run the Invoke-CsUcsRollback cmdlet in order to move the user's contacts out of Exchange 2013 and back to Lync Server 2013. For example, after assigning Ken Myer a new user services policy you can then move his contacts out of the unified contact store by using the following command:

```
Invoke-CsUcsRollback -Identity "Ken Myer"
```

If you change the user services policy but do not run the Invoke-CsUcsRollback cmdlet

Ken's contacts will not be removed from the unified contact store. What if you run Invoke-CsUcsRollback but do not change Ken Myer's user services policy? In that case, Ken's contacts will be temporarily removed from the unified contact store. The fact that this removal is temporary is important to keep in mind. After Ken's contacts have been removed from the unified contact store, Lync Server 2013 will wait 7 days and then check to see which user services policy has been assigned to Ken. If Ken is still assigned a policy that enables the user of the unified contact store, then his contacts will automatically be moved back to into the contact store. To permanently remove contacts from the unified contact store you must change the user services policy in addition to running the Invoke-CsUcsRollback cmdlet.

1.3.14.1.6 Configuring the Use of High-Resolution Photos in Microsoft Lync Server 2013

Configuring the Use of High-Resolution Photos in Microsoft Lync Server 2013

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2012-10-22*

Microsoft Lync Server 2010 provided the ability for users to view photos of their contacts (and to make their own photos available to others). Typically these photos were stored as part of the user's thumbnailPhoto attribute in Active Directory. That placed a serious limitation on the size and resolution of the photos: the thumbnailPhoto attribute can only hold a photograph with a maximum size of 48 pixels by 48 pixels.

In Microsoft Lync Server 2013, however, photos can be stored in a user's Microsoft Exchange Server 2013 mailbox; that allows for photo sizes up to 648 pixels by 648 pixels. In addition to that, Exchange 2013 can automatically resize these photos for use in different products as needed. Typically that means three different photo sizes and resolutions:

- 48 pixels by 48 pixels, the size used for the Active Directory thumbnailPhoto attribute. If you upload a photo to Exchange 2013 Exchange will automatically create a 48 pixel by 48 pixel version of that photo and update the user's thumbnailPhoto attribute. Note, however, that the reverse is not true: if you manually update the thumbnailPhoto attribute in Active Directory the photo in the user's Exchange 2013 mailbox will not automatically be updated.
- 96 pixels by 96 pixels, for use in Microsoft Outlook 2013 Web App, Microsoft Outlook 2013, Microsoft Lync Web App, and Lync 2013.
- 648 pixels by 648 pixels for use in Lync 2013 and Microsoft Lync Web App.

Note:

If you have the resources, it is recommended that you upload 648x648 photos; that provides the maximum resolution and optimal picture quality in any of the Office 2013 applications. Each JPEG photo with a size of 648x648 and a depth of 24 bits results in a file size of approximately 240 kilobytes. That means you will need approximately 1 megabyte of disk space for every 4 user photos.

High-resolution photos, which are accessed by using Exchange Web Services, can be uploaded by users who are running Outlook 2013 Web App; users are only allowed to update their own photo. Administrators, however, can update the photo for any user by using the Exchange Management Shell and a series of Windows PowerShell commands similar to the following:

```
$photo = ([Byte]] $(Get-Content -Path "C:\Photos\Kenmyer.jpg" -Encoding Byte -Rea
Set-UserPhoto -Identity "Ken Myer" -PictureData $photo -Confirm:False
```

```
Set-UserPhoto -Identity "Ken Myer" -Save -Confirm:False
```

The first command in the preceding example uses the Get-Content cmdlet to read the contents of the file C:\Photos\Kenmyer.jpg and store that data in a variable named $photo. In the second command, the Exchange cmdlet Set-UserPhoto is used to upload the photo and attach that photo to Ken Myer's user account.

Note:

In this example, Ken Myer's Active Directory display name is used as the user account Identity. You can also reference a user account by using other identifiers such as the user's SMTP address or his or her User Principal Name. See the documentation for the Set-UserPhoto cmdlet at http://go.microsoft.com/fwlink/p/?LinkId=268536 for more information

Uploading the photo does not equate to assigning that photo to Ken Myer's user account. Instead, uploading the photo simply results in a preview of that photo to be displayed on the Outlook Web App Options page. To actually assign that photo to the user account the user must click **Save** on the Options page or the administrator must execute the third command in the example. That third command uses the Save parameter to assign the photo to Ken Myer's user account:

```
Set-UserPhoto -Identity "Ken Myer" -Save -Confirm:False
```

To verify that the new photo has been assigned to the user account, Ken Myer can log on to Lync 2013, select **Options**, and then select **My Picture**. The newly-uploaded photo should be displayed as Ken's personal photo. Alternatively, administrators can verify the photo for any user by starting Internet Explorer and navigating to a URL similar to this:

```
https://atl-mail-001.litwareinc.com/ews/Exchange.asmx/s/GetUserPhoto?email=kenmye
```

If the administrator can view the photo using Internet Explorer but the user cannot view his or her photo in Lync 2013, that typically indicates a connectivity problem with Exchange Web Services or with the Exchange autodiscover service.

1.3.14.1.7 Configuring Microsoft Exchange Server 2013 Unified Messaging for Microsoft Lync Server 2013 Voicemail

Configuring Microsoft Exchange Server 2013 Unified Messaging for Microsoft Lync Server 2013 Voicemail

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2013-02-04*

Microsoft Lync Server 2013 enables you to have voicemail messages stored in Microsoft Exchange Server 2013; those voicemail messages will then appear as email messages in your users' Inboxes. This capability was also found in the 2010 editions of Lync Server and Exchange; however, the process of configuring this "unified messaging" has been simplified in in the 2013 editions thanks to the introduction of the UM Call Router component. This component is installed on the Exchange 2013 Client Access server, and all calls to Exchange unified messaging (such as a voicemail) are first routed through the Call Router and then are redirected to the appropriate Mailbox server.

If you have already configured server-to-server authentication between Lync Server 2013 and Exchange 2013 then you are ready to setup unified messaging. To do so, you must first create and assign a new unified messaging dial plan on your Exchange server. For example, these two commands (run from within the Exchange Management Shell) configure a new 3-digit dial plan for Exchange:

```
New-UMDialPlan -Name "RedmondDialPlan" -VoIPSecurity "Secured" -NumberOfDigitsInE
Set-UMDialPlan "RedmondDialPlan" -ConfiguredInCountryOrRegionGroups "Anywhere,*,*
```

In the first command in the example, the VoIPSecurity parameter, and the parameter value "Secured" indicate that the signaling channel is encrypted by using Transport Layer Security (TLS). The URIType "SipName" indicates that messages will be sent and received using the SIP protocol, and the CountryOrRegionCode of 1 indicates that the dial plan applies to the US.

In the second command, the parameter value passed to the ConfiguredInCountryOrRegionGroups parameter specifies the in-country groups that can be used with this dial plan. The parameter value "Anywhere,*,*,*" sets the following:

- Group name ("Anywhere")
- AllowedNumberString (*, a wildcard character indicating that any number string is allowed)
- DialNumberString (*, a wildcard character indicating that any dialed number is allowed)
- TextComment (*, a wildcard character indicating that any text command is allowed)

Note:

Creating a new dial plan will also create a Default Mailbox Policy.

After creating and configuring the new dial plan you must add the new dial plan to your unified messaging server and then modify the startup mode of that server; in particular, you must set the startup mode to "Dual". You can perform both of these tasks from within the Exchange Management Shell:

```
Set-UmService -Identity "atl-exchangeum-001.litwareinc.com" -DialPlans "RedmondDi
```

After the unified messaging server has been configured you should next run the Enable-ExchangeCertificate cmdlet to ensure that your Exchange certificate is applied to the unified messaging service:

```
Enable-ExchangeCertificate -Server "atl-umserver-001.litwareinc.com" -Thumbprint
```

After the certificate has been correctly assigned you must then stop and restart the MsExchangeUM service on the unified messaging server. This service must be stopped and restarted any time you change the startup mode.

After finishing configuration of the unified messaging server you can then configure the UM Call Router:

```
Set-UMCallRouterSettings -Server "atl-exchange-001.litwareinc.com" -UMStartupMode
Enable-ExchangeCertificate -Server "atl-umserver-001.litwareinc.com" -Thumbprint
```

Because the startup mode has changed you must stop and restart the MsExchangeUMCR service on the computer hosting the UM Call Router.

To complete the unified messaging setup, you then need to create a UM mailbox policy and then use that policy to enable users for unified messaging. You can create a mailbox policy by using a command similar to this:

```
New-UMMailboxPolicy -Name "RedmondMailboxPolicy" -AllowedInCountryOrRegionGroups
```

And you can enable a user for unified messaging by using a command similar to this:

```
Enable-UMMailbox -Extensions 100 -SIPResourceIdentifier "kenmyer@litwareinc.com"
```

In the preceding command, the Extensions parameter represents the telephone extension number for the user. In this example, the user has the extension number 100.

After you have enabled his mailbox, the user kenmyer@litwareinc.com should be able to use Exchange unified messaging. You can verify that the user can connect to Exchange UM by running the Test-CsExUMConnectivity cmdlet from within the Lync Server Management Shell:

```
$credential = Get-Credential "litwareinc\kenmyer"
Test-CsExUMConnectivity -TargetFqdn "atl-cs-001.litwareinc.com" -UserSipAddress "
```

If you have a second user who has been enabled for unified messaging you can use the Test-CsExUMVoiceMail cmdlet to verify that this second user can leave a voicemail message for the first user.

```
$credential = Get-Credential "litwareinc\pilar"
Test-CsExUMVoiceMail -TargetFqdn "atl-cs-001.litwareinc.com" -ReceiverSipAddress
```

1.3.14.1.8 Integrating Microsoft Lync Server 2013 and Microsoft Outlook Web App 2013

Integrating Microsoft Lync Server 2013 and Microsoft Outlook Web App 2013

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2013-02-03*

In addition to integrating with Microsoft Outlook 2013, Microsoft Lync Server 2013 can be fully integrated with Microsoft Outlook Web App 2013; among other things, this adds instant messaging and presence to Outlook Web App, and enables your unified contact list to be shared between Outlook Web App and Microsoft Lync 2013. In order to integrate Lync Server 2013 and Outlook Web App, you must first verify that the Unified Communications Managed API 4.0 Runtime has been installed in your Microsoft Exchange Server 2013 backend server. You can do this by looking for the existence of the following registry value:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA \InstantMessaging\ImplementationDLLPath

The ImplementationDLLPath should point to the folder location for the file Microsoft.Rtc.Internal.Ucweb.dll. If it does not, or if the registry value does not exist, then you should download and install the UCMA Runtime setup program from the Microsoft Download Center at http://www.microsoft.com/en-us/download/details.aspx?id=34992. Information on how to install the UCMA Runtime can be found on that same web page.

Backward Compatibility

Lync Server 2013 can be integrated with the Microsoft Exchange Server 2010 versions of both unified messaging and Outlook Web App. For more information, see the article Deploying On-Premises Exchange UM to Provide Lync Server 2010 Voice Mail at http://technet.microsoft.com/en-us/library/gg398768.aspx. If you integrate with Exchange 2010 you will not have Lync Server specific features such as the unified contact store and Lync-to-Exchange archiving.

Microsoft Lync 2013 can also be used in conjunction with Exchange 2010 and Outlook 2010. Once again, however, new functionality such as the unified contact store and high-resolution photos will not be available to Lync 2013 users. These new capabilities require both Lync Server 2013 and Exchange 2013.

Creating a Trusted Application Pool for Outlook Web App

If you have installed the Microsoft Exchange Unified Messaging Call Router service and the Microsoft Exchange Unified Messaging service on the same computer then there is no need to create a trusted application pool for Outlook Web App. (This assumes that the server in question is hosting a SipName UM dial plan.) If you are using a single computer to host both of these services then you can skip to the section of this document titled **Enabling Instant Messaging on Outlook Web App**.

Lync Server 2013 can autodiscover any Exchange servers that host a SipName UM dial plan; these servers are automatically added to the Lync Server Known Servers List. There is no need to create a trusted application pool and add these servers to the Known Servers List. In fact, doing so will cause Outlook Web App integration to stop working.

Note:

This is due to the fact that the Lync Server topology will now have two entries for the same computer: the autodiscovered entry, and the manually-added entry. To fix the problem, and to get Outlook Web App working again, use Windows PowerShell to remove the trusted pool and trusted application entries for the server. See the help topics for the Remove-CsTrustedApplicationPool and Remove-CsTrustedApplication cmdlets for more information.

If these two services are running on separate computers then, after you have verified that the Unified Communications Managed API 4.0 Runtime has been installed, you must create a Lync Server trusted application pool and a trusted application associated with Outlook Web App; that will add the server to the Known Servers List. To do that, first run a command similar to this from within the Lync Server Management Shell:

```
New-CsTrustedApplicationPool -Identity atl-owa-001.litwareinc.com -Registrar atl-
```

In the preceding command, atl-owa-001.litwareinc.com is the fully qualified domain name of the Outlook Web App pool; this must be the same name that appears in the Subject Name and Subject Alternative Name (SAN) fields of the certificate that provides access to Outlook Web App. Likewise, atl-cs-001.litwareinc.com is the fully qualified domain name of the Lync Server 2013 pool that will host the new trusted application pool. Note, too that the specified site, Redmond, represents the SiteID of the Lync Server site. The SiteID is not necessarily the same as the site's DisplayName; you can retrieve SiteIDs for your Lync Server sites by running the following command from the Lync Server Management Shell:

```
Get-CsSite | Select-Object DisplayName, SiteID
```

After creating the trusted application pool, use a command similar to the following to configure an application Identity and a port for Outlook Web App:

```
New-CsTrustedApplication -ApplicationId OutlookWebApp -TrustedApplicationPoolFqdn
```

In the preceding command, the ApplicationID is simply a friendly identifier used to distinguish trusted applications. The ApplicationID can be any text string that does not include blank spaces or other prohibited characters. (To ensure that you create a valid identifier, it is recommended that you use only letters and numbers when specifying an ApplicationId.) The value assigned to the Port parameter is also left to the administrator's discretion: this can be any available network port.

After creating the trusted application you must run the following command to enable the changes to your Lync Server topology:

```
Enable-CsTopology
```

Note that you must also add your Exchange client access and mailbox server to all of your SIP Uri dial plans. In turn, this will configure the servers as trusted SIP peers with the ExUmRouting topology for Lync Server.

Enabling Instant Messaging on Outlook Web App

With Lync Server correctly configured you can then begin to configure Outlook Web App. The first step in that process is to enable instant messaging on all your Outlook Web App virtual directories on your front end servers. (There is no need to enable instant messaging for the virtual directories on your backend servers. In fact, it is recommended that you do not enable instant messaging on your backend servers.) Instant messaging can be enabled on the client access servers by running the following command from within the Exchange Management Shell:

```
Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -InstantMessagingEnabled $True
```

Note:

By default, instant messaging is enabled when you install Outlook Web App; that is, the InstantMessagingEnabled property is set to True. However, you must still run the preceding command in order to set the instant messaging type to OCS. By default, InstantMessagingType is set to None.

Next you must add the following two lines to Outlook Web App Web.config file (this file is typically located in the folder C:\Program Files\Microsoft\Exchange Server\V15 \ClientAccess\Owa). These two lines should be added under the <AppSettings> node in the Web.config file, and this procedure should be carried out only on the backend servers where Outlook Web App has been installed:

```
<add key="IMCertificateThumbprint" value="EA5A332496CC05DA69B75B66111C0F78A110D22
<add key="IMServerName" value="atl-cs-001.litwareinc.com"/>
```

In the preceding example, the value for IMCertificateThumbprint must be the thumbprint for the Exchange 2013 certificate that is installed on your backend servers. You can retrieve that information by running the following command from the Exchange Management Shell:

```
Get-ExchangeCertificate
```

Note, too that the value assigned to IMServerName is the fully qualified domain name of the Lync Server pool where you created the trusted application pool for Outlook Web App.

The certificate that you use for Outlook Web App must be a certificate that is trusted by Lync Server. One way to ensure that the certificate will be trusted by both Lync Server and Exchange is to use your internal certificate authority to create a certificate on the mailbox server, making sure that the server FQDN is used for the subject name and that this FQDN appears in the certificate alternate name field. After the certificate has been created it can then be imported to your backend servers. The net result is that the same certificate is used for two purposes: 1) communication between Exchange unified messaging and Lync Server; and, 2) the integration between Outlook Web App and Lync Server.

After you have updated the Web.config file you should then run the following command on the Exchange backend server in order to recycle the Outlook Web App pool:

```
C:\Windows\System32\Inetsrv\Appcmd.exe recycle apppool /apppool.name:"MSExchangeO
```

If the recycle operation succeeds you will see the following message in the Exchange Management Shell:

```
"MSExchangeOWAAppPool" successfully recycled
```

Configuring Outlook Web App Mailbox Policies

At this point you can use the following command to configure instant messaging on the appropriate Outlook Web App mailbox policy (or policies). For example, this command, run on one of your mailbox servers, enables instant messaging on the Default policy:

```
Set-OwaMailboxPolicy -Identity "Default" -InstantMessagingEnabled $True -InstantM
```

And this command enables instant messaging for all your Outlook Web App mailbox policies:

```
Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -InstantMessagingEnabled $True -Insta
```

After the mailbox policy has been enabled then all users managed by that policy will have full integration between Lync Server and Outlook Web App, provided that:

- The user has a mailbox on Exchange 2013.
- The user has been enabled for Lync Server 2013.
- The user has a valid SIP proxy address.

Disabling Instant Messaging in Outlook Web App

As noted previously, instant messaging is enabled by default in Outlook Web App. That means that, if you do not integrate Outlook Web App with Lync Server, users will see blank presence icons and an error message each time they log on to Outlook Web App. To prevent this problem, use the following Exchange Management Shell command to disable instant messaging in Outlook web App:

```
Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -InstantMessagingEnabled $False
```

Verifying Integration With Outlook Web App

To verify that instant messaging and presence have been integrated with Outlook Web App, sign on to Outlook Web App 2013. In the upper right-hand corner of the screen, you will see your Exchange display name. If there is a presence icon next to your name (for example, a green icon indicating that your current status is Available) that indicates that you have successfully integrated Lync Server and Outlook Web App.

After the initial sign-on to Outlook Web App, check to see if an event with the Event ID 112 (and the source MSExchange OWA) has been written to the event log on the mailbox server. This event indicates that the Instant Messaging Endpoint Manager was successfully initialized. If instant messaging does not appear to be working then, on the mailbox server, look for log files in the folder C:\Program Files\Microsoft\Exchange server \V15\Logging\OWA\InstantMessaging. If either the Logging or the InstantMessaging folders do not exist that indicates that integration has failed. In that case, you can use SIPStack tracing on Lync Server (All Levels and All Flags) to try and determine why integration failed.

1.3.14.2 Planning for Exchange Unified Messaging Integration

Planning for Exchange Unified Messaging Integration

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-10-13*

Lync Server 2013 supports integration with Exchange Unified Messaging (UM) for combining voice messaging and email messaging into a single messaging infrastructure. In Microsoft Exchange Server 2007 Service Pack 1 (SP1) and Microsoft Exchange Server 2010, Exchange Unified Messaging (UM) is one of several Exchange server roles that you can install and configure.

In Microsoft Exchange Server 2013, Exchange UM runs as a service on an Exchange Mailbox server. For Lync Server 2013 Enterprise Voice deployments, Unified Messaging combines voice messaging and email messaging into a single store that is available from a telephone (Outlook Voice Access) or a computer. Unified Messaging and Lync Server 2013 work together to provide call answering, Outlook Voice Access, and auto-attendant services to users of Enterprise Voice.

For more information about the architecture changes in Microsoft Exchange Server 2013, see “Voice Architecture Changes” in the Microsoft Exchange Server 2013 documentation at http://go.microsoft.com/fwlink/p/?LinkId=266730.

For these features to be supported in an on-premises Exchange UM deployment, you must be running one of the following:

- Microsoft Exchange Server 2007 Service Pack 1 (SP1) or latest service pack
- Microsoft Exchange Server 2010 or latest service pack
- Microsoft Exchange Server 2013
- Features of Integrated Unified Messaging and Lync Server 2013
- Components and Topologies for On-Premises Unified Messaging
- Guidelines for Integrating On-Premises Unified Messaging and Lync Server 2013
- Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013

1.3.14.2.1 Features of Integrated Unified Messaging and Lync Server 2013

Features of Integrated Unified Messaging and Lync Server 2013

Planning > Planning for Enterprise Voice > Planning for Exchange Unified Messaging Integration >

Topic Last Modified: *2012-10-01*

Lync Server 2013, Enterprise Voice uses the Exchange Unified Messaging (UM) infrastructure to provide call answering, call notification, voice access (including voice mail), and auto-attendant services.

Call Answering

Call answering is the receiving of voice messages on behalf of users whose calls are not answered or are busy. It includes playing a personal greeting, recording a message, and submitting the message to be queued for delivery to the user's mailbox, which is stored on the Exchange mailbox server.

If a caller leaves a message, the message is routed to the user's Inbox. If a caller chooses not to leave a message, a missed call notification is stored in the user's mailbox. Users can then access their Inbox by using the Microsoft Outlook messaging and collaboration client, Outlook Web Access, the Exchange ActiveSync technology, or Outlook Voice Access. The subject and priority of calls can be displayed in a way similar to that of email.

Outlook Voice Access

Outlook Voice Access enables an Enterprise Voice user to access not just voice mail, but also the Exchange inbox, including email, calendar, and contacts from a telephony interface. The subscriber access number is assigned by an Exchange UM administrator.

Auto Attendant

Auto attendant is an Exchange UM feature that can be used to configure a phone number that outside users can dial to reach company representatives. In particular, it provides a series of voice prompts that assist an external caller in navigating a menu system. The list of available options is configured on the Exchange UM server by the Exchange UM administrator.

Fax Services

Exchange UM includes fax features, which enable users to receive incoming faxes in their Exchange mailboxes. For details, see "Unified Messaging" in the Microsoft Exchange Server documentation at http://go.microsoft.com/fwlink/p/?linkId=135652.

Note:

Fax services provided by the Exchange UM server are not available in Lync Server deployments that are integrated with Microsoft Exchange Server 2010, Exchange 2010 with the latest service pack, or Exchange 2013.

1.3.14.2.2 Components and Topologies for On-Premises Unified Messaging

Components and Topologies for On-Premises Unified Messaging

Server Software and Infrastructure Support > Voice Support > Exchange Unified Messaging (UM) Support >

Topic Last Modified: *2012-09-25*

This topic describes the Microsoft Exchange Server 2013 components required to provide Exchange Unified Messaging (UM) features to Lync Server 2013 deployment. It also describes the supported topologies for on-premises Exchange UM integration.

Exchange Server Components

To provide the Exchange UM features and services described in Features of Integrated Unified Messaging and Lync Server 2013 to Enterprise Voice users in your organization, you must deploy an Microsoft Exchange Mailbox server and Client Access server, which hosts user mailboxes and provides a single storage location for email and voice mail. Exchange UM runs as a service on Exchange Mailbox and Client Access servers.

For details about Exchange UM components in Microsoft Exchange Server 2007 and Microsoft Exchange Server 2010, see Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail in the Deployment documentation.

Supported Topologies

You can deploy Lync Server 2013 and Exchange Unified Messaging (UM) in the same forest or multiple forests. If the deployment spans multiple forests, you must perform the Exchange integration steps for each Exchange UM forest. Furthermore, you must configure each Microsoft Exchange forest to trust the Lync Server 2013 forest and the Lync Server 2013 forest to trust each Exchange UM forest. In addition to this forest trust, the Exchange UM settings for all users must be set on the user objects in the Lync Server 2013 forest.

Lync Server 2013 supports the following topologies for Exchange UM integration:

- Single forest
- Single domain (that is, a single forest with a single domain). Lync Server 2013, Microsoft Exchange, and users all reside in the same domain.
- Multiple domain (that is, a root domain with one or more child domains). Lync Server 2013, and Microsoft Exchange servers are deployed in different domains from the domain where you create users. Exchange UM servers can be deployed in different domains from the Lync Server 2013 pool they support.
- Multiple forest (that is, resource forest). Lync Server 2013 is deployed in a single forest, and then users are distributed across multiple forests. The users' Exchange UM attributes must be replicated over to the Lync Server 2013 forest.

  Note:
  Exchange can be deployed in multiple forests. Each Exchange organization can provide Exchange UM to its users, or Exchange UM can be deployed in the same forest as Lync Server 2013.

1.3.14.2.3 Guidelines for Integrating On-Premises Unified Messaging and Lync Server 2013

Guidelines for Integrating On-Premises Unified Messaging and Lync Server 2013

See Also

Planning > Planning for Enterprise Voice > Planning for Exchange Unified Messaging Integration >

***Topic Last Modified:** 2012-09-25*

The following are guidelines and best practices to consider when you deploy Enterprise Voice:

Important:
Exchange Unified Messaging (UM) supports IPv6 only if you are also using UCMA 4.

- Deploy a Lync Server 2013 Standard Edition server or a Front End pool. For details about installation, see Deploying Lync Server 2013 in the Deployment documentation.
- Work with Exchange administrators to confirm which tasks each of you will perform to assure a smooth and successful integration.
- Deploy the Exchange Mailbox server roles in each Exchange Unified Messaging (UM) forest where you want to enable users for Exchange UM. For details about installing Exchange server roles, see the Microsoft Exchange Server 2013 documentation.

  Important:
  When Exchange Unified Messaging (UM) is installed, it is configured to use a self-signed certificate.
  The self-signed certificate, however, does not enable Lync Server 2013 and Exchange UM to trust each other, which is why it is necessary to request a separate certificate from a certification authority that both servers trust.

- If Lync Server 2013 and Exchange UM are installed in different forests, configure each Exchange forest to trust the Lync Server 2013 forest and the Lync Server 2013 forest to trust each Exchange forest. Also, set the users' Exchange UM settings on the user objects in the Lync Server 2013 forest, typically by using a script or a cross-forest tool, such as Identity Lifecycle Manager (ILM).
- If necessary, install the Exchange Management Console to manage your Unified Messaging servers.
- Obtain valid phone numbers for Outlook Voice Access and auto attendant.

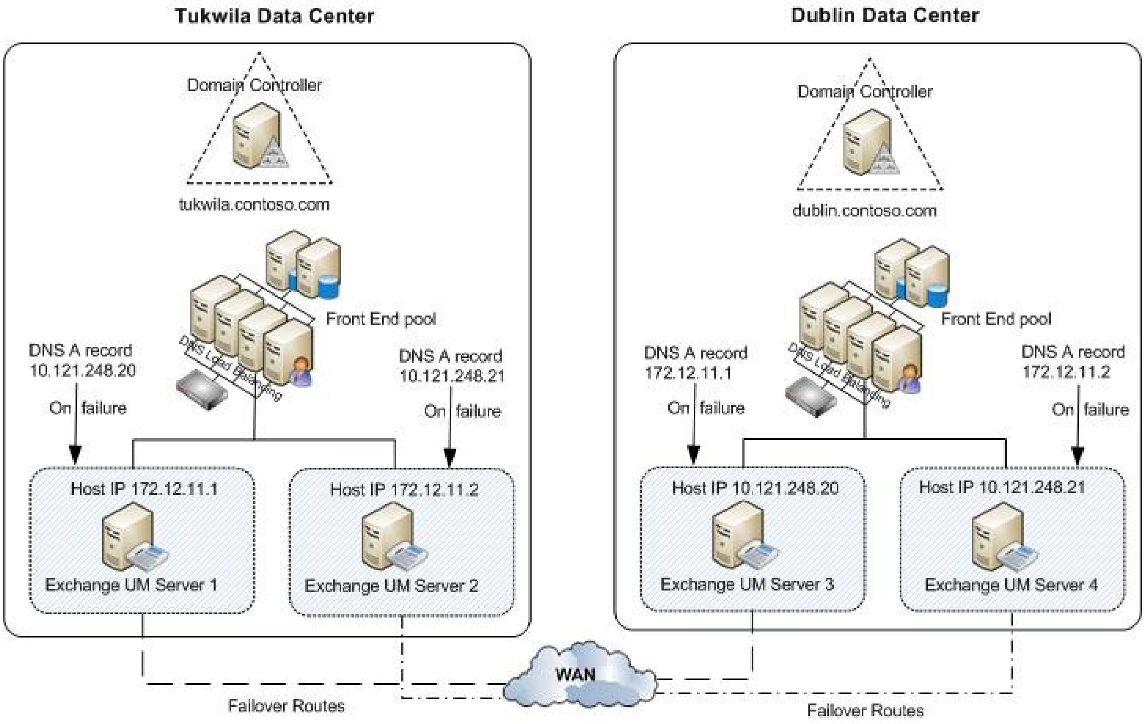
- If you are using a version of Exchange UM earlier than Microsoft Exchange Server 2010 Service Pack 1 (SP1), coordinate names for Exchange UM SIP URI dial plans and Enterprise Voice dial plans.

Deploying Redundant Exchange UM Servers

Important:

We recommend that you deploy a minimum of two servers on which Exchange UM services is running for each Exchange UM SIP URI dial plan that you configure for your organization. In addition to providing expanded capacity, deploying redundant servers provides high availability. In the event of an server failure, Lync Server 2013 can be configured to fail over to another server.

The following example configurations provide Exchange UM resiliency.

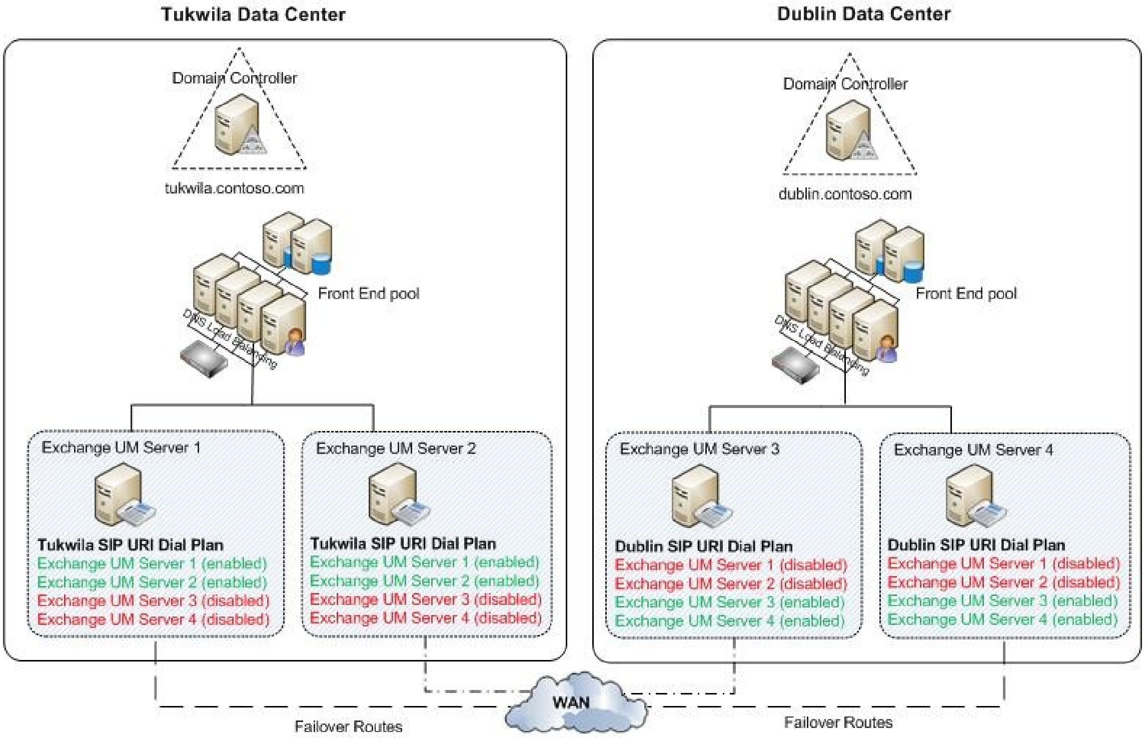


In Example 1, Exchange UM servers 1 and 2 are enabled in the Tukwila data center, and Exchange UM servers 3 and 4 are enabled in the Dublin data center. In the event of an Exchange UM outage in Tukwila, the Domain Name System (DNS) A records for servers 1 and 2 should be configured to point to servers 3 and 4, respectively. In the event of an Exchange UM outage in Dublin, the DNS A records for servers 3 and 4 should be configured to point to servers 1 and 2, respectively.

Note:

For Example 1, you should also assign one of following certificate on each Exchange UM server:

- Use a certificate with a wildcard in the Subject Alternative Name (SAN).
- Put the fully qualified domain name (FQDN) of each of the four Exchange UM servers in the SAN.


Tukwila Data Center
Domain Controller
tukwila.contoso.com
Front End pool
DNS Load Balancing
Exchange UM Server 1
Tukwila SIP URI Dial Plan
Exchange UM Server 1 (enabled)
Exchange UM Server 2 (enabled)
Exchange UM Server 3 (disabled)
Exchange UM Server 4 (disabled)
Exchange UM Server 2
Tukwila SIP URI Dial Plan
Exchange UM Server 1 (enabled)
Exchange UM Server 2 (enabled)
Exchange UM Server 3 (disabled)
Exchange UM Server 4 (disabled)
Dublin Data Center
Domain Controller
dublin.contoso.com
Front End pool
DNS Load Balancing
Exchange UM Server 3
Dublin SIP URI Dial Plan
Exchange UM Server 1 (disabled)
Exchange UM Server 2 (disabled)
Exchange UM Server 3 (enabled)
Exchange UM Server 4 (enabled)
Exchange UM Server 4
Dublin SIP URI Dial Plan
Exchange UM Server 1 (disabled)
Exchange UM Server 2 (disabled)
Exchange UM Server 3 (enabled)
Exchange UM Server 4 (enabled)
WAN
Failover Routes
Failover Routes

In Example 2, under ordinary operating conditions Exchange UM servers 1 and 2 are enabled in the Tukwila data center, and Exchange UM servers 3 and 4 are enabled in the Dublin data center. All four servers are included in the Tukwila users' SIP URI dial plan; however, servers 3 and 4 are disabled. In the event of an Exchange UM outage in Tukwila, for example, Exchange UM servers 1 and 2 should be disabled and Exchange UM servers 3 and 4 should be enabled so the Tukwila Exchange UM traffic will be routed to the servers in Dublin.

For details about how to enable or disable Unified Messaging on Exchange 2013, see “Integrate Exchange 2013 UM with Lync Server” at http://go.microsoft.com/fwlink/p/?LinkId=265372.

For details about how to enable or disable Unified Messaging on Microsoft Exchange Server 2010, see:

- "Enable Unified Messaging on Exchange 2010" at http://go.microsoft.com/fwlink/p/?LinkId=204418.
- "Disable Unified Messaging on Exchange 2010" at http://go.microsoft.com/fwlink/p/?LinkId=204416.

⊟See Also

Concepts

Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013

1.3.14.2.4 Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013

Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013

Planning > Planning for Enterprise Voice > Planning for Exchange Unified Messaging Integration >

Topic Last Modified: *2012-12-17*

If you want to integrate Exchange Unified Messaging (UM) with Lync Server 2013, you must perform the tasks described in this topic. Also be sure that you review the planning and deployment best practices described in Guidelines for Integrating On-Premises Unified Messaging and Lync Server 2013. This topic assumes that you have deployed Lync Server 2013 with a collocated Mediation Server and that you have enabled users for Lync Server 2013, but not necessarily that you have performed all deployment and configuration steps to enable Enterprise Voice, as described in Deploying Enterprise Voice in the Deployment documentation.

Unified Messaging Integration Process

◆**Important:**
It is important that you coordinate with your organization’s Exchange administrators to confirm the tasks that each of you will perform to help ensure a smooth, successful integration.

Phase	Steps	Required groups and roles	Deployment documentation
Deploy one of the following: • Microsoft Exchange Server 2007 Service Pack 1 (SP2) or latest service pack • Microsoft Exchange Server 2010 or latest service pack • Microsoft Exchange Server 2013	If you are using Microsoft Exchange Server 2013, install the following Exchange Server roles in either the same forest or a different forest as Lync Server 2013: • Client Access • Mailbox If Microsoft Exchange Server 2013 and Exchange Unified Messaging (UM) are installed in different forests, configure each Exchange forest to trust the Lync Server 2013 forest. If you are using Exchange 2010, install the following Exchange Server roles in either the same forest or a different forest as Lync Server 2013: • Unified Messaging • Hub Transport • Client Access • Mailbox If Lync Server 2013 and Exchange Unified	Enterprise administrators (if this is the first Exchange Server in the organization) -OR- Exchange Organization administrator (if this is not the first Exchange Server in the organization)	See the appropriate documentation for your version of Exchange Server: • Exchange Server 2007 deployment documentation at http://go.microsoft.com/fwlink/p/?LinkId=268694. • Exchange Server 2010 or latest service pack deployment documentation at http://go.microsoft.com/fwlink/p/?LinkId=268695. • Microsoft Exchange Server 2013 Planning and Deployment at http://go.microsoft.com/fwlink/p/?LinkId=266569.

	Messaging (UM) are installed in different forests, configure each Exchange forest to trust the Lync Server 2013 forest.		
Install certificates.	Download and install certificates for each Exchange UM server from a trusted root certificate authority (CA). The certificates are required for mutual Transport Level Security (MTLS) between the servers running Exchange UM and Lync Server 2013.	Administrators	Configure Certificates on the Server Running Microsoft Exchange Server Unified Messaging
Create and configure a new Exchange UM SIP dial plan.	On the Exchange UM server, create a SIP dial plan based on your organization’s specific deployment requirements.	Exchange Organization administrator	For Exchange 2007 SP1 or latest service pack, see "How to Create a Unified Messaging SIP URI Dial Plan" at http://go.microsoft.com/fwlink/p/?linkId=268632. For Exchange 2010 or latest service pack, see "Create a UM Dial Plan" at http://go.microsoft.com/fwlink/p/?linkId=268674. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.
Configure security settings for the Exchange UM SIP dial plan.	To encrypt Enterprise Voice traffic, configure the security settings on the Exchange UM SIP dial plan as **SIP Secured** or **Secured**. This is an especially important step if you have deployed or plan to deploy Lync Phone Edition devices in your environment. For Lync Phone Edition devices to function in an environment with Exchange UM integration, Lync Server encryption settings must	Exchange Organization administrator	Configure Unified Messaging on Microsoft Exchange For Exchange 2007 SP1 or latest service pack, see also: "How to Configure Security on a Unified Messaging Dial Plan" at http://go.microsoft.com/fwlink/p/?LinkId=268696. For Exchange 2010 or latest service pack, see also:

	align with the Exchange UM dial plan security settings. For details, refer to the Deployment documentation.		"Configure VoIP Security on a UM Dial Plan" http://go.microsoft.com/fwlink/p/?LinkId=268697. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.
Add Unified Messaging servers to the Exchange UM SIP dial plan.	To enable a newly installed Unified Messaging server to answer and process incoming calls, you must add the Unified Messaging server to a UM dial plan. In this case, add the server to the Exchange UM SIP dial plan.	Administrators Exchange Server administrators	For Exchange 2007 SP1 or latest service pack, see "How to Add Unified Messaging Server to a Dial Plan" at http://go.microsoft.com/fwlink/p/?linkId=268681. For Exchange 2010 or latest service pack, see "View or Configure the Properties of a UM Server" at http://go.microsoft.com/fwlink/p/?linkId=268682. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.
Configure mailboxes with SIP addresses.	Assign SIP addresses to the mailboxes of Enterprise Voice users who will be using Exchange UM features.	Lync Server 2013 administrator Exchange Recipient administrator	For Exchange 2007 SP1 or latest service pack, see "How to Add, Remove, or Modify a SIP Address for a UM-Enabled User" at http://go.microsoft.com/fwlink/p/?LinkId=268698. For Exchange 2010 or latest service pack, see "Modify a SIP Address for a UM-Enabled User" at http://go.microsoft.com/fwlink/p/?LinkId=268699. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.
Run the exchucutil.ps1	On the server running Exchange UM services,	Exchange Organization	Configure Unified

script.	open the Exchange Management Shell and run the exchucutil.ps1 script, which does the following: • Grants Lync Server 2013 permission to read Exchange UM Active Directory Domain Services (AD DS) objects, specifically, the SIP dial plans created in the previous task. • Creates a Unified Messaging IP gateway object in Active Directory for each Lync Server 2013 Enterprise Edition pool or Standard Edition server that hosts users who are enabled for Enterprise Voice. • Creates an Exchange UM hunt group for each gateway. The hunt group pilot identifier will be the name of the dial plan that is associated with the corresponding gateway. These need to be mapped 1:1 if there is more than one dial plan.	administrator Exchange Recipient administrator	Messaging on Microsoft Exchange

Configure Lync Server 2013 dial plans.	If you are integrating with Exchange 2007 SP1 or latest service pack, or Exchange 2010, create a new Enterprise Voice dial plan with a name that matches the Exchange UM dial plan fully qualified domain name (FQDN). **Note:** You will need to do this for each UM Dial plan. If you are integrating with Exchange 2010 SP1, ensure that suitable global/site-level or pool-level Enterprise Voice dial plans have been configured. **Note:** If you are integrating with Exchange 2010 SP1, the Lync Server dial plan and Exchange UM SIP dial plan names do not need to match.	RTCUniversalServerAdmins	Configuring Dial Plans
Run the Exchange UM Integration tool.	On the Lync Server 2013, run **ocsumutil.exe**, which: - Creates Subscriber Access and Auto Attendant contact objects. - Validates that there is an Enterprise Voice dial plan with a name that matches the Exchange UM dial plan FQDN. If you are running Exchange 2010 SP1 or later, the dial plan names do not need to match, and you can ignore the	RTCUniversalServerAdmins *and* RTCUniversalUserAdmins **Important:** To run ocsumutil.exe successfully, the user must belong to both of these groups. **Note:** To create Contact objects, the user who runs ocsumutil.exe must have the correct permission to the Active Directory	Configure Lync Server 2013 to Work with Unified Messaging on Microsoft Exchange Server

	tool's warning about this. This tool works by scanning the Active Directory for Exchange UM settings and allowing the Lync Server 2013 administrator to view, create, and edit contact objects.	organizational unit (OU) where the new contact objects are stored. This permission can be granted by running the **Grant-CsOUPermission** cmdlet. For details, see the Lync Server Management Shell documentation.	
If necessary, perform other Enterprise Voice configuration steps.	If you have not already configured Enterprise Voice settings on your servers or users, do one or more of the following: • Deploy and configure Public switched telephone network (PSTN) gateways and Mediation Servers • Define voice policies, PSTN usage records, and outbound call routes. • Enable users for Enterprise Voice. • Optionally, configure specific users with dial plans. Other configuration steps may be required depending on the Enterprise Voice features that you enable.	RTCUniversalServerAdmins RTCUniversalUserAdmins	See topics in the following sections: • Configuring Voice Policies, PSTN Usage Records, and Voice Routes • Deploying Enterprise Voice

Enable Enterprise Voice users for Exchange UM.	On the Exchange UM server, ensure that a Unified Messaging mailbox policy has been created and that each user has a unique extension number assignment, and then enable the user for Unified Messaging.	Exchange Recipient administrator	For Exchange 2007 SP1 or latest service pack, see "How to Enable a User for Unified Messaging" at http://go.microsoft.com/fwlink/p/?LinkId=268700. For Exchange 2010 or latest service pack, see "Enable a User for Unified Messaging" at http://go.microsoft.com/fwlink/p/?LinkId=268701. For Exchange 2013, see Unified Messaging at http://go.microsoft.com/fwlink/p/?LinkId=266579.

1.3.14.3 Hosted Exchange Unified Messaging Integration

Hosted Exchange Unified Messaging Integration

Microsoft Lync Server 2013 > Planning > Planning for Enterprise Voice >

Topic Last Modified: *2012-09-20*

In addition to the support that previous Lync Server 2013 releases have provided for integration with *on-premises* deployments of Exchange Unified Messaging (UM), Lync Server 2013 introduces support for integration with *hosted* Exchange UM. Hosted Exchange UM enables Lync Server 2013 to provide voice messaging to your users if you transfer some or all of them to a hosted Exchange service provider such as Microsoft Exchange Online.

Lync Server 2013 Enterprise Voice uses the Exchange UM infrastructure to provide call answering, call notification, voice access (including voice mail), and auto attendant services. For details, see Features of Integrated Unified Messaging and Lync Server 2013.

- Hosted Exchange UM Architecture and Routing
- Hosted Voice Mail Policies
- Hosted Exchange User Management
- Hosted Exchange Contact Object Management
- Deployment Process for Integrating Hosted Exchange UM with Lync Server 2013

1.3.14.3.1 Hosted Exchange UM Architecture and Routing

Hosted Exchange UM Architecture and Routing

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-03-26*

This section provides an overview of the architecture for on-premises and hosted

Exchange UM integration, including supported modes, shared SIP space, and routing considerations.

- Hosted Exchange UM Integration Architecture
- Hosted Exchange UM Routing

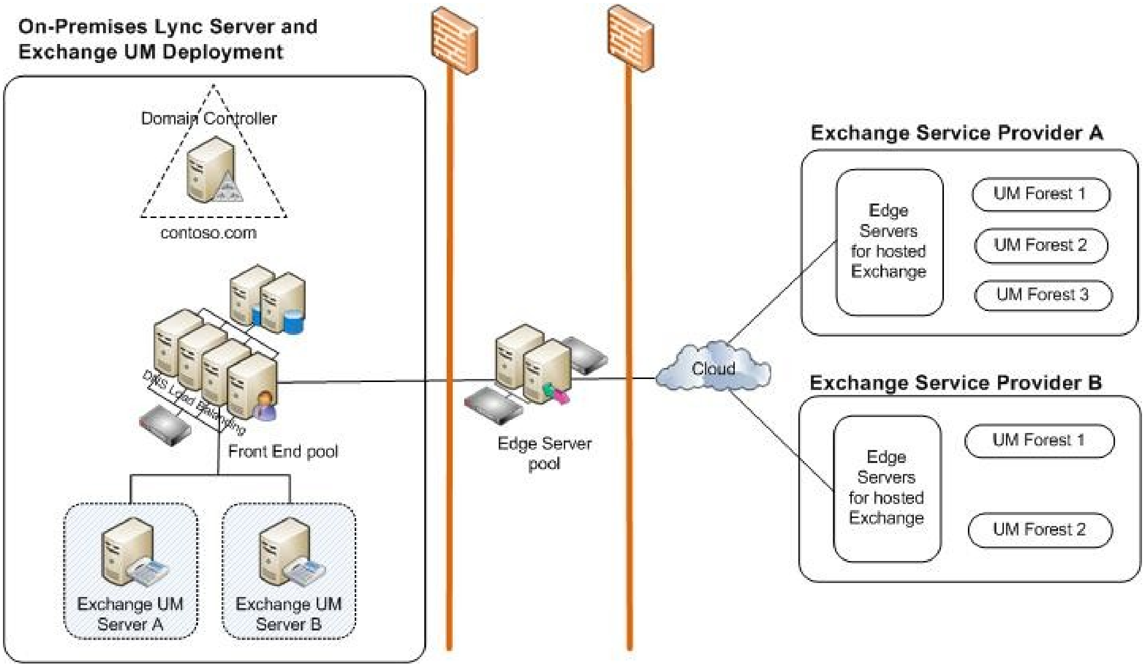
1.3.14.3.1.1 Hosted Exchange UM Integration Architecture

Hosted Exchange UM Integration Architecture

Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration > Hosted Exchange UM Architecture and Routing >

Topic Last Modified: *2012-09-25*

The Lync Server 2013 ExUM Routing application supports integration with an on-premises Exchange Unified Messaging (UM) deployment, with Exchange UM hosted by a service provider, or with a combination of the two. The following diagram shows all three possibilities.



The following modes are supported:

- **On-premises deployment:** Lync Server 2013 and Exchange UM are both deployed on local servers within your enterprise.
- **Cross-premises deployment:** Lync Server 2013 is deployed on local servers within your enterprise and Exchange UM is hosted in an online service provider's facility, such as a Microsoft Exchange Online data center.
- **Mixed deployment:** Your Lync Server 2013 deployment has some user mailboxes homed on local Exchange servers within your enterprise and some mailboxes homed in a hosted Exchange service data center.

> **Note:**
> The mixed deployment can be used as a transitional solution during evaluation and phased migration of users to hosted Exchange UM, or a permanent solution if you opt to keep some users' Exchange UM services on-

premises after transferring others.

Shared SIP Address Space

To integrate Lync Server 2013 with an on-premises Exchange UM deployment, you grant Lync Server 2013 permission to read Exchange UM Active Directory Domain Services objects. This approach does not work for integration with hosted Exchange UM, however, because Lync Server 2013 and Exchange UM are installed in separate forests with no trust between them.

To integrate Lync Server 2013 with hosted Exchange UM, you must configure a *shared SIP address space*. In this configuration, the same SIP domain address space is available to both Lync Server 2013 and the hosted Exchange UM service provider.

Note:

Use of the shared SIP address space is similar to the approach used in a cross-premises Lync Server 2013 environment, in which some users are homed in the on-premises deployment and some are homed in a hosted deployment (such as Lync Online). The SIP domain is split between them. When you integrate Lync Server 2013 with hosted Exchange UM, ensure that you include the Exchange UM service provider in the shared SIP address space.

To configure the shared SIP address space for integrating with an Exchange UM service provider, you need to configure your Edge Server as follows:

1. Configure the Edge Server for federation by running the **Set-CsAccessEdgeConfiguration** cmdlet to set the following parameters:
   - **UseDnsSrvRouting** specifies that Edge Servers will rely on DNS SRV records when sending and receiving federation requests.
   - **AllowFederatedUsers** specifies whether internal users are allowed to communicate with users from federated domains. This property also determines whether internal users can communicate with users in a split domain scenario.
   - **EnablePartnerDiscovery** specifies whether Lync Server 2013 will use DNS records to try to discover partner domains that are not listed in the Active Directory allowed domains list. If False, Lync Server 2013 will federate only with domains that are found on the allowed domains list. This parameter is required if you use DNS service routing. In most deployments, the value is set to false to avoid opening up federation to all partners.
2. Replicate the Central Management store to the Edge Server and verify the replication. For details, see Export Your Topology and Copy It to External Media for Edge Installation in the Deployment documentation.
3. Configure a *hosting provider* on the Edge Server by running the **New-CsHostingProvider** cmdlet to set the following parameters:
   - **Identity** specifies a unique string value identifier for the hosting provider that you are creating, for example, **Hosted Exchange UM**.
   - **Enabled** indicates whether the network connection between your domain and the hosting provider is enabled. Must be set to **True**.
   - **EnabledSharedAddressSpace** indicates whether the hosting provider will be used in a shared SIP address space scenario. Must be set to **True**.
   - **HostsOCSUsers** indicates whether the hosting provider is used to host Lync Server 2013 accounts. Must be set to **False**.
   - **ProxyFQDN** specifies the fully qualified domain name (FQDN) for the proxy server used by the hosting provider, for example, **proxyserver.fabrikam.com**. Contact your hosting provider for this information. This value cannot be modified. If the hosting provider changes its proxy server, you will need to delete and then recreate the entry for that provider.
   - **IsLocal** indicates whether the proxy server used by the hosting provider is contained within your Lync Server 2013 topology. Must be set to **False**.

1.3.14.3.1.2 Hosted Exchange UM Routing

Hosted Exchange UM Routing

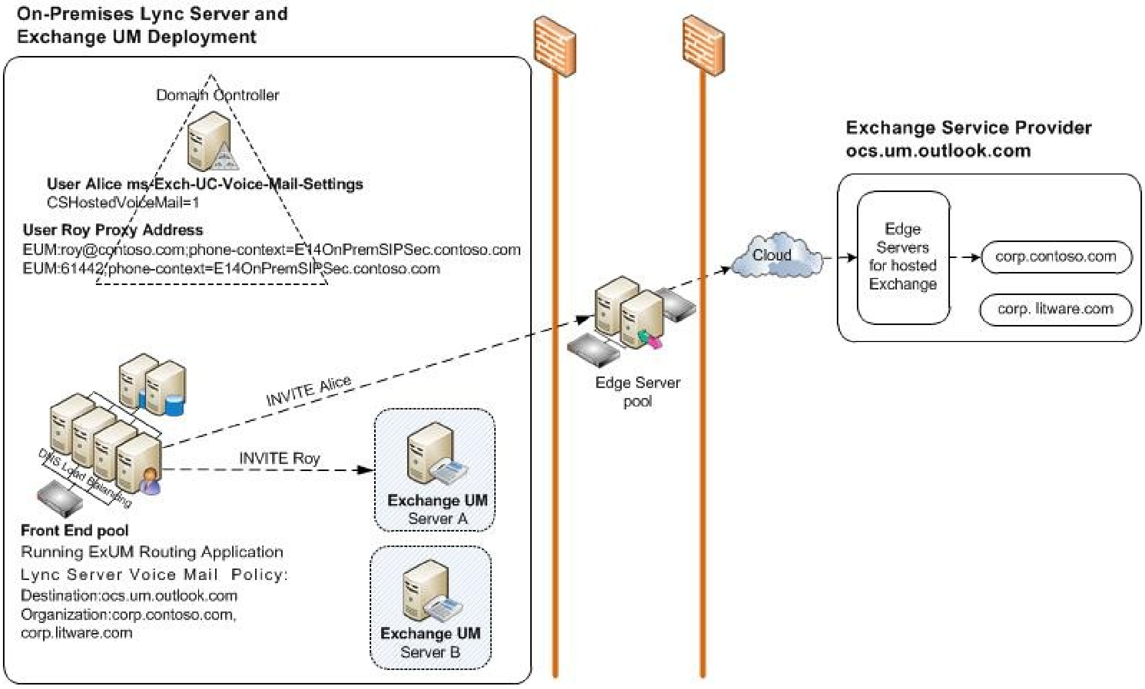
Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration > Hosted Exchange UM Architecture and Routing >

Topic Last Modified: *2012-10-01*

The Exchange UM Routing application runs on the Front End Server to route calls, either to an on-premises Microsoft Exchange Server Unified Messaging (UM) deployment or to hosted Exchange UM service.

The ExUM Routing Application

The Lync Server 2013 Exchange UM Routing application uses information from user account settings and from hosted voice mail policy parameters to determine how to route calls for hosted voice messaging, as shown in the following diagram.


On-Premises Lync Server and Exchange UM Deployment
Domain Controller
User Alice ms-Exch-UC-Voice-Mail-Settings
CSHostedVoiceMail=1
User Roy Proxy Address
EUM:roy@contoso.com;phone-context=E14OnPremSIPSec.contoso.com
EUM:61442;phone-context=E14OnPremSIPSec.contoso.com
DNS Load Balancing
INVITE Alice
INVITE Roy
Front End pool
Running ExUM Routing Application
Lync Server Voice Mail Policy:
Destination:ocs.um.outlook.com
Organization:corp.contoso.com,
corp.litware.com
Exchange UM
Server A
Exchange UM
Server B
Edge Server
pool
Cloud
Exchange Service Provider
ocs.um.outlook.com
Edge
Servers
for hosted
Exchange
corp.contoso.com
corp. litware.com

Exchange UM routing can be configured to route calls to users who are enabled for on-premises Exchange UM, to users who are enabled for hosted Exchange UM, or to a combination of the two.

For example, suppose that Roy’s mailbox and Exchange UM service are homed in an on-premises Exchange deployment.

- The proxy address information from Roy’s user account provides the information that the ExUM Routing application uses to route his calls to an on-premises Exchange UM server.

Alice’s mailbox and Exchange UM service are located at a hosted Exchange service provider’s data center. Routing for her Exchange UM calls is configured as follows:

- The values set in the msExchUCVoiceMailSettings attribute of Alice’s user account tell the ExUM Routing application to check for routing details in a hosted voice mail policy.

> **Note:**
> The value of the msExchUCVoiceMailSettings attribute can be set by either the Exchange service provider or the Lync Server 2013 administrator. In the example shown in the preceding diagram, the value (CsHostedVoiceMail=1) was set by the Lync Server 2013 administrator to enable hosted voice mail for Alice. For details about this attribute, see Hosted Exchange User Management.

- The hosted voice mail policy that is assigned to Alice's user account provides routing details:
  - Destination is the hosted Exchange UM service provider (ls.ExUm.<*hostedExchangeServer*>.com in this example).
  - Organizations are identified by the tenant IDs, which are the routing FQDNs for SIP messages for Exchange Server tenants that are located on ls.ExUm.<*hostedExchangeServer*>.com (corp.contoso.com and corp.litwareinc.com in this example).

    > **Note:**
    > The FQDN for Exchange Online is exap.um.outlook.com.

    For details, see Hosted Voice Mail Policies.

> **Note:**
> If both the msExchUCVoiceMailSettings attribute and the UM proxy address settings are present in a user account, the msExchUCVoiceMailSettings attribute takes precedence.

1.3.14.3.2 Hosted Voice Mail Policies

Hosted Voice Mail Policies

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-10-01*

A *hosted voice mail policy* provides information to the Lync Server 2013 ExUM Routing application about where to route calls for users whose mailboxes are located on a hosted Exchange service.

> **Note:**
> Hosted voice mail policies are required only for Lync Server 2013 integration with hosted Exchange UM. They are not needed for integration with on-premises Exchange UM.

Hosted Voice Mail Policy Scope

Hosted voice mail policy scope determines the hierarchical level at which the policy applies. You can configure hosted voice mail policies with the following scope levels:

- The *global* policy can potentially affect all users in the Lync Server 2013 deployment. If a user is enabled for hosted Exchange UM access and has not been assigned a per-user policy, and if a site policy has not been assigned to the user's site, the global policy applies. The global policy is installed with Lync Server 2013. You can modify it to meet your needs, but you cannot rename or delete it.
- A *site* policy can affect all users that are homed on the site for which the policy is defined. If a user is configured for hosted Exchange UM access and has not been assigned a per-user policy, the site policy applies.
- A *per-user* policy can affect only individual users or groups. To enforce a per-user policy, you must explicitly assign the policy to individual users, groups, and contact objects.

> **Note:**

In most cases, only one hosted voice mail policy is required. You can often modify the global policy to meet all your needs. If you deploy multiple hosted voice mail policies, all such policies have per-user scope.

Hosted Voice Mail Policy Attributes

A voice mail policy defines two attributes that the Lync Server 2013 ExUM Routing application inserts in the request URI of an INVITE message that is sent to the hosted Exchange UM implementation:

- **Destination:** The fully qualified domain name (FQDN) of the hosted Exchange UM service. This value is used by the on-premises Lync Server Edge Server for routing purposes.

  Note:

  The FQDN for Exchange Online is exap.um.outlook.com.

- **Organization:** The FQDN of the tenant on the hosted Exchange UM service that homes your Lync Server 2013 users' mailboxes. A voice mail policy can contain multiple organizations. If more than one organization is included in the policy, this attribute must be a comma-separated list of the Exchange Server tenants that home your Lync Server 2013 user mailboxes.

Note:

The tenant administrator of your hosted Exchange UM service will provide the necessary values for your Destination and Organization attribute settings. To configure your policy, you must run the New-CsHostedVoicemailPolicy cmdlet or use the Set-CsHostedVoicemailPolicy cmdlet to modify one that exists (for example, the global policy).

For details about managing hosted voice mail policies, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsHostedVoicemailPolicy
- Set-CsHostedVoicemailPolicy
- Get-CsHostedVoicemailPolicy

Per-User Voice Mail Policy Assignment

If your hosted voice mail policy is defined with per-user scope, you must explicitly assign it. You can run the Grant-CsHostedVoicemailPolicy cmdlet to assign the policy to individual users or groups.

For details about assigning or removing a per-user hosted voice mail policy, see the Lync Server Management Shell documentation for the following cmdlets:

- Grant-CsHostedVoicemailPolicy
- Remove-CsHostedVoicemailPolicy

1.3.14.3.3 Hosted Exchange User Management

Hosted Exchange User Management

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-10-18*

To provide voice mail services for Lync Server 2013 users whose mailboxes are located on a hosted Exchange service, you must enable their user accounts for hosted voice mail.

Note:

Before a Lync Server 2013 user can be enabled for hosted voice mail, a hosted voice mail policy that applies to the corresponding user account must be deployed. The policy can be global, site, or per-user in scope, as long as it applies to the user whom you want to enable. For details, see Hosted Voice Mail Policies.

The msExchUCVoiceMailSettings Attribute

Lync Server 2013 introduces a new user attribute named **msExchUCVoiceMailSettings**, which is created as part of the Lync Server 2013 Active Directory schema preparation. This multivalued attribute holds voice mail settings that are shared by Lync Server 2013 and the hosted Exchange service.

The hosted Exchange service may in some cases set the value of the msExchUCVoiceMailSettings attribute in the process of enabling Exchange UM, or during the process of transferring mailboxes to a hosted Exchange Server. If this attribute is not set by Exchange, the Lync Server 2013 administrator must set it by running the Set-CsUser cmdlet, as described earlier in this topic.

The attribute’s key/value pairs and their authors are shown in the following table.

The msExchUCVoiceMailSettings Attribute Key/Value Pairs

Value	Author	Meaning
ExchangeHostedVoiceMail=1	Exchange	User has been enabled for hosted UM access by Exchange Server. The Exchange UM Routing application will check the user’s hosted voice mail policy for routing details.
ExchangeHostedVoiceMail=0	Exchange	User has been disabled for hosted UM access by Exchange Server.
CsHostedVoiceMail=1	Lync Server	User has been enabled for hosted UM access by Lync Server 2013. The Lync Server 2013 ExUM Routing application will check the user’s hosted voice mail policy for routing details.
CsHostedVoiceMail=0	Lync Server	User has been disabled for hosted UM access by Lync Server 2013.

Note:

If the attribute already has values other than one of the Lync Server 2013 key/value pairs (CSHostedVoiceMail=0 or CSHostedVoiceMail=1), a warning will indicate that the attribute may be managed by a different application. For example, a warning is displayed if the key/value pair ExchangeHostedVoiceMail=0 or ExchangeHostedVoiceMail=1 is already present. In that case, you can change the value by editing it the Active Directory, or run the following cmdlet to set the value to null:
Set-CsUser –identity user –HostedVoicemail $null

Enabling Users for Hosted Voice Mail

To enable a user’s voice mail calls to be routed to hosted Exchange UM, you must run the Set-CsUser cmdlet to set the value of the *HostedVoiceMail* parameter. This parameter also signals Lync Server 2013 to light up the “call voice mail” indicator.

- The following example enables Pilar Ackerman’s user account for hosted voice mail:

  ```
  Set-CsUser -Identity "Pilar Ackerman" -HostedVoiceMail $True
  ```

  The cmdlet verifies that a hosted voice mail policy (global, site-level or per-user) applies to this user. If no policy applies, the cmdlet fails.
- The following example disables Pilar Ackerman’s user account for hosted voice mail:

  ```
  Set-CsUser -Identity "Pilar Ackerman" -HostedVoiceMail $False
  ```

  The cmdlet verifies that no hosted voice mail policy (global, site-level or per-user) applies to this user. If a policy does apply, the cmdlet fails.

For details about using the Set-CsUser cmdlet, see the Lync Server Management Shell documentation.

1.3.14.3.4 Hosted Exchange Contact Object Management

Hosted Exchange Contact Object Management

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-09-25*

You need to configure a Contact object for each auto-attendant number and subscriber access number in your cross-premises deployment.

For integration with hosted Exchange UM, ocsumutil.exe cannot be used to manage Contact objects, because it depends on Active Directory Exchange UM settings. In a cross-premises deployment, Lync Server 2013 and hosted Exchange UM are installed in separate forests with no trust between them. For security reasons, Lync Server 2013 administrators have no direct access to Exchange UM Active Directory settings. As a result, Lync Server 2013 provides a different model for managing Contact objects in a *shared SIP address space* that is accessible to both Lync Server 2013 and the hosted Exchange UM service.

Hosted Contact Object Workflow

The following are the general steps for working with your hosted Exchange tenant administrator to manage contact objects:

1. The Exchange administrator requests phone numbers for the Exchange UM subscriber access and auto-attendant Contact objects.
2. The Lync Server 2013 administrator creates a Contact object for each phone number and assigns a hosted voice mail policy to each Contact object.
3. The Lync Server 2013 administrator provides the phone numbers to the Exchange administrator.
4. The Exchange administrator assigns the phone numbers to appropriate Exchange UM dial plans for auto attendants and subscriber access.

Note:

There is no need to configure any Lync Server 2013 dial plan settings on the Contact objects as there is with on-premises deployments.

Configuring Hosted Contact Objects

Note:

Before Lync Server 2013 Contact objects can be enabled for hosted Exchange UM, a hosted voice mail policy that applies to them must be deployed. The policy can be of global, site-level, or per-user scope, as long as it applies to the contact object you want to enable. For details, see Hosted Voice Mail Policies.

To configure hosted auto-attendant and subscriber access Contact objects in a cross-premises deployment, you must use the following cmdlets:

- **New-CsExUmContact** creates a new Contact object for hosted UM.
- **Set-CsExUmContact** modifies an existing Contact object for hosted Exchange UM.

The following example creates an auto-attendant Contact object:

```
New-CsExUmContact -SipAddress sip:exumaa1@fabrikam.com -RegistrarPool RedmondPool
```

This example creates a new Exchange UM Contact object with the SIP address sip:exumaa1@fabrikam.com. The name of the pool where the Lync Server 2013 Registrar service is running is RedmondPool.litwareinc.com. The Active Directory organizational unit where this information will be stored is OU=ExUmContacts,DC=litwareinc,DC=com. The phone number of the Contact object is 2065554567. The optional -AutoAttendant $True parameter specifies that this object is an auto-attendant Contact object. Setting the -AutoAttendant parameter to False (the default) specifies a subscriber access Contact object.

For details about the New-CsExUmContact and Set-CsExUmContact cmdlets, see the Lync Server Management Shell documentation.

1.3.14.3.5 Deployment Process for Integrating Hosted Exchange UM with Lync Server 2013

Deployment Process for Integrating Hosted Exchange UM with Lync Server 2013

Planning > Planning for Enterprise Voice > Hosted Exchange Unified Messaging Integration >

Topic Last Modified: *2012-09-25*

Effective planning for integrating Lync Server 2013 with hosted Exchange Unified Messaging (UM) requires that you take into account the following:

- Prerequisites for integrating Lync Server 2013 with hosted Exchange UM
- Steps required during the integration process

Deployment Prerequisites for Integrating with Hosted Exchange UM

Before you can begin the integration process, you must already have deployed Lync Server 2013 (at a minimum, a Front End pool or a Standard Edition server), an Edge Server, and Lync 2013 or Lync 2010 clients.

Integration Process

The following table provides an overview of the hosted Exchange UM integration process. For details about deployment steps, see Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM in the Deployment documentation.

Phase	Steps	Rights and permissions	Deployment documentation
Configure the Edge Server.	1. Configure the Edge Server for federation. 2. Manually replicate data to the Edge Server. 3. Configure the hosting provider on the Edge Server.	RTCUniversalServerAdmins	Configure the Edge Server for Integration with Hosted Exchange UM
Configure hosted voice mail policy.	1. Either modify the global hosted voice mail policy or create a new hosted voice mail policy with Site or Per-User scope. 2. For policies with Per-User scope, assign the policy to users or groups.	RTCUniversalServerAdmins	Manage Hosted Voice Mail Policies
Enable users for hosted voice mail.	- Configure user accounts for users whose mailboxes are on a hosted Exchange service.	RTCUniversalUserAdmins	Enable Users for Hosted Voice Mail
Configure hosted contact objects.	1. Create auto-attendant Contact objects for hosted Exchange UM. 2. Create Subscriber Access contact objects for hosted Exchange UM.	RTCUniversalUserAdmins **Note:** To create, modify or remove contact objects, the user who runs the New-CsExUmContact, Set-CsExUmContact or Remove-CsExUmContact cmdlet must have the correct permission to the Active Directory organizational unit where the new contact objects are stored. This permission can be granted by running the Grant-CsOUPermission cmdlet. For details, see the Lync Server Management Shell documentation.	Create Contact Objects for Hosted Exchange UM

1.3.15 Planning for Clients and Devices in Lync Server 2013

Planning for Clients and Devices in Lync Server 2013

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-06-04*

The topics in this section describe how to plan for Lync Server 2013 clients and devices in your organization.

- Planning for Clients
- Planning for Mobile Clients
- Planning for Devices

1.3.15.1 Planning for Clients

Planning for Clients

Microsoft Lync Server 2013 > Planning > Planning for Clients and Devices in Lync Server 2013 >

Topic Last Modified: *2013-02-12*

The topics in this section discuss planning considerations for deploying Microsoft Lync Server 2013 clients. Whether you are deploying a new Lync Server 2013 installation or migrating from a previous deployment, these topics provide important client planning information.

- Clients for Lync Server 2013
- Client Comparison Tables
- Client System Requirements
- Client Policies and Settings
- Lync 2013 Compatibility
- Client Interoperability in Lync 2013

1.3.15.1.1 Clients for Lync Server 2013

Clients for Lync Server 2013

See Also

Microsoft Lync Server 2013 > Planning > Planning Primer: Planning for Your Organization >

Topic Last Modified: *2013-02-19*

Lync Server 2013 supports several types of client software that you can deploy to your organization’s users, including computer-installed client software, web-based clients, and mobile devices. This topic outlines the clients that you can use. For a detailed comparison of the features provided by Lync Server 2013 clients, see Client Comparison Tables.

Lync 2013

Lync 2013 is the full-featured client for Lync Server. The Lync 2013 user interface has been fully redesigned and includes newly integrated features, such as Persistent Chat (Lync 2010 had a separate client for chat functionality), tabbed conversations, video preview, and multiparty video. For a summary of changes, see What's New for Clients.

Lync 2013 client setup is part of the Office setup program on the installation media.

Online Meeting Add-in for Lync 2013

The Online Meeting Add-in for Lync 2013 supports meeting management from within Microsoft Outlook messaging and collaboration client. The Online Meeting Add-in for Lync 2013 software installs automatically with Lync 2013.

Lync Web Scheduler

Lync Web Scheduler is a web-based meeting scheduling and management tool for users who don't have access to Microsoft Outlook, or who are on an operating system not based on Windows. With Lync Web Scheduler, users can create new meetings, modify existing meetings, and send invitations using their preferred email program.

Lync Web App

Lync Web App is the web-based conferencing client for Lync Server 2013 meetings. In this release, the addition of computer audio and video to Lync Web App provides a complete in-meeting experience for anyone who does not have a Lync client installed locally. Meeting participants have access to all collaboration and sharing features and presenter meeting controls.

If Lync 2013 is not installed on a user's computer and the user clicks a meeting link in a meeting request, Lync Web App opens. You can also configure the Meeting Join page to allow users to join meetings by using previous versions of clients; see Configuring the Meeting Join Page in the Deployment documentation.

Because of the enhancements to Lync Web App, an updated version of Microsoft Lync 2010 Attendee is not available for Lync Server 2013. Lync Web App is the client of choice for participants outside your organization. With Lync Web App, no local client installation is required, although audio, video, and sharing features require installation of a plug-in during first use.

Lync 2013 Basic

Lync 2013 Basic is a downloadable client for customers who have a licensed, on-premises Lync Server 2013 deployment and customers who subscribe to a Microsoft Office 365 plan that does not include the full Lync 2013 client. The Lync Basic client includes enhanced presence, contacts, instant messaging (IM), Lync meetings, and basic voice functionality. Features not supported in Lync Basic include multiparty video, OneNote integration, virtual desktop infrastructure (VDI) support, skill search, recording, Enterprise Voice features, and advanced call handling (for example, call forwarding and Team Call). For details, see Client Comparison Tables.

Lync Windows Store App

The Lync Windows Store app is a touch-optimized Lync app designed specifically for Windows 8 and Windows RT. Users can download the app through the Windows Store by searching for "Lync." For more information, see Client Comparison Tables, Lync Windows Store App Requirements, and Deploying Lync Windows Store App.

Lync 2013 for Mobile Devices

Lync 2013 mobile apps now include voice over IP (VoIP) and video over IP capabilities, in addition to contacts, presence, and IM features. Mobile users can choose to communicate with others through IM, voice calls, or video calls by using either Wi-Fi or their cellular data connection. With a single click of the meeting link in a calendar item, mobile users can join voice and video meetings. For more information about Lync 2013 mobile apps, see Planning for Mobile Clients.

Supported Clients from Previous Releases

Lync Server 2013 supports the following clients from previous server releases. You can make certain previous clients available to users when they join meetings. For details, see Configuring the Meeting Join Page in the Deployment documentation.

- **Lync 2010** Lync 2010 provides a full desktop experience, including IM, enhanced presence, voice, video, sharing, and telephony. However, none of the new features introduced in Lync Server 2013 will be available until the user's client is upgraded to Lync 2013.
- **Lync 2010 Mobile** Lync Server 2013 supports all of the Microsoft Lync 2010 Mobile mobile apps. Microsoft Lync 2010 Mobile provides IM, enhanced presence, and telephony for users in your organization who are connecting from a smartphone or a phone running a Professional edition of Windows Mobile. You can instruct your users to install Microsoft Lync 2010 Mobile by directing them to the app marketplace for their mobile phone. For details, see "Planning for Mobile Clients" in the Lync Server 2010 documentation at http://go.microsoft.com/fwlink/p/?LinkID=235955.
- **Lync Phone Edition** Lync Phone Edition software for intelligent IP phones (for example, USB-attached phones) has not been updated for Lync Server 2013. Lync Phone Edition continues to be supported in for placing and receiving calls, enhanced presence, and client audio capabilities for conferences.
- **Lync 2010 Attendant** The Microsoft Lync 2010 Attendant integrated call-management program enables a receptionist to manage multiple conversations at the same time through rapid call handling, IM, and onscreen routing.

⊟See Also

Concepts

Client Interoperability in Lync 2013

1.3.15.1.2 Client Comparison Tables

Client Comparison Tables

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Clients >

Topic Last Modified: *2013-03-08*

The following tables compare the features and capabilities of clients running on Microsoft Lync Server 2013 in the following categories:

- Enhanced Presence Support
- Contacts and Contact Groups Support
- IM Support
- Conferencing Support
- Telephony Support
- External Users Support
- Archiving and Compliance Support

Note:

- These tables indicate the features that are available to Lync users in an on-premises deployment of Lync Server 2013. The same features are also available to Lync Online and Office 365 users unless otherwise indicated. For details about Lync Online subscription plans, see the Lync Online Service Description at http://go.microsoft.com/fwlink/p/?LinkId=282430.

- For information about Lync 2013 for mobile clients, see Mobile Client Comparison Tables.
- Lync Server 2013 supports the following previously released clients: Lync 2010, Lync 2010 Mobile, Lync Phone Edition, and Lync 2010 Attendant. For information about these clients, see the Lync 2010 version of the Client Comparison Tables at http://go.microsoft.com/fwlink/p/?LinkID=213798.

Enhanced Presence Support

Feature/ capability	Lync 2013	Lync Windows Store app	Lync 2013 Basic	Lync Web App	Lync 2010 Attendant	Lync Phone Edition	Communicator for Mac 2011	Lync for Mac 2011
Publish and view status	?	?	?		?	?	?	?
View status based on calendar free/busy information	?	?	?		?	?	?	?
View status notes and Out of Office messages	?	?	?		?	?	?	?
Add a custom location	?		?					
Add a custom note	?	?	?		?		?	?

Contacts and Contact Groups Support

Feature/ capability	Lync 2013	Lync Windows Store app	Lync 2013 Basic	Lync Web App	Lync 2010 Attendant	Lync Phone Edition	Communicator for Mac 2011	Lync for Mac 2011
View Contacts list	?	?	?		?	?	?	?
Modify Contacts list	?	?	?		?	?	?	?

Tag contacts for status change alerts	?		?		?			
Control privacy relationships	?		?		?			
Search the corporate address book	?	?	?		?	?	?	?
Search Microsoft Outlook contacts	?		?		?	?		
Manage contact groups	?	?	?		?		?	?
Expand distribution groups	?	?	?		?	?		
Search for Response Groups[1]	?				?			
Display recent contacts group	?		?		?			
Display current conversations group	?		?		?	?		
Display alternate contact views (for example, tile)	?	?	?		?			?

[1] Not available to Lync Online and/or Office 365 users.

IM Support

Feature/ capability	Lync 2013	Lync Windows Store app	Lync 2013 Basic	Lync Web App	Lync 2010 Attendant	Lync Phone Edition	Communicator for Mac 2011	Lync for Mac 2011
Initiate IM with a contact	?	?	?		?		?	?
Navigate among multiple IM conversations	?	?	?		?		?	?
Log IM conversations in Outlook	?	?	?		?		Saved in Communicator for Mac	Saved in Lync for Mac
Initiate an email to a contact	?	?	?		?		?	?
Use prepared conversation templates					?			
Spelling checker		?						?
Skill search (with SharePoint Server integration) [1]	?	?			?			
Persistent Chat (Group Chat) integration[2]	?		?					

[1] Skill search is available with on-premises Lync Server 2013 and on-premises SharePoint 2013.

[2] Persistent Chat is not available to Lync Online and/or Office 365 users.

Conferencing Support

Note:

- Lync meeting features are not available in Lync Online Standalone Plan 1.
- In Lync-to-Lync sessions, a Lync Online Plan 1 user can participate in desktop sharing and application sharing if they are invited by a user who has access to sharing features.
- For details, see the Lync Online Service Description at http://go.microsoft.com/fwlink/?LinkID=282430.

Feature/ capability	**Lync 2013**	**Lync Windows Store app**	**Lync 2013 Basic**	**Lync Web App**	**Lync 2010 Attendant**	**Lync Phone Edition**	**Communicator for Mac 2011**	**Lync for Mac 2011**
Add computer audio	?	?	?	?	?	?	?	?
Add video	?	?	?	?			?	?
View multiparty video	?	?		?				?
Use in-meeting presenter controls	?		?	?				?
Access detailed meeting roster	?	?	?	?	?			?
Participate in multiparty IM	?	?	?	?	?		?	?
Share the desktop (if enabled)	?		?	? (requires plug-in)			?[1]	?[1]
Share a program (if enabled)	?		?	? (requires plug-in)				View only
Add anonymous participants (if enabled)	?		?	?				?
Use dial-in audio conferencing	?	?	?	?	?			?
Initiate a	?		?					?

meeting								
Add Microsoft PowerPoint files	?		?	?				View only, annotations not available
Navigate Microsoft PowerPoint files	?		?	?				?
Use OneNote meeting notes	?			?				
Use a whiteboard	?		?	?				
Conduct polls	?		?	?				
Share files	?		?	?				?

[1] Participants cannot control desktops that are shared by Lync for Mac 2011 or Communicator for Mac 2011 users. Lync for Mac 2011 and Communicator for Mac 2011 users can control desktops shared by Windows users.

Telephony Support

Note:

Lync Voice features are limited to certain Lync Online subscription plans. For details, see the "Lync Voice Features" topic in the Lync Online Service Description at http://go.microsoft.com/fwlink/?LinkID=282430.

Feature/ capability	**Lync 2013**	**Lync Windows Store app**	**Lync 2013 Basic**	**Lync Web App**	**Lync 2010 Attendant**	**Lync Phone Edition**	**Communicator for Mac 2011**	**Lync for Mac 2011**
Initiate a voice call	?	?	?		?	?	?	?
Click to call a contact	?	?	?		?	?	?	?
Transfer a call	?	?			?	?		?
Manage call forwarding	?	?			?	?		?

Manage team call settings	?				?			
Manage delegates	?							
Initiate a call to a Response Group	?				?			
Support emergency services (E9-1-1)	?	?	?		?	?		
Connect to voice mail	?	?			?	?		
Make calls on behalf of another contact (manager/delegate scenario)	?							
Handle another's calls if configured as a delegate	?				?	?		
Manage a high volumes of calls					?			

External Users Support

Feature/ capability	Lync 2013	Lync Windows Store app	Lync 2013 Basic	Lync Web App	Lync 2010 Attendant	Lync Phone Edition	Communicator for Mac 2011	Lync for Mac 2011
Initiate IM with a public contact	?	?	?		?		?	?
Initiate IM with a federate	?	?	?		?		?	?

d contact								
Conduct two-party or multiparty calls with external users	?	?	?		?	?	?	?

Archiving and Compliance Support

Feature/ capability	Lync 2013	Lync Windows Store app	Lync 2013 Basic	Lync Web App	Lync 2010 Attendant	Lync Phone Edition	Communicator for Mac 2011	Lync for Mac 2011
Provide client-side archiving [1]	?				?		?	?
Provide client-side recording [2]	?							

[1] Application sharing archiving and desktop sharing archiving is unavailable in Lync Online subscription plans.

[2] Client-side recording is unavailable in certain Lync Online standalone plans. For details, see the Lync Online Service Description at http://go.microsoft.com/fwlink/?LinkID=282430.

1.3.15.1.3 Client System Requirements

Client System Requirements

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Clients >

Topic Last Modified: *2012-11-06*

This section describes the hardware and software requirements for Lync 2013 clients.

- Lync Client Hardware Support
- Lync Client Video Requirements
- Lync Client Software Support
- Lync Web App Supported Platforms
- Lync Windows Store App Requirements

1.3.15.1.3.1 Lync Client Hardware Support

Lync Client Hardware Support

Supportability > Supported Hardware > Client and Device Hardware Support >

Topic Last Modified: *2012-12-14*

This section describes the recommended hardware for Lync 2013 and the Online Meeting Add-in for Lync 2013.

Recommended Hardware for Lync 2013 and the Online Meeting Add-in for Lync 2013

System component	Minimum requirement
Computer/processor	Intel Pentium 4, AMD Athlon 64, or equivalent
Memory	2 gigabytes (GB) of RAM
Data and Voice	Minimum 1.6 gigahertz (GHz) or faster processor. We recommend 2.0 gigahertz (32-bit or 64- bit).
Video	See Lync Client Video Requirements
Display resolution	1024x768 required
Graphics hardware	• Support for Microsoft DirectX 9 application programming interface • 128 megabytes (MB) of graphics memory (minimum). We recommend 256 MB of graphics memory. • Windows Display Driver Model driver • Pixel Shader 2.0 in hardware • 32 bits per pixel
Telephony	Microphone and speakers, headset with microphone, or equivalent device(s). Recommended devices: • Phones with the "Optimized for Microsoft Lync" logo (see Phones and Devices Qualified for Microsoft Lync at http://go.microsoft.com/fwlink/p/?LinkID=208938 for a list) • Phones that run Lync Phone Edition
Video source	USB 2.0 video camera or Polycom CX5000 HD device (RoundTable device)
Bandwidth Requirements	See Network Bandwidth Requirements for Media Traffic

1.3.15.1.3.2 Lync Client Video Requirements

Lync Client Video Requirements

Planning for Clients and Devices in Lync Server 2013 > Planning for Clients > Client System Requirements >

Topic Last Modified: *2012-12-07*

This section describes video hardware support for Lync 2013 video calls and describes how to determine the expected video quality for various computer configurations.

Lync 2013 introduces hardware acceleration for video encoding and decoding based on the H.264/MPEG-4 Part 10 Advanced Video Coding standard. This feature allows computers with lower CPU clock speeds to encode and decode higher resolution video. Video hardware requirements vary depending on the computer configuration and the video resolution wanted.

Video Hardware Requirements

Feature	Requirement
Hardware accelerated H.264 decoding using DirectX Video Acceleration (DXVA)	• Graphics card must support DirectX 9.0 and must expose the DXVA2_ModeH264_VLD_NoFGT decoding mode. • The latest graphics card driver must be installed. **Note:** For details about decoding modes, see http://go.microsoft.com/fwlink/p/?LinkId=268530.
Hardware accelerated H.264 encoding: Chipset Requirements	The following hardware accelerated video encoding solutions are supported: • Second and third generation Intel HD Graphics 2000, 2500, 3000, and 4000 chipsets (or later versions) with integrated hardware video encoders. • Intel HD Graphics driver 15.28.9.2884 or the latest driver containing the following: • Display driver 9.17.10.2884 or the latest driver • Hardware media foundation transform (HMFT) version 3.12.10.31 or the latest HMFT
Hardware accelerated H.264 encoding: Camera Requirements	USB video cameras with integrated H.264 hardware encoder that conforms to the USB Video Class (UVC) specification version 1.5. **Note:** Lync 2013 supports UVC 1.5 cameras with Windows 8, which includes support for UVC 1.5. Because Windows 7 does not include support for UVC 1.5, Lync 2013 treats UVC 1.5 cameras as regular cameras with no hardware encoding support.

Determining H.264 Video Encoding and Decoding Capabilities

Generally, there are four major factors that determine the maximum encoding and decoding capability of a particular computer configuration:

- Support for hardware accelerated decoding by using DXVA
- Support for hardware accelerated encoding
- Number of physical cores
- Windows Experience Index (WEI)

The Windows System Assessment Tool (WinSAT) determines the WEI. When you run the WinSAT tool, it generates a Formal.Assessment XML document on the computer in the %windir%\Performance\WinSAT\DataStore directory. This XML file contains the following two scores that are of particular importance for determining encoding and decoding capabilities:

- The VideoEncodeScore indicates the software-based video encoding capability of the computer.
- The GraphicsScore value indicates the hardware accelerated encoding capability of the computer.

The following three tables explain the maximum encoding and decoding capability for different PC types depending on what hardware acceleration they support. For resolutions of 640x360 and higher, the maximum supported frame rate is 30 frames per second (fps). For resolutions lower than 640x360, the maximum supported frame rate is 15 fps.

Computer Without DXVA And Without Hardware Accelerated Encoder

Capable Encoder Resolution	Capable Decoder Resolution	Requirement
424x240	424x240 (640x360 at 15fps for receive only scenarios)	1 Core and VideoEncodeScore ≥ 4.0
640x360	640x360	2 Cores and VideoEncodeScore ≥ 4.5
640x360	1280x720	2 Cores and VideoEncodeScore ≥ 4.5
640x360	1920x1080	4 Cores and VideoEncodeScore ≥ 4.5
1280x720	1280x720	4 Cores and VideoEncodeScore ≥ 7.3
1280x720	1920x1080	4 Cores and VideoEncodeScore ≥ 7.3
1920x1080	1920x1080	N/A

Computer With DXVA But Without Hardware Accelerated Encoder

Capable Encoder Resolution	Capable Decoder Resolution	Requirement
424x240	1920x1080	1 Core and VideoEncodeScore ≥ 3.0
640x360	1920x1080	2 Cores and VideoEncodeScore ≥ 4.5
960x540	1920x1080	2 Cores and VideoEncodeScore ≥ 6.0
1280x720	1920x1080	4 Cores and VideoEncodeScore ≥ 6.7
1920x1080	1920x1080	4 Cores and VideoEncodeScore ≥ 8.2

Note:

The WinSAT score on Windows 7 is limited to a maximum of 7.9. Therefore, the encoding capability for a computer without a hardware accelerated encoder can only be achieved on Windows 8, where the maximum WinSAT score is 9.9.

Computer With DXVA And With Intel HD Graphics Hardware Accelerated Encoder

Capable Encoder Resolution	Capable Decoder Resolution	Requirement
1280x720	1920x1080	All 2nd and 3rd generation Intel HD Graphics
1920x1080	1920x1080	2nd and 3rd generation Intel HD Graphics and GraphicsScore ≥ 5.0

1.3.15.1.3.3 Lync Client Software Support

Lync Client Software Support

See Also

Microsoft Lync Server 2013 > Supportability > Client and Device Software and Infrastructure Support >

Topic Last Modified: *2013-03-07*

This section summarizes software support for Lync 2013 and the Online Meeting Add-in for Lync 2013.

Note:

The Online Meeting Add-in for Lync 2013, which supports meeting management from within the Outlook messaging and collaboration client, installs automatically with Lync 2013.

Software Requirements for Lync 2013 and the Online Meeting Add-in for Lync 2013

System component	Minimum requirement
Windows Operating system	Windows 8 Windows 7 operating system Windows Server 2008 R2 with latest service pack
Installation and updates	Administrator rights and permissions
Browser	Windows Internet Explorer 10 Internet browser Windows Internet Explorer 9 Internet browser Windows Internet Explorer 8 Internet browser Windows Internet Explorer 7 Internet browser Mozilla Firefox web browser **Note:** If you are using Lync with Microsoft Exchange Online and your organization has deployed an authenticating HTTP proxy, Internet Explorer 9 or Internet Explorer 8 is required.
Microsoft Office Integration	For the full set of integration features: • Outlook 2013 messaging and collaboration client • Outlook 2010 messaging and collaboration client

Microsoft Exchange Integration	For the full set of integration features: • Microsoft Exchange Server 2013 • Microsoft Exchange Server 2010

Macintosh Operating Systems

Lync 2013 is available only for Windows. However, Lync Server 2013 supports the following clients on computers that are running Mac OS 10.5.8 or latest service pack or release (Intel-based) operating systems. For details about supported features, see Client Comparison Tables.

- Microsoft Lync for Mac 2011 (see "Lync for Mac 2011 Deployment Guide" at http://go.microsoft.com/fwlink/p/?LinkId=268786)
- Microsoft Communicator for Mac 2011 (see "Communicator for Mac 2011 Deployment Guide" at http://go.microsoft.com/fwlink/p/?LinkId=268787)

Lync Web App Browsers

Lync Web App supports specific combinations of operating systems and browsers. For details, see Lync Web App Supported Platforms in the Planning documentation.

Microsoft Office Supportability

Lync Server 2013 clients support integration with various versions of Microsoft Office, as summarized in this section.

- Lync 2013 integration features are supported on Outlook 2013 and Microsoft Outlook 2010.
- Lync 2013 integration features are supported on Microsoft Exchange Server 2013 and Microsoft Exchange Server 2010.
- Certain Lync 2013 integration features are supported on Microsoft Office 2007 and Microsoft Office 2003 Service Pack 3 (SP3). For integration with Microsoft Office 2007 to work correctly, you may have to install an update to Microsoft Office 2007. For details about the Outlook update, see Microsoft Knowledge Base article 936864, "Description of the 2007 Office hotfix package" at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=936864.
- The Online Meeting Add-in for Lync 2013 is supported with Office 2013, Microsoft Office 2010, Microsoft Office 2007, and the Microsoft Office 2003 suites.

Using Mandatory Profiles

If users are planning to use Lync 2013 conferencing features, they should not use Active Directory Domain Services (AD DS) mandatory profiles to sign in to the Lync 2013 client. Because mandatory profiles are read-only user profiles, the public key infrastructure (PKI) keys that are required for Lync 2013 conferencing cannot be saved to the profile. For details, see Microsoft Knowledge Base article 2552221, "Lync 2010 conferencing feature fails when the user is signed in using a mandatory user profile," at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=2552221.

⊟See Also

Concepts

Lync Client Hardware Support
Lync Client Video Requirements
Supported Clients from Previous Deployments

1.3.15.1.3.4 Lync Web App Supported Platforms

Lync Web App Supported Platforms

Planning for Clients and Devices in Lync Server 2013 > Planning for Clients > Client System Requirements >

Topic Last Modified: *2013-02-19*

To use Lync Web App, you must have one of the following supported operating system and browser combinations.

Note:

A plug-in is required for certain Lync Web App features, including computer-based voice, video, sharing, and viewing of ongoing screen sharing. The first time users initiate a sharing session, they will be prompted to download the required sharing plug-in.

Supported Operating System and Browser Combinations for Lync Web App

Operating system	32-bit Internet Explorer 10	64-bit Internet Explorer 10	32-bit Internet Explorer 9	64-bit Internet Explorer 9	32-bit Internet Explorer 8	64-bit Internet Explorer 8	32-bit Version of Firefox 12.X	64-bit Version of Safari 5.X	32-bit Version of Chrome 18.x
Windows 8 (Intel based)[1]	Yes	Yes	N/A	N/A	N/A	N/A	Yes	N/A	Yes
Windows 7 with SP1[2]	Yes[3]	Yes[3]	Yes	Yes	Yes	Yes	Yes	No	Yes
Windows Vista with Service Pack 2 (SP2)[4]	N/A	No	Yes	No	Yes	No	Yes	No	Yes
Windows XP with Service Pack 3 (SP3)[4]	N/A	N/A	N/A	N/A	Yes	No	Yes	No	Yes
Windows Server 2008 R2 with SP1[2]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Windows Server 2008 with SP2[4]	Yes	No	Yes	No	Yes	No	Yes	No	Yes

Mac OS-x (Intel-based)[2]	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes

[1] The plug-in required to use computer-based audio, video, application viewing, application sharing, desktop viewing, and desktop sharing can be installed only if you're running Internet Explorer 10 for the desktop. These features are not available with Internet Explorer 10 (non-desktop).

[2] On supported Windows 7, Windows Server 2008 R2, and Macintosh operating systems, all features are available including computer-based voice, video, application viewing, application sharing, desktop viewing, and desktop sharing. To use these features, you must install a plug-in when prompted.

Note:

Macintosh operating systems do not support application sharing. Consequently, Lync Web App will not support application sharing with Macintosh operating systems.

[3] This combination will be supported when available.

[4] On supported Windows XP, Windows Vista, and Windows Server 2008 operating systems, computer-based voice and video are not available. Application viewing, application sharing, desktop viewing, and desktop sharing are available.

1.3.15.1.3.5 Lync Windows Store App Requirements

Lync Windows Store App Requirements

See Also

Planning for Clients and Devices in Lync Server 2013 > Planning for Clients > Client System Requirements >

Topic Last Modified: *2013-02-20*

Organizations with an on-premises deployment of Lync Server must meet the following requirements to support Lync Windows Store app.

Note:

For Lync Server 2010, run the cumulative update for Lync Server 2010: February 2012 (available at http://go.microsoft.com/fwlink/?linkid=3052&kbid=2670352) or later on all servers. To enable users to join meetings, run the cumulative update for Lync Server 2010: October 2012 (available at http://go.microsoft.com/fwlink/?linkid=3052&kbid=2737915) on the servers.

- Enable the Autodiscover, Lync Web App, and Web Ticket services on the server.
- Enable certificate authentication on the Registrar.
- Publish the DNS alias (CNAME) resource records for the Autodiscover service.
- Make sure the Certificate Revocation List (CRL) Distribution Point (CDP) for the certificates issued to Lync server points to an HTTP resource instead of an LDAP resource.
- Configure HTTP proxies in the enterprise to allow Lync server related HTTP traffic. Add exceptions for the Autodiscover, Lync Web App, and WebTicket services, if necessary.

If your organization subscribes to Lync Online or Office 365 and you are using your own domain name, you must take some extra steps to set up your network for autodiscovery of the Lync servers. The network configuration requirements are the same for Lync Windows Store app and Lync on mobile devices. Follow the instructions “Set up your network” in the Office 365 wiki article “Set up Lync mobile devices,” available at http://go.microsoft.com/fwlink/?LinkId=271822.

Concepts

Deploying Lync Windows Store App

1.3.15.1.4 Client Policies and Settings

Client Policies and Settings

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Clients >

Topic Last Modified: *2012-06-18*

This topic provides an overview of the client-related settings and policies that you can configure in Lync Server 2013. Lync Server 2013 includes the following tools for managing and configuring clients:

- **Lync Server 2013 Control Panel** A web-based graphical user interface for managing and configuring servers, users, clients, and devices.
- **Lync Server Management Shell** A management interface with a rich set of Windows PowerShell command-line interface cmdlets and a number of pre-defined scripts.
- **Lync 2013 Group Policy** A set of policies that you can configure for clients by using the Office Group Policy Administrative Template. Certain client bootstrapping policies must be configured before you deploy Lync 2013 clients. Other optional settings from Lync 2010 continue to be honored in Lync 2013.

This section describes changes to client-related settings in Lync Server 2013.

In this Section

- New and Changed Settings for Lync 2013
- Group Policy Settings for Lync 2013

1.3.15.1.4.1 New and Changed Settings for Lync 2013

New and Changed Settings for Lync 2013

Planning for Clients and Devices in Lync Server 2013 > Planning for Clients > Client Policies and Settings >

Topic Last Modified: *2012-12-04*

This topic discusses changes to Lync Server Management Shell cmdlets that relate directly to client management. Lync Server 2013 introduces several new parameters, and deprecates parameters for features that can be configured through other means.

New Client Management Parameters

New	Lync Server Management Shell Cmdlet	Description

TracingLevel	CsClientPolicy	When set to True, software tracing will be enabled in Lync; when set to False, software tracing will be disabled. Software tracing involves keeping a detailed record of everything that a program does (including tracking API calls). Tracing is mostly useful to developers and to application support personnel.This setting is equivalent to the Communications Server 2007 R2 Group Policy setting "Turn on tracing for Communicator." The settings are as follows: • Off = Tracing is disabled and the user cannot change this setting. • Light = Minimal tracing is performed, and the user cannot change this setting. • On = Verbose tracing is performed, and the user cannot change this setting. By default TracingLevel is set to a null value. That means that minimal tracing is performed, but the user can enable or disable this minimal tracing.
EnableMediaRedirection	CsClientPolicy	When set to True ($True) allows audio and video streams to be separated from other network traffic, In turn, this allows client devices to do encoding and decoding of audio and video locally. Media redirection typically results in lower bandwidth usage, higher server scalability, and a more-optimal user experience compared to similar techniques such as device remoting or codec compression.
AllowLargeMeetings	CsConferencing	When set to True, all Lync Meetings are treated as "large meetings." With a large meeting, restrictions are placed on the number of notifications that are sent to participants, in addition to the size of the meeting roster that is transmitted by default.
DisablePowerPointAnnotations	CsConferencing	When set to True ($True) users won't be able to add annotations to PowerPoint slides used in a conference. However (depending on the value of the AllowAnnotations property), users will still have access to other whiteboarding features. The default value is False, meaning that PowerPoint annotations are allowed.
AllowSharedNotes	CsConferencing	When set to True (the default value)

		any open OneNote notebooks linked to the conference will automatically be updated with information such as conference participants and details about content shared during the conference.
EnableInviteCustomization	CsMeetingConfiguration	Used along with the other new CsMeetingConfiguration parameters to customize the meeting invitations generated by the Online Meeting Add-in for Lync 2013.
LogoURL	CsMeetingConfiguration	Adds your organization’s logo to all invitations generated by the Online Meeting Add-in for Lync 2013. You specify the URL of a GIF or JPG image.
HelpURL	CsMeetingConfiguration	Adds your organization’s help or support URL to all invitations generated by the Online Meeting Add-in for Lync 2013.
LegalURL	CsMeetingConfiguration	Adds legal text or disclaimer text to all invitations generated by the Online Meeting Add-in for Lync 2013. You specify the URL for the location of the text.
CustomFooterText	CsMeetingConfiguration	Adds a custom footer to all invitations generated by the Online Meeting Add-in for Lync 2013. You specify the URL for the location of the custom footer text.

Deprecated Client Management Parameters

Parameter	**Lync Server Management Shell Cmdlet**	**Description**
EnableSQMData	CsClientPolicy	The EnableSQMData parameter of the Set-CSClientPolicy cmdlet has been removed in Lync Server 2013. Instead, you can use the shared Group Policy setting for Software Quality Management (SQM) data to determine the user interface for the Customer Experience Improvement option in the Lync client General options page: HKEY_CURRENT_USER \Software\Policies\Microsoft \Office\Common\QMEnable Values: 1 = Display and select the check box (the user can clear

		the check box) 0 = Turn off and disable the check box (user can't override) Null = The value is determined by Office setup, and the check box is displayed for users to set as they choose
AllowExchangeContactStore	CsClientPolicy	This parameter has been removed. Instead, when you deploy Lync Server 2013 and publish the topology, unified contact store is enabled for all users by default. This means that all a user's contacts are kept in Exchange and are available in Lync, Outlook, and Outlook Web Access. You can use the Set-CsUserServicesPolicy cmdlet to customize which users have unified contact store available. You can enable users globally, by site, by tenant, or by individuals or groups of individuals. For details, see Enable Users for Unified Contact Store.
MAPIPollInterval	CsClientPolicy	This parameter is not used by Lync 2013. In previous releases, this parameter specified how often the client retrieved MAPI data from Exchange public folders

1.3.15.1.4.2 Group Policy Settings for Lync 2013

Group Policy Settings for Lync 2013

Planning for Clients and Devices in Lync Server 2013 > Planning for Clients > Client Policies and Settings >

Topic Last Modified: *2012-10-03*

In previous versions of Lync and Office Communicator, a stand-alone Communicator.adm administrative template was available for configuring client Group Policy settings. For Lync 2013, new administrative template files (.admx and .adml files) are included along with the Office Group Policy Administrative Template. The availability of Lync 2013 .admx and .adml files allows you to download templates and centrally manage Group Policy settings for all your Office programs and language packs. For details, see “Office 2013 Administrative Template files (ADMX, ADML)” in the Office 2013 documentation at http://

go.microsoft.com/fwlink/p/?linkid=267516.

Client Bootstrapping Policies

There are several client bootstrapping policies that you should configure before users sign in to the server for the first time. Because these policies take effect before the client signs in and begins receiving in-band provisioning settings from the server, you can use Group Policy to configure them. For more information, see Configuring Client Bootstrapping Policies in the Deployment documentation.

1.3.15.1.5 Lync 2013 Compatibility

Lync 2013 Compatibility

See Also

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Clients >

Topic Last Modified: *2013-02-20*

This section describes the compatibility of Lync 2013 with various versions of Microsoft Office suites, Microsoft Exchange Server, Windows operating systems, and selected public instant messaging (IM) clients.

Office and Lync 2013

The following table describes the Lync 2013 features that are supported by various versions of Office.

Lync 2013 and Microsoft Office Compatibility

Feature	Microsoft Office 2003 with Service Pack 3 (SP3) (required) or the latest service pack (recommended)	Microsoft Office 2007	Microsoft Office 2010	Microsoft Office 2013
Customize Outlook meeting invitations (add logo, help URL, disclaimer, footer text)	No	No	No	Yes
In Outlook, configure meeting option to mute attendee audio and video by default	No	No	No	Yes
Unified Contact Store for managing	No	No	No	Yes (requires Exchange 2013)[1]

Contacts lists across Office and Lync				
High-resolution pictures	No	No	No	Yes (requires Exchange 2013)[1]
Lync 2013 setup integrated into the Office setup program	No	No	No	Yes
OneNote shared notes	No	No	No	Yes
PowerPoint 2013 presentation content	Yes	Yes	Yes	Yes
Presence status in the Microsoft Outlook To and Cc fields	Presence status appears on hover	Presence status is always shown	Presence status is always shown	Presence status is always shown
Reply with conference call from the availability menu	No	Yes	Yes (from the contact card)	Yes (from the contact card)
Presence status in a meeting request on the Scheduling Assistant tab	No	Yes	Yes	Yes
Reply with IM, or call from the toolbar or ribbon in a received email message	No	Yes	Yes	Yes
Presence status in the Outlook From field	Yes	Yes	Yes	Yes
Reply with IM or voice from availability menu	Yes	Yes	Yes (from the contact card)	Yes (from the contact card)
IM and presence in Microsoft Word and Microsoft Excel files (smart tags enabled)	Yes	Yes	Microsoft Word only	Microsoft Word only
IM and presence in Microsoft SharePoint sites (Outlook must be installed)	Yes	Yes	Yes	Yes

[1] For more information, see Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 in the Planning documentation.

The following features are available only with Office 2010 or Office 2013:

- Contact card with expanded options, such as video call and desktop sharing
- Quick search from the Find a Contact field in Outlook
- Reply with an IM or call from the Outlook Home ribbon in the Mail, Calendar, Contacts, and Tasks folders
- Lync Contacts list in Outlook To-Do Bar
- Office Backstage (File tab) presence status, program sharing, and file transfer
- Presence menu in Microsoft Office SharePoint Workspace 2010 (formerly Microsoft Office Groove 2007)
- Presence menu extensibility

Exchange Server and Lync 2013

The following table describes Lync 2013 support for various versions of Exchange Server. Outlook must be installed on the client computer to handle Extended MAPI calls, and some features require the use of Exchange Web Services (EWS).

Lync 2013 and Exchange Server Compatibility

Exchange Server version	Lync 2013 support
Exchange Server 2013	Same as Exchange Server 2010 support, with the addition of Unified Contact Store, high-resolution pictures, and archiving integration. **Note:** For details, see Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013.
Exchange Server 2010	Same as Exchange Server 2007 support, with the addition of Exchange contact sync.
Exchange Server 2007 with Service Pack 1 (SP1) (required) or the latest service pack (recommended)	The following features are available only through EWS: • Read or delete items in the Conversation History folder • Read or delete voice mail items • Display extended free/busy information and meeting subject and location Public folders are optional in Exchange Server 2007 with Service Pack 1 (SP1) (required) or the latest service pack or release (recommended).
Exchange Server 2003	Outlook MAPI only. EWS-only features are not available (see the previous row).

Windows and Lync 2013

For information about Lync 2013 and Windows supportability, see Lync Client Software Support in the Planning documentation.

Macintosh and Lync 2013

Lync Server 2013 supports certain clients on computers that are running Macintosh operating systems. For details, see Lync Client Software Support in the Planning documentation.

Public Instant Messaging Clients and Lync 2013

If you have configured your server for public IM connectivity, Lync supports the following capabilities with public IM networks. Presence status is filtered to those presence states supported by the public IM client. For details, see Planning for Public Instant Messaging Connectivity in the Planning documentation and Manage External Access Policy for Your Organization in the Operations documentation.

In addition, the XMPP integration feature of Lync Server 2013 lets users exchange instant messages and presence information with users of public IM providers that use Extensible Messaging and Presence Protocol, such as Google Talk. For details, see Planning for Extensible Messaging and Presence Protocol (XMPP) Federation in the Planning documentation.

Lync 2013 and Public IM Clients Compatibility

Client	Supported Capabilities
Windows Live Messenger	IM, basic presence, audio/video (A/V)*
AOL	IM and basic presence
Yahoo!	IM and basic presence
Google Talk	IM and basic presence

*A/V is supported with the latest version of Windows Live Messenger. If you are implementing audio/video (A/V) federation with Windows Live Messenger, you must also modify the server encryption level. By default, the encryption level is Required. You must change this setting to Supported by using the Lync Server Management Shell.

Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

See Also

Concepts

Client Interoperability in Lync 2013
Lync Client Software Support
Lync Web App Supported Platforms
Lync Windows Store App Requirements

Other Resources

Client System Requirements

1.3.15.1.6 Client Interoperability in Lync 2013

Client Interoperability in Lync 2013

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Clients >

Topic Last Modified: *2013-01-11*

This topic discusses the ability of Microsoft Lync Server 2013 clients to coexist and interact with clients from earlier versions of Lync Server and Office Communications Server.

Server and Client Compatibility

The following table shows the supported combinations of client versions and server versions. This table indicates whether sign-in is supported when the client attempts to connect to the server indicated. Lync Server 2013 supports the previous client version. Also, unlike previous releases, Lync Server 2010 supports the new Lync 2013 clients. This allows organizations who are upgrading from Lync Server 2010 to roll out new clients independent of Lync Server upgrades.

Client	Lync Server 2013	Lync Server 2010	Office Communications Server 2007 R2
Lync 2013	Supported	Supported	Not Supported
Lync Web App 2013	Supported	Not Supported	Not Supported
Lync 2010	Supported	Supported	Not Supported
Lync 2010 Attendant	Supported	Supported	Not Supported
Lync 2010 Group Chat	Not Applicable	Supported[1]	Not Applicable
Lync Web App 2010	Not Supported	Supported	Not Supported
Lync 2010 Attendee	Not Supported[2]	Supported	Not Supported
Office Communicator 2007 R2	Interoperable[3]	Supported	Supported
Microsoft Office Communications Server 2007 R2 Attendant	Not Supported	Supported	Supported
Office Communicator 2007	Not Supported	Supported	Supported
Office Live Meeting 2007	Not Supported	Supported	Supported

[1] In Microsoft Lync Server 2010, group chat functionality was available with Group Chat Server, a third-party trusted application for Lync Server 2010. Lync 2013 clients are not compatible with Lync Server 2010, Group Chat.

[2] Lync Web App 2013 now provides a full in-meeting experience, including computer audio and video, and is considered the replacement for Lync 2010 Attendee.

[3] The presence and IM features in Office Communicator 2007 R2 are compatible with Lync Server 2013, but conferencing features are not. During migration from Office Communications Server 2007 R2, Office Communicator 2007 R2 is suitable for presence and IM interoperability, but users should use Lync Web App 2013 to join Lync Server 2013 meetings.

Interoperability among Clients

With the Lync Server 2013 release, various client versions can interact seamlessly in both peer-to-peer and conferencing scenarios. This section discusses feature availability when users interact with other users who are using different versions of clients and servers.

Peer-to-Peer Feature Support

Peer-to-peer features are supported for users who are homed on different versions of the server and who are using different client versions. The end-user experience and available features are consistent with the capabilities of the user's client and the version of the server the user is signed in to. In other words:

- If a user is signed in to Lync Server 2013 with an older client, the user will have the same experience he or she is used to. None of the new features introduced in Lync Server 2013 will be available until the user's client is upgraded.
- If a user is signed in to Lync Server 2010 with a Lync 2013 client, any new features not supported by Lync Server 2010 will be unavailable until the user is moved to Lync Server 2013.

The following table compares feature availability in peer-to-peer sessions where the client is signed in to either Lync Server 2013 or Lync Server 2010.

Note:

Lync Web App and Lync 2010 Attendee are meeting-only clients and aren't included in this table.

Client	Instant Messaging	Presence	Voice	Video	Application Sharing	File Transfer
Lync 2013	Yes	Yes	Yes	Yes	Yes	Yes
Lync 2010	Yes	Yes	Yes	Yes	Yes	Yes
Lync 2010 Attendant	Yes	Yes	Yes			
Lync 2010 Mobile	Yes	Yes				
Lync Phone Edition	Yes	Yes	Yes			
Office Communicator 2007 R2	Yes	Yes	Yes	Yes	Yes[1]	Yes
Public IM (AOL, Yahoo!)	Yes	Yes				
Public IM	Yes	Yes	Yes	Yes		

(MSN, Windows Live Messenger)						

Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

[1] In Office Communicator 2007 R2, only desktop sharing (and not program sharing) is available.

Conferencing Feature Support

In Lync Server 2013 meetings, conferencing features are supported for users who are homed on different versions of the server and who are using different clients and client versions. When clients join a Lync Server 2013 meeting, users have access to the features and capabilities shown in this table.

Client	Peer-to-peer IM	Voice	Video	Application Sharing	PowerPoint	File Transfer	Whiteboard	Polling
Lync 2013	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Lync Web App	Yes	Yes	Yes	Yes	Yes[2]	Yes	Yes	Yes
Lync 2010	Yes	Yes	Yes	Yes	Yes[3]	Yes	Yes	Yes
Office Communicator 2007 R2	Yes	Yes	Yes	Yes[1]		[4]		

[1] In Office Communicator 2007 R2, only desktop sharing (and not program sharing) is available.

[2] Lync Server 2013 uses an updated mechanism for uploading PowerPoint files. Lync Web App users who join a meeting that was originally scheduled on Lync Server 2010 can view and navigate PowerPoint presentations, but cannot upload PowerPoint files.

[3] If the meeting was scheduled on Lync Server 2013 and PowerPoint slides were uploaded by a Lync 2013 client, Lync 2010 users have view-only access to the slides.

[4] In Office Communicator 2007 R2, file transfer is supported in peer-to-peer sessions, but not in conferencing sessions.

Scheduling Add-in Support

Server support for the various scheduling add-ins is consistent with server and client version compatibility. In general, the following scheduling add-ins are supported on Lync Server 2013. However, previous versions of add-ins do not provide new Lync 2013 add-in features, such as the option to mute all attendee audio and video upon meeting entry.

- **Online Meeting Add-in for Lync 2013** Provides the same features as the Online Meeting Add-in for Lync 2010, with the addition of attendee mute controls, which allow meeting organizers to schedule conferences that have attendee audio and video muted by default. Administrators can also customize the organization’s meeting invitations by adding a custom logo, a support URL, a legal disclaimer URL, or custom footer text.
- **Online Meeting Add-in for Lync 2010** Provides scheduling for Lync meetings and removes the capability to schedule Office Live Meeting conferences.
- **Office Communicator 2007 R2 Conferencing Add-in** Provides scheduling for both Office Live Meeting conferences and Office Communicator 2007 R2 conferences.

Note:

Live Meeting conferences cannot be scheduled on Lync Server 2013.

Scheduling Client	Lync Server 2013	Lync Server 2010	Office Communications Server 2007 R2
Online Meeting Add-in for Lync 2013 (can be used with Office 2013, Outlook 2010, and Outlook 2007)	Supported	Supported (new add-in features not available)	Not Supported
Lync 2013 Web Scheduler	Supported	Not Supported	Not Supported
Online Meeting Add-in for Lync 2010	Supported	Supported	Not Supported
Office Communicator 2007 R2 Conferencing Add-in	Not Supported	Supported	Supported

Support for Joining Meetings

All of the clients that Lync Server 2013 supports are allowed to join Lync 2013 meetings. Because Lync Web App is a web component of the server, in cases where Lync Web App is used to join a Lync Server 2013 meeting, the newer version of Lync Web App is always used.

Lync 2013 clients can join meetings hosted on Lync 2010 and Office Communications Server 2007 R2 with scaled-down functionality. In-meeting features are limited by the version of the server on which the meeting is hosted.

1.3.15.2 Planning for Mobile Clients

Planning for Mobile Clients

Microsoft Lync Server 2013 > Planning > Planning for Clients and Devices in Lync Server 2013 >

Topic Last Modified: *2013-02-19*

Lync 2013 mobile clients provide enhanced presence, IM, Lync meetings, and voice and video calls over the Internet or the cellular connection. For a matrix that lists the features and capabilities of mobile clients and compares them to the desktop client, see Mobile Client Comparison Tables.

Note:

Lync Server 2013 also supports Lync 2010 mobile clients. For more information, see "Planning for Mobile Clients" in the Lync Server 2010 TechNet Library at http://go.microsoft.com/fwlink/p/?LinkID=235955.

- Mobile Client Comparison Tables
- Lync for Windows Phone Requirements
- Lync for iPhone and iPad Requirements
- Mobile Client Deployment Process

1.3.15.2.1 Mobile Client Comparison Tables

Mobile Client Comparison Tables

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Mobile Clients >

Topic Last Modified: *2013-03-12*

The following tables compare the features and capabilities among Lync 2013 mobile clients and the Lync 2013 desktop client in the following categories:

- Sign-in, sign-out, and push notifications
- Enhanced presence
- Contacts and contact groups
- Instant messaging (IM)
- Lync-to-Lync audio and video
- Conferencing
- Telephony
- External users
- Archiving and compliance

These tables indicate the features that are available to Lync users in an on-premises deployment of Lync Server 2013. The same features are also available to Lync Online and Microsoft Office 365 users, unless otherwise indicated in the table footnotes.

Note:

- For online help and resources for end users, see "Microsoft Lync 2013 for Mobile Clients" at http://go.microsoft.com/fwlink/?LinkId=286237.
- To compare the features available in other Lync 2013 clients, see Client Comparison Tables.
- Lync Server 2013 also supports Lync 2010 mobile apps. For details, see "Mobile Client Comparison Tables" in the Lync Server 2010 documentation at http://go.microsoft.com/fwlink/p/?LinkID=234777.

Sign-in and Push Notifications

Feature/	Lync 2013	Windows Phone	iPhone	iPad

Capability	desktop client			
Lync session remains signed in	?	?[1]	?[1]	?[1]
Support for push notifications		?		
Country code populates based on region settings			?	?
Account information for multiple users can be cached on the same device	?			

[1] On Windows Phone, Lync signs out automatically if the user has not used the application for a period of time, as follows:

- If the user has enabled push notifications, Lync signs out after 36 hours.
- If the user has not enabled push notifications, Lync signs out after 1 hour.

On iPhone and iPad, Lync signs out automatically if the user has not used the application for a period of time, as follows:

- If the mobile client has not contacted the server for 10 days due to loss of network connectivity or other issues.

Enhanced Presence Support in Lync Mobile Clients

Feature/ Capability	Lync 2013 desktop client	Windows Phone	iPhone	iPad
Publish and view status	?	?	?	?
View status based on calendar free/ busy information	?	?	?	?
View status notes and Out of Office messages	?	?	?	?
Add a custom location	?			
Add a custom note	?	?	?	?
Publish status based on calendar free/ busy information	?[1]			
Set manual presence state	?	?	?	?

(such as Busy, Do Not Disturb, and so on)				

[1] Lync mobile clients do not update a user’s presence based on the user’s free/busy calendar information. If a mobile client user is also signed in to the Lync desktop client, the desktop client updates the user’s presence based on the user’s free/busy calendar information. If the user is signed in to a mobile client only, the user’s presence does not update based on free/busy calendar information.

Contacts and Contact Groups Support in Lync Mobile Clients

Feature/ capability	**Lync 2013 desktop client**	**Windows Phone**	**iPhone**	**iPad**
View Contacts list	?	?	?	?
View contact groups	?	?	?	?
View Frequent Contacts group	?			
Modify Contacts list	?			
Tag contacts for status change alerts	?			
Control privacy relationships	?			
Search the corporate address book	?	?	?	?
Search Contacts list	?	?	?	?
Manage contact groups	?			
Expand distribution groups	?	?	?	?
Search for Response Groups	?[1]	?	?	?
Display or hide contact photos	?	?	?	?

[1] Not available to Lync Online and/or Office 365 users.

Instant Messaging Support in Lync Mobile Clients

Feature/ capability	Lync 2013 desktop client	Windows Phone	iPhone	iPad
Initiate instant messaging (IM) with a contact	?	?	?	?
Participate in multiparty IM	?	?[1]	?[1]	?[1]
Invite others from within the conversation window	?			
Display current conversations	?	?	?	?
Navigate among multiple IM conversations	?	?	?	?
Automatically log IM conversations in Exchange	?			
Send an IM conversation as an email message	?	?	?	?
Initiate an email to a contact	?	?	?	?
View missed IM invitations	?	?	?	?
Vibrate with incoming IM		?[2]	?	?
Send location in an IM				

[1] Mobile users cannot initiate multiparty IM or add users to an existing IM, but they can participate in multiparty IM if invited.

[2] This device vibrates every time an IM is received even if the current message in the IM conversation is displayed

Lync-to-Lync Audio and Video

Feature/ Capability	Lync 2013 desktop client	Windows Phone	iPhone	iPad

Lync-to-Lync voice	?	?	?	?
Lync-to-Lync video	?	?	?	?

Conferencing Support in Lync Mobile Clients

Feature/ Capability	**Lync 2013 desktop client**	**Windows Phone**	**iPhone**	**iPad**
Click a link in the meeting reminder to join a meeting (public switched telephone network (PSTN))	?	?[1]	?[1]	?[1]
Click a link in the meeting reminder to join a video or VoIP meeting	?	?	?	?
Participate in multiparty IM	?	?	?	?
Use dial-out conferencing (server calls the mobile device)	?	?[2]	?[2]	?[2]
Use dial-in audio conferencing	?[3]			
View meeting video	?	?	?	?
View multiparty video (gallery view)	?			
Wait in meeting lobby	?	?	?	?
Use in-meeting presenter controls	?			
Access detailed meeting roster for audio conferences	?	?	?	?
Access detailed meeting roster for IM conferences	?	?	?	?

Share desktop or program	?			
View shared desktop or program	?			?
View shared PowerPoint	?			?
Use meeting tools (present Microsoft PowerPoint files, use whiteboard, conduct polls, share files)	?			
Navigate a list of your meetings		?	?	?

[1] For Office 365 users, this feature is available for audio conferencing provider (ACP)-enabled meetings only.

[2] Not available to Office 365 users.

[3] For Lync Online and/or Office 365 users, this feature is available from third-party audio conferencing providers.

Telephony Support in Lync Mobile Clients

Feature/ Capability	Lync 2013 desktop client	Windows Phone	iPhone	iPad
In Lync, tap the call icon to call a contact	?[1]	?[2]	?[2]	?[2]
Transfer a call	?[1]			
Manage call forwarding	?[3]	?	?	?
Manage team call settings	?[3]			
Manage delegates	?[3]			
Initiate a call to a Response Group	?[3]			
Support emergency services	?[4]			
Make calls on behalf of another contact	?[3]			

(manager/ delegate scenario)				
Handle another contact's calls, if configured as a delegate	?[3]	?[3]	?[3]	?[3]
Use Call via Work (Lync Server 2013 places your outgoing calls so that the receiver's caller ID displays your work number instead of your mobile number)		?[3]	?[3]	?[3]
Access voice mail	?[4]	?	?	?
Use the keypad in Lync	?	?[3]	?[3]	?[3]

[1] For Lync Online and/or Office 365 users, this feature is available for PC to PC calls. PSTN calls are supported by Lync to phone mobile partners.

[2] For on-premises Lync Server 2013 users, on Windows Phone, iPhone, and iPad devices, the user taps the call icon in the contact card and accepts the callback from Lync Server 2013. For Office 365 users, on Windows Phone, iPhone, and iPad devices, when the user taps the call button, a dialog box opens asking the user to confirm that he or she wants to call the number.

[3] Not available to Lync Online and/or Office 365 users.

[4] For Lync Online and/or Office 365 users, this feature is supported by Microsoft partners.

External User Support in Lync Mobile Clients

Feature/ Capability	Lync 2013 desktop client	Windows Phone	iPhone	iPad
Initiate IM with a public contact	?	?	?	?
Initiate IM with a federated contact	?	?	?	?
Conduct two-party calls with external users	?			
Conduct multiparty calls	?			

with external users				
Use Call via Work to reach a federated contact on their mobile phone by calling their published work number[1]		?[2]	?[2]	?[2]

[1] By default, federated users are assigned the External Contacts privacy relationship. To be able to reach a federated contact on their mobile phone by calling their published work number, the federated contact must manually assign you the Colleagues privacy relationship.

[2] Not available to Office 365 users.

Archiving and Compliance Support in Lync Mobile Clients

Feature/ Capability	**Lync 2013 desktop client**	**Windows Phone**	**iPhone**	**iPad**
Provide client-side archiving	?			
Provide client-side recording	?[1]			

[1] Not available to Lync Online and/or Office 365 users.

1.3.15.2.2 Lync for Windows Phone Requirements

Lync for Windows Phone Requirements

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Mobile Clients >

Topic Last Modified: *2013-02-20*

Microsoft Lync 2013 for Windows Phone provides instant messaging (IM), enhanced presence, and telephony for users in your organization who are connecting from a smartphone or a Windows Professional mobile device. Mobile devices enable users to extend the reach of Lync 2013. This topic describes planning considerations for Lync 2013 for Windows Phone that include identifying prerequisites and technical requirements, required components, and deployment guidance.

Lync for Windows Phone Prerequisites

Following are the Lync 2013 for Windows Phone prerequisites.

- Windows Phone 8, codenamed "Apollo," or the latest version.
- The Windows Phone device must have the latest updates available from Microsoft. For details, see Windows Phone 8 update history at http://go.microsoft.com/fwlink/p/?LinkID=281961.
- The device must have 12 MB of available disk space.
- The user must have a voice and data plan from a carrier.

1.3.15.2.3 Lync for iPhone and iPad Requirements

Lync for iPhone and iPad Requirements

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Mobile Clients >

Topic Last Modified: *2013-02-20*

To support Microsoft Lync 2013 for iPhone or Microsoft Lync 2013 for iPad, the device must meet the following requirements:

- iPhone 4 mobile digital device with Apple iOS 6 or the latest version.
- iPad 2 or a later version mobile digital device with Apple iOS 6 or the latest version.
- iPad mini mobile digital device with Apple iOS 6 or the latest version.

1.3.15.2.4 Mobile Client Deployment Process

Mobile Client Deployment Process

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Mobile Clients >

Topic Last Modified: *2013-02-20*

After a deployment of Microsoft Lync Server 2013 has been completed, users can install the Lync 2013 app from the mobile marketplace that they are accustomed to using for their specific device.

Lync Mobile Deployment Process

Phase	Steps	Permissions	Documentation
Perform pre-setup tasks.	1. Verify Lync Server 2013 deployment. 2. Verify certificate requirements.	Administrator	Planning for Mobility in the server planning documentation. Deploying Mobility in the server deployment documentation. Certificate Infrastructure Requirements in the server planning documentation.
Install the Lync	1. Install prerequisites.	Administrator	Installation

application on a test device.	2. Install from the marketplace specific to the mobile device.		instructions specific to the mobile device in Deploying Mobile Clients.
Configure the client.	• Configure sign-in settings and server information.	Administrator	Deploying Mobile Clients
Test mobile scenarios.	1. Test instant messaging (IM) and presence. 2. Test dial-out conferencing. 3. Search for a contact in the corporate directory. 4. Test push notifications.	Administrator	Verification instructions specific to the mobile device in Deploying Mobile Clients.
Install the Lync application on mobile phones.	1. Install prerequisites. 2. Install from the marketplace specific to the mobile device.	User	Installation instructions specific to the mobile device in Deploying Mobile Clients.

1.3.15.3 Planning for Devices

Planning for Devices

See Also

Microsoft Lync Server 2013 > Planning > Planning for Clients and Devices in Lync Server 2013 >

Topic Last Modified: *2013-02-28*

Lync Server 2013 includes Lync Phone Edition, software that runs on qualified devices and provides traditional and advanced telephony features, integrated security, manageability, and more. Lync Phone Edition works the same way with Lync Server 2013 as it does with Lync Server 2010. For details about planning for devices, see Planning for Devices in the Lync Server 2010 TechNet Library.

Other Resources

Deploying Devices
Client and Device Software and Infrastructure Support

1.3.15.3.1 Supported Devices

Supported Devices

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Devices >

Topic Last Modified: *2012-10-08*

Lync Server supports all of the phones listed in the following table. Note that not all of the supported phones can run Lync Phone Edition (some can run only earlier versions). Use the table to learn which phones can run Lync Phone Edition and where to get detailed information about all of the supported phones.

Note:

Three types of phones are supported: desk phones (handset IP or USB devices that are designed to be used by employees at their desk), conferencing devices (hands-free IP or USB phones that are designed to be used in meeting rooms), and common area phones (IP phones that are designed to be used in shared areas—such as lobbies, kitchens, factory floors, and shared workspaces—and can be customized to provide different sets of Lync Phone Edition features.

For detailed comparison tables about all devices that are optimized to work with Lync, see "Phones and Devices Qualified for Microsoft Lync" at http://go.microsoft.com/fwlink/p/?linkid=208938. The phone comparison tables at this website include pricing information and technical specifications.

Phone	Runs Lync Phone Edition	Learn More
Aastra 6721ip common area phone	X	Downloads Aastra 6721ip at the Aastra website
Aastra 6725ip desk phone	X	Downloads Aastra 6725ip at the Aastra website
HP 4110 IP Phone (common area phone)	X	HP 4110 IP Phone Series at the HP website
HP 4120 IP Phone (desk phone)	X	HP 4120 IP Phone Series at the HP website
Polycom CX300 USB desk phone		CX300 at the Polycom website
Polycom CX500 IP common area phone	X	CX500 at the Polycom website
Polycom CX600 IP desk phone	X	CX600 at the Polycom website
Polycom CX700 IP desk phone		CX700 at the Polycom website
Polycom CX3000 IP conference phone	X	CX3000 at the Polycom website
Polycom CX5000 USB conferencing device		CX5000 at the Polycom website

Note:
Support for analog devices is also provided. For details, see Planning to Deploy Analog Devices in the Lync Server 2010 TechNet Library. (Lync Phone Edition works the same way in Lync Server 2013 and Lync Server 2010).

1.3.15.3.2 Topologies for IP Phones

Topologies for IP Phones

Planning > Planning for Clients and Devices in Lync Server 2013 > Planning for Devices >

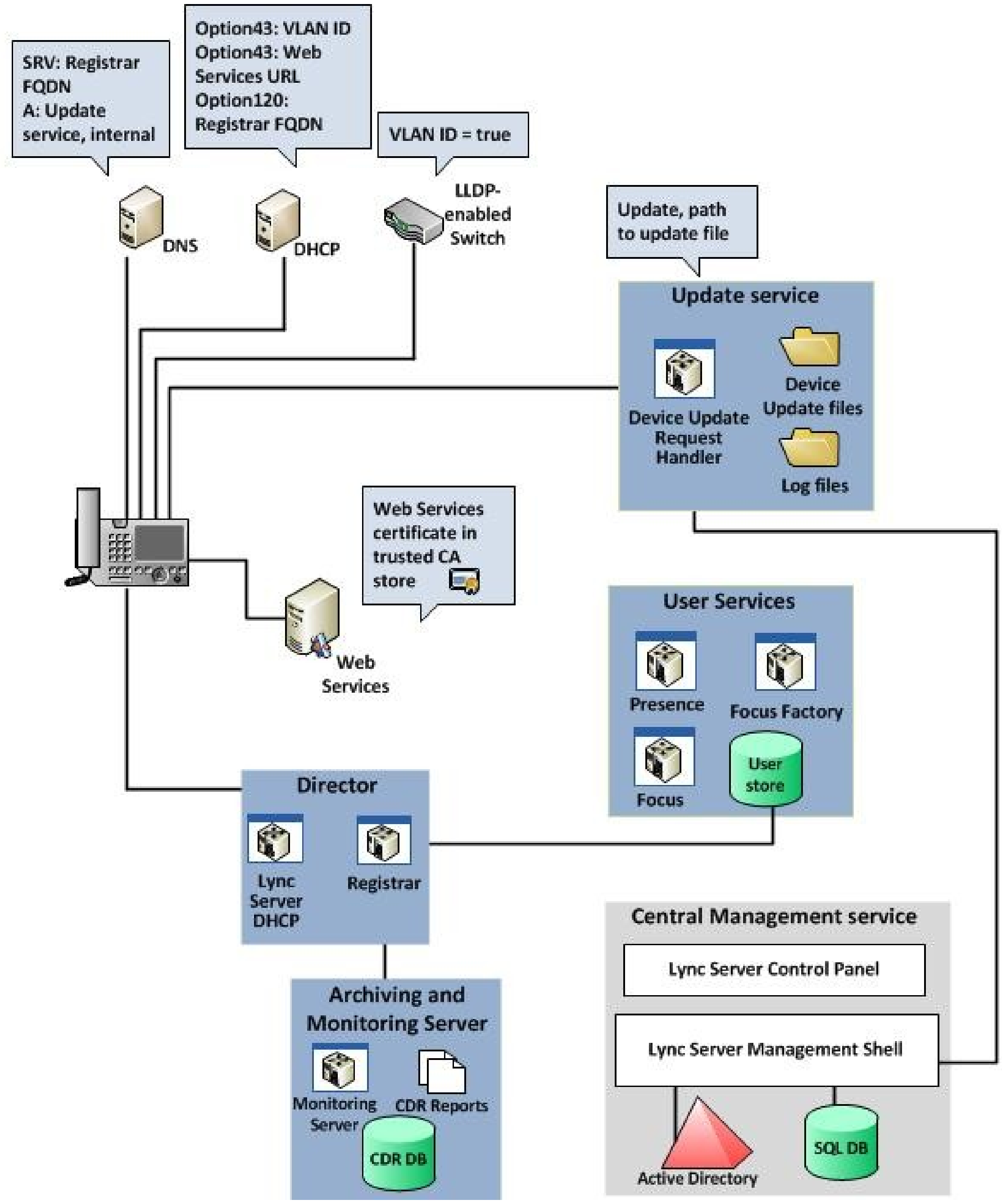
Topic Last Modified: *2012-06-21*

This section provides an overview of the connectivity process and explains the differences between how an IP phone connects in an internal and external network.

Note:

Lync Server provides support for the following IP phones: the Aastra 6721ip common area phone, Aastra 6725ip desk phone, HP 4110 IP Phone (common area phone), HP 4120 IP Phone (desk phone), Polycom CX600 IP desk phone, Polycom CX700 IP desk phone, Polycom CX500 IP common area phone, and Polycom CX3000 IP conference phone. Of those phones, all but the Polycom CX700 can run Lync Phone Edition.

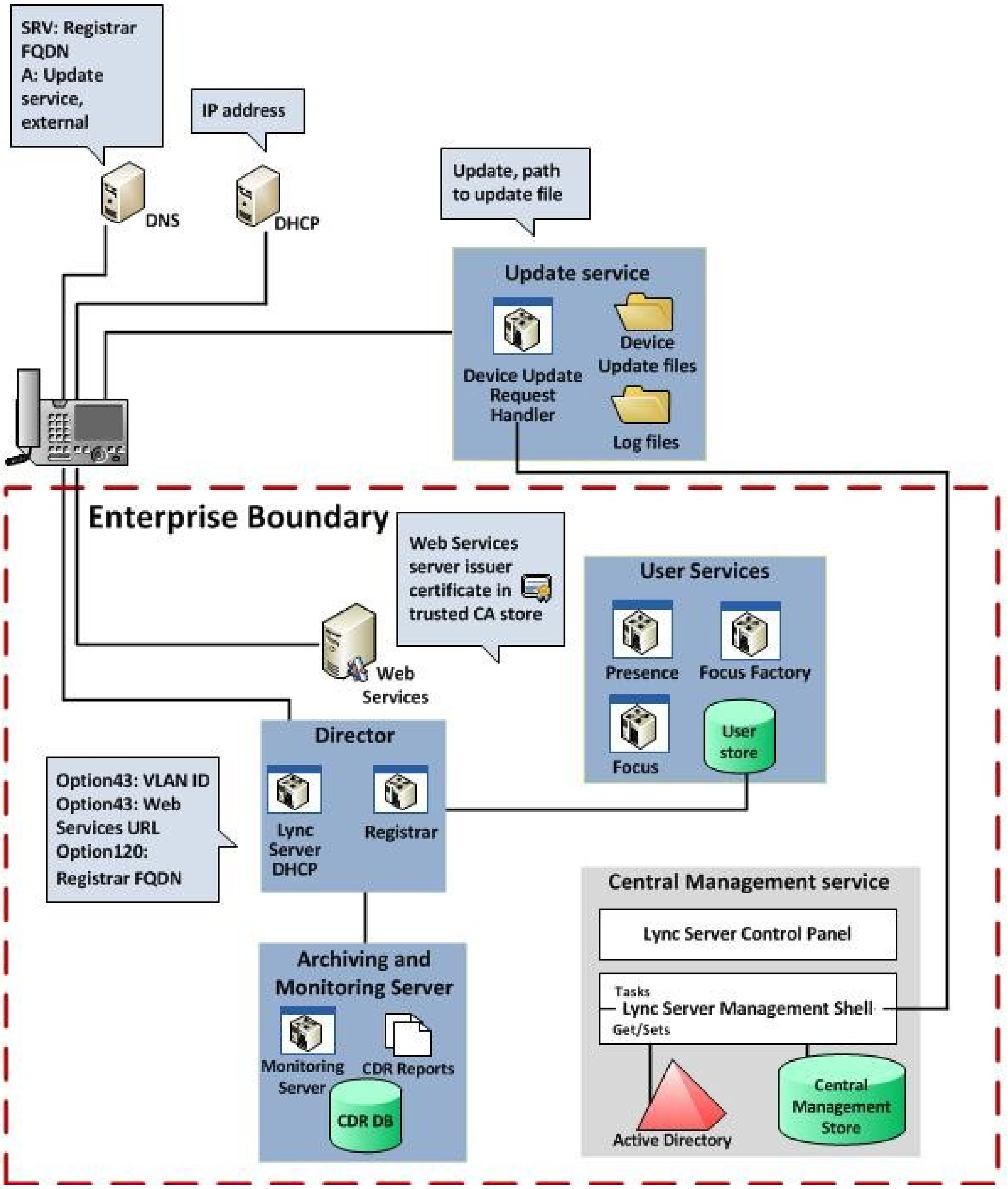
The following diagram describes all the components involved in device connectivity within the corporate environment.


SRV: Registrar FQDN
A: Update service, internal
Option43: VLAN ID
Option43: Web Services URL
Option120: Registrar FQDN
VLAN ID = true
DNS
DHCP
LLDP-enabled Switch
Update, path to update file
Update service
Device Update Request Handler
Device Update files
Log files
Web Services certificate in trusted CA store
Web Services
User Services
Presence
Focus Factory
Focus
User store
Director
Lync Server DHCP
Registrar
Central Management service
Lync Server Control Panel
Lync Server Management Shell
Active Directory
SQL DB
Archiving and Monitoring Server
Monitoring Server
CDR Reports
CDR DB

Note:
The previous figure is a logical representation, not a physical overview. For example, Active Directory Domain Services (AD DS) is rarely located on the same machine as any

Lync Server components. The user store can be located on the Back End Server or on the Archiving and Monitoring Servers. The Lync Server Management Shell, web server, and update services are all part of the Front End Server role.

The following diagram provides an overview of the components involved when the device is located outside the corporate network.


SRV: Registrar FQDN
A: Update service, external
IP address
DNS
DHCP
Update, path to update file
Update service
Device Update Request Handler
Device Update files
Log files
Enterprise Boundary
Web Services server issuer certificate in trusted CA store
Web Services
User Services
Presence
Focus Factory
Focus
User store
Director
Lync Server DHCP
Registrar
Option43: VLAN ID
Option43: Web Services URL
Option120: Registrar FQDN
Central Management service
Lync Server Control Panel
Tasks
Lync Server Management Shell
Get/Sets
Active Directory
Central Management Store
Archiving and Monitoring Server
Monitoring Server
CDR Reports
CDR DB

Note:

The Device Update Web service provides an external and internal website, but only the external one is shown here.
The location of the Registrar and the URL of the Device Update Web service for the organization must be published in DNS if external access is to be enabled. Additionally,

the Edge Server must be deployed and correctly configured to allow external communications from the device to the corporate environment and back. This is omitted from the previous diagram because Edge deployment is not specific to device connectivity.

1.3.16 Planning for Remote Call Control

Planning for Remote Call Control

Microsoft Lync Server 2013 > Planning >

Topic Last Modified: *2012-09-05*

In Lync Server 2013, support for remote call control scenarios enables users to control their private branch exchange (PBX) phones by using Lync 2013 on their desktop computers. This section describes remote call control features and requirements for deploying remote call control.

Integration between a PBX and Lync Server 2013 makes it possible for users enabled for remote call control to use the Lync 2013 user interface (UI) to control calls on their PBX phones in the following ways:

Note:

Ultimately, the capabilities of the PBX that hosts a user's PBX phone determine the remote call control features that will be available to that user.

- Make an outgoing call
- Answer an incoming call
- Answer an incoming call with an instant message

  Note:

  That is, when the caller's phone number can be associated with an instant message address in your organization's global address list (GAL), in the callee's Lync Contacts list, or in a federated partner's organization.
- Transfer a call
- Forward an incoming call
- Place calls on hold
- Alternate between multiple concurrent calls
- Answer a second call while already in a call (that is, call waiting)
- Dial dual-tone multifrequency (DTMF) digits
- In the Conversation window, type notes in Microsoft Office OneNote note-taking program

Additionally, when a user is enabled for remote call control, Lync 2013 provides the user with the following call information:

- Identification of a caller by name when the caller's phone number exists in the Contacts list of a remote call control-enabled user's Microsoft Office Outlook messaging and collaboration client, Lync Contacts list, or your organization's GAL.
- Past incoming and outgoing calls, which are saved in the Conversation History folder in Outlook.
- Missed call notifications, which are sent to the user's Outlook Inbox folder, but are generated only if Lync is running when the incoming call is received.

Remote Call Control and Enterprise Voice

Although remote call control features are separate from Enterprise Voice features and users cannot be enabled for both, Enterprise Voice provides a subset of features that are also available to users who are enabled for remote call control. If Enterprise Voice is deployed, users who are enabled for remote call control can use Lync to access the following Enterprise Voice features:

- Make and receive audio calls to another Lync client
- Join the audio portion of a conference created by a user who is enabled for Enterprise Voice

In This Section

- Deployment Tasks for Remote Call Control

1.3.16.1 Deployment Tasks for Remote Call Control

Deployment Tasks for Remote Call Control

Microsoft Lync Server 2013 > Planning > Planning for Remote Call Control >

Topic Last Modified: *2012-10-05*

This topic describes the deployment tasks that you must perform to enable remote call control for users in your Lync Server environment.

Note:

If you are migrating users previously enabled for remote call control in Microsoft Office Communicator 2007 R2, you must perform an additional deployment task before you begin performing the remote call control deployment tasks described in this topic. During the migration process to Lync Server, trusted application entries (previously known as *authorized host entries*) must be removed by using the Office Communications Server 2007 R2 administrative tools, as appropriate.
For details about removing authorized hosts, see Remove a Legacy Authorized Host (Optional).

Step 1: Install and Configure the SIP/ CSTA Gateway to Communicate with Your PBX

You need to install at least one SIP/CSTA gateway that can connect to both Lync Server and the existing private branch exchange (PBX) in your environment in order to provide remote call control features to your users. A SIP/CSTA gateway is a gateway between SIP and a computer-supported telecommunications application (CSTA). Whether you install multiple gateways or just one, each user can be configured with only one gateway or PBX. If your existing PBX does not have a SIP/CSTA interface, ensure you deploy a SIP/ CSTA gateway that can support the PBX, including support for proprietary PBX vendor-specific signaling protocols. For details about capabilities, consult each vendor directly.

When you are ready to deploy a SIP/CSTA gateway that can integrate with Lync Server for remote call control, also consult with your gateway vendor or the vendor's gateway documentation regarding the syntax required by the gateway for the following information:

- Line server URI of the gateway
- Line URI for users that will be assigned to the gateway

The preceding settings are required during user configuration and must be specified as expected by the gateway to route and connect to the PBX properly.

You can refer to vendors on the Microsoft Unified Communications Open Interoperability Program website at http://go.microsoft.com/fwlink/p/?linkId=203309.

Step 2: Configure Lync Server to Route CSTA Requests to the SIP/CSTA Gateway

You must create static routes on Lync Server pools to the destination address (server URI) of all SIP/CSTA gateways in your deployment to which you intend to route remote call control requests. You must also create a trusted application entry that corresponds to each destination address. When you designate the gateway as a trusted application, it is given trusted status to run as part of the Lync Server environment even though it is developed by a third party (and runs what is referred to as an *external service* because it is a service that is not a built-in part of the product). Finally, if Lync Server will connect to the SIP/CSTA gateway using a Transmission Control Protocol (TCP) connection instead of a Transport Layer Security (TLS) connection, you must also define the gateway IP address by using Topology Builder.

For details about configuring static routes, see Configure a Static Route for Remote Call Control.

For details about configuring trusted application entries, see Configure a Trusted Application Entry for Remote Call Control.

For details about defining a SIP/CSTA gateway IP address in Topology Builder, see Define a SIP/CSTA Gateway IP Address.

Step 3: Configure Lync Users for Remote Call Control

After users have been enabled for Lync Server, you can use Lync Server Control Panel or Lync Server Management Shell to enable them for remote call control. It is during this deployment step that you assign each user a line server URI and a line URI. The line server URI is the SIP URI of the SIP/CSTA gateway that you plan to assign to the user. The line URI is the unique phone number assigned to the user.

For details about configuring users for remote call control, see Enable Lync Users for Remote Call Control.

Step 4: Define the Lync Server Phone Number Normalization Rules

In remote call control scenarios, Lync Server uses phone number normalization rules to convert phone numbers it receives from the SIP/CSTA gateway to E.164 format. Phone numbers must be in this standardized format for certain remote call control features to function properly. Remote call control uses the same phone number normalization rules that you configure for Address Book Service phone number normalization, which are different from the phone number normalization rules used for Enterprise Voice.

For details about how remote call control uses phone number normalization rules, see Remote Call Control and Phone Number Normalization. For details about phone number normalization rules for Address Book Service, see Administering the Address Book Service topic in the Operations documentation.

1.3.17 Planning for Mobility

Planning for Mobility

Planning > Planning for External User Access > Scenarios for External User Access >

Topic Last Modified: *2013-02-14*

With Lync Server 2013, you can deploy the mobility feature to provide Lync 2013 functionality on mobile devices. This section provides details about the mobility feature and how to plan for your deployment.

- Mobility Features and Capabilities
- Topologies and Components for Mobility
- Technical Requirements for Mobility
- Defining Your Mobility Requirements
- Deployment Process for Mobility

1.3.17.1 Mobility Features and Capabilities

Mobility Features and Capabilities

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-19*

```
The information in this topic pertains to Cumulative Updates for Lync Server 2013
```

The mobility feature introduced in the Cumulative Updates for Lync Server 2013: February 2013 supports Lync 2010 Mobile and Lync 2013 Mobile clients functionality. When you deploy the Lync Server 2013 Mobility Service, users can use supported Apple iOS, Android, and Windows Phone, or Nokia Symbian mobile devices to perform activities such as sending and receiving instant messages, viewing contacts, and viewing presence. In addition, mobile devices support some Enterprise Voice features, such as click to join a conference, Call via Work, single number reach, voice mail, and missed calls. New features introduced in the Cumulative Updates for Lync Server 2013: February 2013 include Voice over IP (VoIP) capability and video (H.264) for meeting attendee.

The mobility feature introduced in the Cumulative Updates for Lync Server 2013: February 2013 supports Lync 2013 Mobile client functionality. The Cumulative Updates for Lync Server 2013: February 2013 install Unified Communications Web API, or UCWA. UCWA is the component used for Lync 2013 Mobile clients. In Lync Server 2013, Mcx is used for Lync 2010 Mobile clients. Cumulative Updates for Lync Server 2013: February 2013 introduce UCWA as the new entry point for mobility services. Lync Server 2013 concurrently implements the Mobility Service (Mcx), introduced in the Cumulative Updates for Lync Server 2010: November 2011, and provides support for Lync 2010 Mobile. When you deploy the Cumulative Updates for Lync Server 2013: February 2013, users can use supported Apple iOS, Android, and Windows Phone mobile devices to perform such activities as:

Important:
Features supported by the Mobility Service from the Cumulative Updates for Lync Server 2010: November 2011 are noted with (Mcx). All listed features are supported by the UCWA, introduced in the Cumulative Updates for Lync Server 2013: February 2013.

- Send and receive instant messages (Mcx)
- View presence (Mcx)
- View contacts (Mcx)
- Click to join a conference (Mcx)
- Call via work (Mcx)

- Single number reach (Mcx)
- Voice mail (Mcx)
- Missed call notification (Mcx)
- Voice over IP (VoIP)
- Attendee video (H.264)

Note:

Lync 2010 Mobile provided a client for Nokia Symbian devices. Lync 2013 Mobile will not have a client for Nokia Symbian-based devices.

Apple iPad users will have access to enhanced capabilities. After joining a meeting by using audio call back, an iPad user will be able to view uploaded Microsoft PowerPoint presentations within a meeting, share applications and desktops, view the meeting participant list, and receive notifications of other content types that are being shared within the meeting.

Tip:

With single number reach, a user receives calls on a mobile phone that were dialed to the work number. With Call via Work, the user places an outbound call from the Lync Mobile client by using a work phone number instead of the mobile phone number. With dial-out, the client sends a request to Mcx or UCWA (based on the Lync Mobile version) to make the call for them. The server initiates the call and then calls the user back on the mobile phone. When the user answers, the server completes the call by dialing the other party. By using Call via Work, users can maintain their work identity during a call, which means that the call recipient does not see the caller's mobile number, and the caller avoids incurring outbound calling charges.

Note:

Not all features work exactly the same on all mobile devices. For details about features supported on mobile devices, see the Mobile Client Comparison Tables at http://go.microsoft.com/fwlink/p/?LinkId=234777. For details about supported devices and operating systems, see the requirements topics under Planning for Mobile Clients.

When you use the Lync Server 2013 Autodiscover feature, mobile applications can automatically locate Lync Server 2013 Web Services without requiring users to manually enter the URLs in their device settings. Manually entering URLs in mobile device settings is also supported, primarily for troubleshooting purposes.

Important:

The Mcx and UCWA are complimentary services and both are deployed to support Lync 2010 Mobile and Lync 2013 Mobile clients. Lync 2013 Mobile will not be able to sign in to Lync Server 2010 deployments. Lync 2010 Mobile and Lync 2013 Mobile will be able to use a Lync Server 2013 deployment with the Cumulative Updates for Lync Server 2013: February 2013 applied.

The mobility feature also supports *push notifications* for mobile devices that do not support applications running in the background. A push notification is a notification that is sent to a mobile device about an event that occurs while a mobile application is inactive. For example, a missed instant messaging (IM) invitation can result in a push notification.

Mcx, UCWA, Autodiscover Service, and support for push notifications are provided in Lync Server 2013. Updated client features, capabilities, and the use of UCWA as the mobility entry point are introduced in the Cumulative Updates for Lync Server 2013: February 2013.

1.3.17.2 Topologies and Components for Mobility

Topologies and Components for Mobility

See Also

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-17*

`The information in this topic pertains to Cumulative Updates for Lync Server 2013`

To support Lync mobile applications on mobile devices, Lync Server 2013 provides three services: Lync Server 2013 Mcx Mobility Service, Lync Server 2013 Autodiscover Service, and Lync Server 2013 Push Notification Service. The Cumulative Updates for Lync Server 2013: February 2013 adds a complimentary, but advanced, service for Lync 2013 Mobile clients—mobility support through the use of the Unified Communications Web API, or UCWA. This section briefly describes these components and identifies the Lync Server 2013 topologies that support mobility.

Note:

Mobility services are also available in hybrid deployments. You are not required to deploy services for supporting mobility if your users are homed online. You do need to define a setting for the Autodiscover Service to enable mobile users to find their online identity.

Important:

If you are planning any external user connectivity (for example, federation, external user access, or mobility features), you must use Edge Servers with Standard Edition server and the Front End Server or Front End pool. The Standard Edition server and the Front End Server or Front End pool do not have the necessary components to enable external users to access your internal deployment, or for the internal deployment to communicate with your external users. For all scenarios that include external users collaborating or communicating with internal users, including mobility, you must deploy at least one Edge Server and one reverse proxy.

Push notification uses a type of federation to the Lync Online services, which hosts the Push Notification Clearing House (PNCH). Push notification refers to the sound alerts, on-screen alerts (text), and badges that are pushed by applications to the Apple iPhone, iPad, and Windows Phone, when the mobile device is inactive. PNCH receives push notifications from Lync Server. When PNCH receives a notification of a message, PNCH forwards a notification to mobile clients through either the Apple Push Notification Services or Lync Server 2013 Push Notification Service, based on the mobile client that the message is intended for. PNCH is a required service for these mobile clients. To federate to Lync Online, PNCH uses Edge Servers and certificates to ensure confidentiality and authentication, policies, and correctly configured domain name system (DNS) records. Nokia Symbian and Android-based Lync Mobile clients do not use PNCH.

For details about planning and deploying Edge Servers, see Planning for External User Access and Deploying External User Access.

The Lync 2013 Mobile clients for Apple devices introduced with the Cumulative Updates for Lync Server 2013: February 2013 no longer use push notification or the push notification clearing house (PNCH). Lync 2013 Mobile clients on Windows Phone still use push notification and the (PNCH).

Mobility Components

The services that support mobility are as follows:

- **Lync Server 2013 Unified Communications Web API (UCWA)** Provides services for real-time communications with mobile and web clients in Lync Server 2013. When you deploy the Cumulative Updates for Lync Server 2013: February 2013 to the Front End Server and Director, the installation creates a virtual directory in the internal and external web services (Ucwa). A web component that is part of the Ucwa virtual directory accepts calls from UCWA-enabled clients. The client apps communicate over a REST interface for presence, contacts, instant messaging, VoIP, video conferencing, and collaboration. UCWA uses a P-GET based channel to send events, such as an incoming call, incoming instant message, or a message to the client app.

Note:

REST or representational state transfer, is a software architectural style for distributed systems that has been widely adopted in many forms and is well suited to the requirements of Web services in general.

- **Lync Server 2013 Mobility Service (Mcx)** This service supports Lync functionality, such as instant messaging (IM), presence, and contacts, on mobile devices. The Mobility Service is installed on every Front End Server in each pool that is to support Lync functionality on mobile devices. When you install Lync Server 2013, a new virtual directory (Mcx) is created under both the internal website and the external website on your Front End Servers.

Important:

Lync Server 2013 with the Cumulative Updates for Lync Server 2013: February 2013 supports both the Mobility service introduced in the Cumulative Update for Lync Server 2010: November 2011, commonly known as Mcx, and the UCWA web component. The combination of these two mobility services provides interoperability and use by users with Lync 2010 Mobile and Lync 2013 Mobile clients on Lync Server 2013.

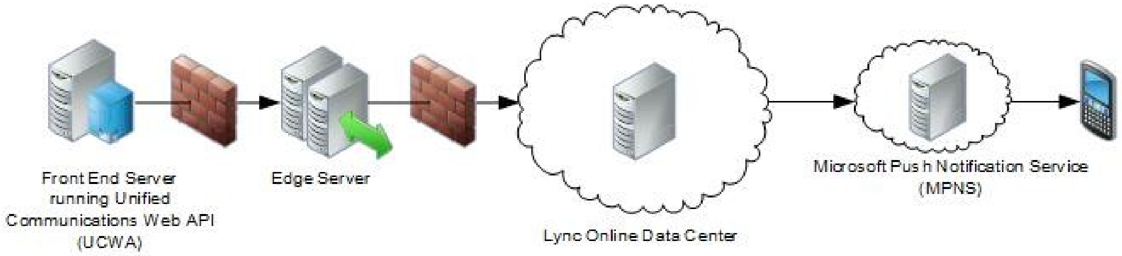
- **Lync Server 2013 Autodiscover Service** This service identifies the location of the user and enables mobile devices and other Lync clients to locate resources—such as the internal and external URLs for Lync Server 2013 Web Services, and the URL for the Mcx or UCWA—regardless of network location. Automatic discovery uses hardcoded host names (lyncdiscoverinternal for users inside the network; lyncdiscover for users outside the network) and the SIP domain of the user. It supports client connections that use either HTTP or HTTPS.
  The Autodiscover Service is installed on every Front End Server and on every Director in each pool that is to support Lync functionality on mobile devices. When you install the Autodiscover Service, a new virtual directory (Autodiscover) is created under both the internal website and the external website, on both Front End Servers and Directors.

Note:

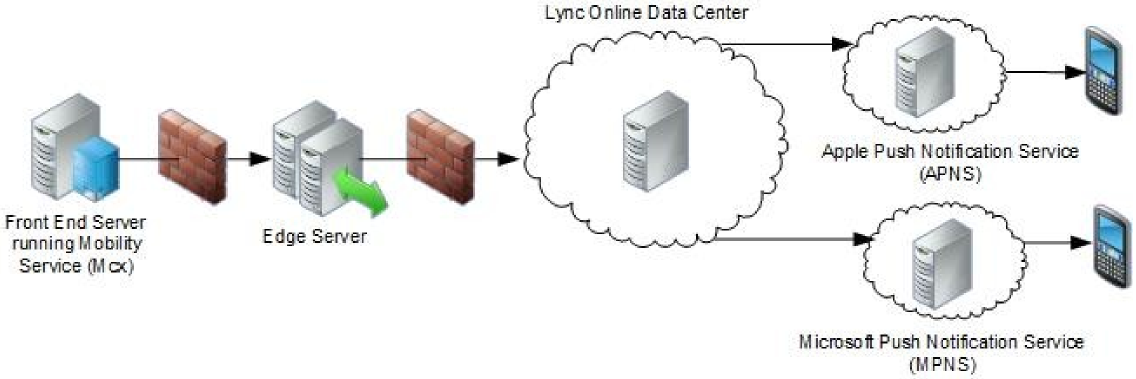
The Autodiscover Service is listed here because it remains a critical component when providing mobile client services. The role of Autodiscover in Lync Server 2013 has been expanded to provide services for all clients. For details about planning for the Autodiscover Service, see Planning for Autodiscover.

- **Push Notification Service** This service is a cloud-based service that is located in the Lync Online data center. When the Lync mobile application on a supported Apple iOS device or Windows Phone is inactive, it cannot respond to new events, such as a new instant messaging (IM) invitation, a missed instant message, a missed call, or voice mail, because these devices do not support mobile applications running in the background. In these cases, a notification of the new event—called a *push notification*—is sent to the mobile device. The Mobility Service sends the notification to the cloud-based Push Notification Service, which then sends the notification either to the Apple Push Notification Service (APNS) (for supported Apple iOS devices) or to the Microsoft Push Notification Service (MPNS) (for Windows Phone), which then sends it on to the mobile device. The user can then respond to the notification on the mobile device to activate the application.
  The Lync 2010 Mobile on Apple and Windows Phone devices use push notifications. The Lync 2013 Mobile client for Apple devices introduced with the Cumulative Updates for Lync Server 2013: February 2013 no longer uses push notification or the push notification clearing house (PNCH).

The following diagram illustrates how the Push Notification Service fits within a Lync Server 2013 topology that uses UCWA and Lync 2013 Mobile clients.


Front End Server running Unified Communications Web API (UCWA)
Edge Server
Lync Online Data Center
Microsoft Push Notification Service (MPNS)

Introduced in Cumulative Update for Lync Server 2010: November 2011, the Mcx service provides services to Lync 2010 Mobile clients. The following diagram illustrates the Push Notification Service as it applies to a topology using Mcx and Lync 2010 Mobile clients.


Lync Online Data Center
Apple Push Notification Service (APNS)
Front End Server running Mobility Service (Mcx)
Edge Server
Microsoft Push Notification Service (MPNS)

Supported Topologies

Applying the Cumulative Updates for Lync Server 2013: February 2013 adds the UCWA web components to support mobility for Lync 2013 Mobile client features in the following topologies:

- Lync Server 2013 Standard Edition
- Lync Server 2013 Enterprise Edition

The Edge Server can be a Lync Server 2010 Edge Server.

A Lync Server 2013 deployment without the Cumulative Updates for Lync Server 2013: February 2013 will use the Mcx Mobility Service and can provide services only for Lync 2010 Mobile.

Important:
The Mobility Service is supported on Front End Servers that is collocated with the Mediation Server role with two network interfaces, but you must take appropriate steps to configure the interfaces. You must assign the IP addresses to the specific interface that will communicate as the Mediation Server, and the network interface IP that will communicate as the Front End Server. You can do this in Topology Builder by selecting the correct IP address for each service, instead of using the default **Use all configured IP addresses**.

See Also

Other Resources

Planning for External User Access
Deploying External User Access

Planning for Autodiscover

1.3.17.3 Technical Requirements for Mobility

Technical Requirements for Mobility

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-19*

Some information in this topic pertains to Cumulative Updates for Lync Server 201

Mobile users encounter various mobile application scenarios that require special planning. For example, someone might start using a mobile application while away from work by connecting through the 3G network, then switch to the corporate Wi-Fi network when arriving at work, and then switch back to 3G when leaving the building. You need to plan your environment to support such network transitions and guarantee a consistent user experience. This section describes the infrastructure requirements that you must have in order to support mobile applications and automatic discovery of mobility resources.

Note:

Although mobile applications can also connect to other Lync Server 2013 services, the requirement to send all mobile application web requests to the same external web fully qualified domain name (FQDN) applies only to the Lync Server 2013 Mobility Service. Other mobility services do not require this configuration.

The requirement for cookie affinity in hardware load balancers is dramatically reduced, and you substitute Transmission Control Protocol (TCP) affinity if you are using the Lync Mobile delivered with Lync Server 2013. Cookie affinity can still be used, but the web services no longer require it.

Important:

All Mobility Service traffic goes through the reverse proxy, regardless of where the origination point is—internal or external. In the case of a single reverse proxy or a farm of reverse proxies, or a device that is providing the reverse proxy function, an issue can arise when the internal traffic is egressing through an interface and attempting to immediately ingress on the same interface. This often leads to a Security rule violation known as TCP packet spoofing or just spoofing. *Hair pinning* (the egress and immediate ingress of a packet or series of packets) must be allowed in order for mobility to function. One way to resolve this issue is to use a reverse proxy that is separate from the firewall (the spoofing prevention rule should always be enforced at the firewall, for security purposes). The hairpin can occur at the external interface of the reverse proxy instead of the firewall external interface. You detect the spoofing at the firewall, and relax the rule at the reverse proxy, thereby allowing the hairpin that mobility requires.
Use the Domain Name System (DNS) host or CNAME records to define the reverse proxy for the hairpin behavior (not the firewall), if at all possible.

Lync Server 2013 supports mobility services for Lync 2010 Mobile and Lync 2013 mobile clients. Both clients use the Lync Server 2013 Autodiscover Service to find its mobility entry point, but differ on which mobility service they use. Lync 2010 Mobile uses the Mobility Service known as *Mcx*, introduced with the Cumulative Update for Lync Server 2010: November 2011. Lync 2013 mobile clients use the Unified Communications Web API, or *UCWA*, as their mobility service provider.

Internal and External DNS Configuration

The Mobility Services Mcx (introduced with the Cumulative Update for Lync Server 2010: November 2011) and UCWA (introduced in the Cumulative Updates for Lync Server 2013: February 2013) use DNS in the same way.

When you use Automatic Discovery, mobile devices use DNS to locate resources. During the DNS lookup, a connection is first attempted to the FQDN that is associated with the internal DNS record (lyncdiscoverinternal.<*internal domain name*>). If a connection cannot be made by using the internal DNS record, a connection is attempted by using the external DNS record (lyncdiscover.<*sipdomain*>). A mobile device that is internal to the network connects to the internal Autodiscover Service URL, and a mobile device that is external to the network connects to the external Autodiscover Service URL. External Autodiscover requests go through the reverse proxy. The Lync Server 2013 Autodiscover Service returns all Web Services URLs for the user's home pool, including the Mobility Service (Mcx and UCWA) URLs. However, both the internal Mobility Service URL and the external Mobility Service URL are associated with the external Web Services FQDN. Therefore, regardless of whether a mobile device is internal or external to the network, the device always connects to the Lync Server 2013 Mobility Service externally through the reverse proxy.

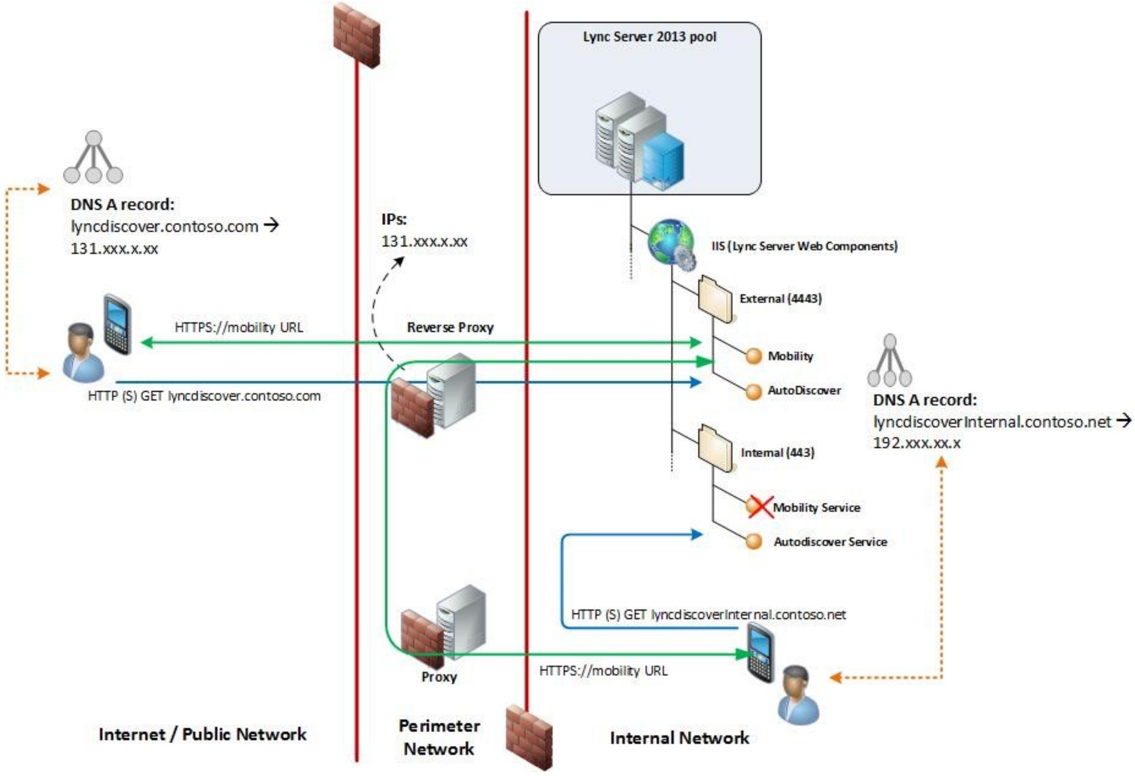
Note:

It is important to understand that your deployment can consist of multiple distinct namespaces for internal and external use. Your SIP domain name may be different than the internal deployment domain name. For example, your SIP domain may be **contoso.com**, while your internal deployment may be **contoso.net**. Users who log in to Lync Server will use the SIP domain name, such as **john@contoso.com**. When addressing the external web services (defined in Topology Builder as **External web services**), the domain name and the SIP domain name will be consistent, as defined in DNS. When addressing the internal Web services (defined in Topology Builder as **Internal web services**), the default name of the internal web services will be the FQDN of the Front End Server, Front End pool, Director, or Director pool. You have the option to override the internal web services name. You should use the internal domain name (and not the SIP domain name) for internal web services and define the DNS host A (or, for IPv6, AAAA) record to reflect the overridden name. For example, the default internal web services FQDN may be **pool01.contoso.net**. An overridden internal web services FQDN may be **webpool.contoso.net**. Defining the web services in this way helps to ensure that the internal and external locality of the services—and not the locality of the user who is using them—is observed.

However, because the web services are defined in Topology Builder and the internal web services name can be overridden, as long as the resulting web services name, the certificate that validates it, and the DNS records that define it, are consistent, you can define the internal web services with any domain name—including the SIP domain name—that you want. Ultimately, the resolution for the name to the IP address is determined by DNS host records and a consistent namespace.

For the purposes of this topic and the examples, the internal domain name is used to illustrate the topology and the DNS definitions.

The following diagram illustrates the flow of mobile application web requests for the Mobility Service and for the Autodiscover Service when using an internal and external DNS configuration.



Note:

The diagram illustrates generic web services. A virtual directory named Mobility depicts the Mobility services Mcx and/or UCWA. If you have not applied the Cumulative Updates for Lync Server 2013: February 2013, you may or may not have the virtual directory Ucwa defined on your internal and external Web services. You will have a virtual directory Autodiscover, and you may have a virtual directory Mcx.
Autodiscover and the discovery of services work the same way, regardless of the mobility services technology that you have deployed.

To support mobile users from both inside and outside the corporate network, your internal and external web FQDNs must meet some prerequisites. In addition, you may need to meet other requirements, depending on the features you choose to implement:

- New DNS, CNAME or A (host, if IPv6, AAAA) records, for automatic discovery.
- New firewall rule, if you want to support push notifications through your Wi-Fi network.
- Subject alternative names on internal server certificates and reverse proxy certificates, for automatic discovery.
- Front End Server hardware load balancer configuration changes source affinity.
- .

Your topology must meet the following requirements to support the Mobility Service and the Autodiscover Service:

- The Front End pool internal web FQDN must be distinct from the Front End pool external web FQDN.
- The internal web FQDN must only resolve to and be accessible from inside the corporate network.
- The external web FQDN must only resolve to and be accessible from the Internet.
- For a user who is inside the corporate network, the Mobility Service URL must be addressed to the external web FQDN. This requirement is for the Mobility

Service and applies only to this URL.
- For a user who is outside the corporate network, the request must go to the external web FQDN of the Front End pool or Director.

If you support automatic discovery, you need to create the following DNS records for each SIP domain:

- An internal DNS record to support mobile users who connect from within your organization's network.
- An external, or public, DNS record to support mobile users who connect from the Internet.

The internal automatic discovery URL should not be addressable from outside your network. The external automatic discovery URL should not be addressable from within your network. However, if you cannot meet this requirement for the external URL, mobile client functionally will probably not be affected, because the internal URL is always tried first.

The DNS records can be either CNAME records or A (host, if IPv6, AAAA) records.

Note:
Mobile device clients do not support multiple Secure Sockets Layer (SSL) certificates from different domains. Therefore, CNAME redirection to different domains is not supported over HTTPS. For example, a DNS CNAME record for lyncdiscover.contoso.com that redirects to an address of director.contoso.net is not supported over HTTPS. In such a topology, a mobile device client needs to use HTTP for the first request, so that the CNAME redirection is resolved over HTTP. Subsequent requests then use HTTPS. To support this scenario, you need to configure your reverse proxy with a web publishing rule for port 80 (HTTP). For details, see "To create a web publishing rule for port 80" in Configuring the Reverse Proxy for Mobility. CNAME redirection to the same domain is supported over HTTPS. In this case, the destination domain's certificate covers the originating domain.

For details about the DNS records required for your scenario, see DNS Summary - Autodiscover.

Port and Firewall Requirements

If you support push notifications and want Apple mobile devices to receive push notifications over your Wi-Fi network, you also need to open port 5223 on your enterprise Wi-Fi network. Port 5223 is an outbound TCP port used by the Apple Push Notification Service (APNS). The mobile device initiates the connection. For details, see http://support.apple.com/kb/TS1629 .

⚠**Warning:**
An Apple device using the Lync 2013 Mobile client does not require push notifications.

For additional details and guidance on port and protocol requirements for Autodiscover, see Port Summary - Autodiscover.

Certificate Requirements

If you support automatic discovery for Lync mobile clients, you need to modify the subject alternative name lists on certificates to support secure connections from the mobile clients. You need to request and assign new certificates, adding the subject alternative name entries described in this section, for each Front End Server and Director that runs the Autodiscover Service. The recommended approach is to also modify the subject alternative names lists on certificates for your reverse proxies. You need to add subject alternative name entries for every SIP domain in your organization.

Reissuing certificates by using an internal certificate authority is typically a simple process, but adding multiple subject alternative name entries to public certificates used by the reverse proxy can be expensive. If you have many SIP domains, making the addition of subject alternative names very expensive, you can configure the reverse proxy to make the initial Autodiscover Service request over port 80 using HTTP, instead of port 443 using HTTPS (the default configuration). The request is then redirected to port 8080 on the Director or Front End pool. When you publish the initial Autodiscover Service request on port 80, you do not need to change certificates for the reverse proxy, because the request uses HTTP rather than HTTPS. This approach is supported, but we do not recommend it.

Internet Information Services (IIS) Requirements

We recommend that you use IIS 7.5 or IIS 8.0 for mobility. The Mobility Service installer sets flags in ASP.NET to improve performance. IIS 7.5 is installed by default on Windows Server 2008 R2 and IIS 8.0 is installed on Windows Server 2012. The Mobility Service installer automatically changes the ASP.NET settings.

Hardware Load Balancer Requirements

On the hardware load balancer that is supporting the Front End pool, the external Web Services virtual IPs (VIPs) for Web Services traffic must be configured for source. Source affinity helps to ensure that multiple connections from a single client are sent to one server to maintain session state. For details about affinity requirements, see Load Balancing Requirements.

If you plan to support Lync mobile clients only over your internal Wi-Fi network, you should configure the internal Web Services VIPS for source as described for external Web Services VIPs. In this situation, you should use source_addr (or TCP) affinity for the internal Web Services VIPs on the hardware load balancer. For details, see Load Balancing Requirements.

Reverse Proxy Requirements

If you support automatic discovery for Lync mobile clients, you need to update the current publishing rule as follows:

- If you decide to update the subject alternative names lists on the reverse proxy certificates and use HTTPS for the initial Autodiscover Service request, you must update the web publishing rule for lyncdiscover.<*sipdomain*>. Typically, this is combined with the publishing rule for the external Web Services URL on the Front End pool.
- If you decide to use HTTP for the initial Autodiscover Service request so that you do not need to update the subject alternative names list on the reverse proxy certificates, you must create a new web publishing rule for port HTTP/ TCP 80, if one does not already exist. If a rule for HTTP/TCP 80 does already exist, you can update that rule to include the lyncdiscover.<*sipdomain*> entry.

1.3.17.4 Autodiscover Service Requirements

Autodiscover Service Requirements

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-25*

The Microsoft Lync Server 2013 Autodiscover Service runs on the Director and Front End pool servers, and when published in DNS, can be used by mobile devices running Lync Mobile to locate mobility services. Before mobile devices running Lync Mobile can take advantage of automatic discovery, you need to modify certificate subject alternative name lists on any Director and Front End Server running the Autodiscover Service. In addition, it may be necessary to modify the subject alternative name lists on certificates used for external web service publishing rules on reverse proxies.

For details about the subject alternative name entries that are required for Directors, Front End Servers, and reverse proxies, see Technical Requirements for Mobility in Planning for Mobility.

The decision about using subject alternative name lists on reverse proxies is based on whether you publish the Autodiscover Service on port 80 or on port 443:

- **Published on port 80** No certificate changes are required if the initial query to the Autodiscover Service occurs over port 80. This is because mobile devices running Lync will access the reverse proxy on port 80 externally and then be redirected to a Director or Front End Server on port 8080 internally. For details, see the "Initial Autodiscover Process Using Port 80" section later in this topic.
- **Published on port 443** The subject alternative name list on certificates used by the external web services publishing rule must contain a *lyncdiscover.<sipdomain>* entry for each SIP domain within your organization.

Reissuing certificates using an internal certificate authority is typically a simple process but for public certificates used on the web service publishing rule, adding multiple subject alternative name entries can become expensive. To work around this issue, we support the initial automatic discovery connection over port 80, which is then redirected to port 8080 on the Director or Front End Server.

For example, assume that a mobile client running Lync Mobile is configured to sign in to Lync Server 2013 using the automatic discovery feature using HTTP for the initial request.

Initial Autodiscover Process for Mobile Devices Using Port 80

1. Mobile device running Lync Mobile looks up lyncdiscover.contoso.com using DNS, where an A record exists.
2. External DNS returns the IP address for the external web services to the client.
3. Mobile device running Lync Mobile sends request http://lyncdiscover.contoso.com?sipuri=lyncUser1@contoso.com to the reverse proxy
4. The web publishing rule will bridge the request from port 80 externally to port 8080 internally, which will then route it to either a Director or Front End Server.
   Since the request is HTTP and not HTTPS, no modifications are needed to the certificate on the external web service publishing rule to support the Autodiscover Service.
5. The Autodiscover Service returns the external web service URLs (in HTTPS format).
6. The mobile device running Lync Mobile can then reconnect to the reverse proxy on port 443 and is redirected over 4443 to the mobility service running on the user's home pool.
   Since the HTTPS query is to the external web services URL vs. the Autodiscover Service URL, it succeeds because the certificate will already

contain subject alternative name entries for the external web services fully qualified domain names (FQDNs).
In this scenario, there are no certificate changes required to support mobility.

> **Note:**
> If the target web server has a certificate that does not have a matching value for lyncdiscover.contoso.com as a subject alternative name list value:
> a. Web server responds with a "Server Hello" and no certificate.
> b. Mobile device running Lync Mobile immediately terminates the session.
> If the target web server has a certificate that includes lyncdiscover.contoso.com as a subject alternative name list value:
> a. Web server responds with a "Server hello" and a certificate.
> b. Mobile device running Lync Mobile validates the certificate and completes the handshake.

To support an initial connection to the Autodiscover Service using port 80 on your reverse proxy server, you can create an http publishing rule similar to this example for a Forefront Threat Management Gateway 2010 reverse proxy web publishing rule:

1. Create a new web publishing rule (for example, **Lync Server Autodiscover (HTTP)**).
2. In **Public Name**, enter lyncdiscover.contoso.com.
3. On the **Bridging** tab, select only the option to bridge requests from Port 80 to Port 8080.
4. On the **Authentication** tab, select **No authentication**, and **Client cannot authenticate directly**.
5. Commit changes, and move the rule to the top of the list of Lync rules (first in processing order).

Mobility for the Split Domain Deployment

A shared SIP address space, also known as a *split-domain*, or a *hybrid deployment* is a configuration where users are deployed across an on-premise deployment and an online environment. The desired outcome is to have a user, regardless of where their home server is located (on-premise or online), to log into the deployment and be redirected to their home server location. To accomplish this, the Autodiscover feature of Microsoft Lync Server 2013 is used to redirect the online user to the online topology. This is done by configuring the Autodiscover uniform resource locator (URL) by using the Lync Server Management Shell and the cmdlets **Get-CsHostingProvider** and **Set-CsHostingProvider**.

You will need to collect and record the following deployed attributes:

- From the Lync Server Management Shell, type

```
Get-CsHostingProvider
```

- In the results, find the online provider with the attribute **ProxyFQDN**. For example, sipfed.online.lync.com
- Record the value of the ProxyFQDN
- Enable federation in the on-premise Lync Server Control Panel, allowing federation with the online provider
- Enable federation for the online provider. By default, all online users are enabled for domain federation and can communicate with all domains
- If you will define blocked and allowed domains, determine the domains that you will explicitly allow or explicitly block
- For online federation, you must plan for firewall exceptions, certificates and DNS host (A or AAAA, if using IPv6) records. Additionally, you must configure federation policies. For details, see Planning for Lync Server and Office Communications Server Federation

1.3.17.5 Defining Your Mobility Requirements

Defining Your Mobility Requirements

See Also

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-14*

```
Some information in this topic pertains to Cumulative Updates for Lync Server 201
```

During the planning phase for the Lync Server 2013 mobility feature, when you are using Lync 2010 Mobile and Lync 2013 Mobile clients, you make decisions that determine your deployment steps.

Here are the decisions that you must consider:

- **Do you want to use automatic discovery for Lync mobile clients?**
  If you want to support automatic discovery, you need to create new internal and external Domain Name System (DNS) records, add subject alternative names to certificates on the Front End Servers, Directors, and reverse proxy, and modify the existing publishing rules on the reverse proxy. For details, see Technical Requirements for Mobility. With automatic discovery, users can automatically locate Lync Server 2013 Web Services from anywhere inside or outside the corporate network, without entering URLs in their mobile device settings.
  If you use manual settings instead of automatic discovery, mobile users need to manually enter the following URLs in their mobile devices:
  - https://<ExtPoolFQDN>/Autodiscover/autodiscoverservice.svc/Root for external access
  - https://<IntPoolFQDN>/AutoDiscover/ autodiscoverservice.svc/Root for internal access

  We strongly recommend using automatic discovery. The primary use of manual settings is for troubleshooting.
- **If you decide to support automatic discovery, are you willing to update certificates on the reverse proxy with subject alternative names for each SIP domain?**
  If you have many SIP domains, updating public certificates on the reverse proxy can become very expensive. If this is the case, you can choose to implement automatic discovery so that the initial Autodiscover Service request uses HTTP on port 80, instead of using HTTPS on port 443. However, this is not the recommended approach. If you decide to choose this alternative, you do not need to update the certificates on the reverse proxy, but you need to create a web publishing rule for HTTP on port 80. For more details, see Technical Requirements for Mobility.
- **Do you want to support Lync mobile clients both internal and external to the corporate network, or support clients only inside the corporate network?**
  If you want to support mobile clients internal and external to your network, mobile devices can access mobility features from any location. The default configuration is to support clients both internal and external to the corporate network.
  Although the default configuration enables mobile client traffic to go through the external site, you can restrict mobile client traffic to the internal corporate network. When you restrict the traffic to the internal network, users can use Lync mobile applications on their mobile devices only when they are inside the network.
  For deployments that support mobility using the Mcx mobility service and Lync 2010 Mobile, you run the **Set-CsMcxConfiguration** cmdlet. To set mobility for internal use only, you would use a command similar to the following:

```
Set-CsMcxConfiguration -Identity site:Redmond -ExposedWebURL Internal
```

Note:
There are no additional configurations required for UCWA. UCWA does not have an equivalent internal-only configuration.

Important:
If you are using a Lync Server 2013 Front End Server or Front End pools and **you do not have** any Lync Server 2010 Front End Servers or Front End pools, **there is no requirement for cookie-based persistence**. If you need to retain any Lync Server 2010 Front End Servers or Front End pools, the same rules still apply as in Lync Server 2010 for cookie-based persistence.

- **Do you want to support push notifications for Apple iOS devices and Windows Phones?**
  If you support push notifications, supported Apple iOS devices and Windows Phones receive a notification of events that occur when the mobile application is inactive. You must configure your Edge Server to have a federation relationship with the cloud-based Lync Server Push Notification Service, which is located in the Lync Online datacenter, and run a cmdlet to enable push notifications.
  If you want to support push notifications over your Wi-Fi network, in addition to supporting push notifications over the mobile device providers' 3G or data networks, you must open port 5223 outbound on your enterprise Wi-Fi network. Supporting push notifications over the Wi-Fi network supports mobile devices that use only Wi-Fi and mobile devices that have poor indoor reception.

  Important:
  Opening port TCP 5223 is required only when supporting Apple devices running the Lync 2010 Mobile client.

  If you do not support push notifications, users of Apple mobile devices and Windows Phones will not find out about events—such as instant message invitations or missed messages—that occur when the mobile application is inactive.

  Note:
  Lync 2013 Mobile clients on Apple devices do not require push notification. The Lync 2013 Mobile clients on Windows Phone use push notification. Planning for push notification and the push notification clearinghouse remain the same for Lync Mobile on Windows Phone and Apple devices that are not able to run the Lync 2013 Mobile client.

- **Do you want all users to have access to mobility features, or do you want to be able to specify which users have access to these features?**
  The table describes features available to users in Lync Server 2013. The defaults allow Call via Work, allow Voice over IP (VoIP), and enable Mobility. Here is the full set of available options:

Feature/Paramater Name/Scope (Policy parameter names may not be the same)	**Description**	**Introduced**
Enable Mobility Parameter Name : `EnableMobility` Scope: Global/Site/User	Administrative setting to control users in a given scope that have the Lync Mobile installed, If the policy is set to False, the user would not be able to sign into the client. The default setting is	Cumulative Update for Lync Server 2010: November 2011

	True.	
Enable Outside Voice Parameter Name : `EnableOutsideVoice` Scope: Global/Site/User	Controls a user's ability to use Call Via Work, a feature that enables users to make and receive calls by using their work number instead of their mobile number. If set to False, the user will not be able to make or receive calls by using their work number from their mobile device. The default setting is True	Cumulative Update for Lync Server 2010: November 2011
Enable IP Audio and Video Parameter Name : `EnableIPAudioVideo` Scope: Global/Site/User	Controls whether a user can use VoIP to make or receive voice or video calls on their mobile device. If set to False, the user will not be able to make or receive VoIP or video calls on their device. The default setting is True.	Microsoft Lync Server 2013
Require WiFi for IP Audio Parameter Name : `RequireWiFiForIPAudio` Scope: Global/Site/User	This setting defines whether the client will be required to make and receive calls over VoIP on WiFi instead of the cellular data network. If set to True, the user can make and receive VoIP calls only when connected to a WiFi network. The default setting is False.	Microsoft Lync Server 2013
Require WiFi for IP Video Parameter Name : `RequireWiFiForIPVideo` Scope: Global/Site/User	This setting defines whether the client will be required to make and receive video calls on Wi-Fi instead of on the cellular data network. If set to True, the user can make and receive video calls only when connected to a Wi-Fi network. The default setting is False.	Microsoft Lync Server 2013

For a description of the policy settings that you can configure, and how to manage the policies, see New-CsMobilityPolicy, Set-CsMobilityPolicy, Get-CsMobilityPolicy, Grant-CsMobilityPolicy and Remove-CsMobilityPolicy.

- **Do you want users who are not enabled for Enterprise Voice to be able to**

use Click to Join to join conferences?
For users to have access to mobility features and Call via Work, they must be enabled for Enterprise Voice. However, users who are not enabled for Enterprise Voice can join conferences by clicking the link on their mobile device, if they have an appropriate voice policy assigned to them. You can either assign a specific voice policy to these users or make sure that a global policy or site-level policy exists that applies to them. The voice policy that you assign must have public switched telephone network (PSTN) usage records and routes that define the areas to which users can dial out to join a conference. For details about setting voice policy, PSTN usage records, and routes, see Configuring Voice Policies, PSTN Usage Records, and Voice Routes.

Note:
Mobile users who want to use Click to Join require a voice policy, along with the related PSTN usage records and voice routes, because clicking the link on the mobile device results in an outbound call from Lync Server 2013.

Concepts

Technical Requirements for Mobility

Other Resources

Configuring Voice Policies, PSTN Usage Records, and Voice Routes

1.3.17.6 Deployment Process for Mobility

Deployment Process for Mobility

Planning for External User Access > Scenarios for External User Access > Planning for Mobility >

Topic Last Modified: *2013-02-19*

```
Some information in this topic pertains to Cumulative Updates for Lync Server 201
```

This section describes the sequence of steps required to deploy the Lync Server 2013 mobility feature.

Mobility Deployment Process

Phase	Steps	Permissions	Deployment documentation
Create Domain Name System (DNS) records	• Create an internal DNS CNAME or A (host, if IPv6, AAAA) record to resolve the internal Autodiscover Service URL. • Create an external DNS CNAME or A (host, if IPv6, AAAA) record to resolve the external Autodiscover Service URL.	Domain Admins DnsAdmins	Creating DNS Records for the Autodiscover Service
Modify certificates	Add subject alternative name entries to the following certificates to support secure connections for mobile users: • Director certificate • Front End pool certificate	Local administrator	Modifying Certificates for Mobility

	• Reverse proxy certificate		
Configure the reverse proxy	• Assign certificates updated with subject alternative names to the Secure Sockets Layer (SSL) Listener. • Reconfigure the web publishing rule for the external Autodiscover Service URL. • Be sure that a web publishing rule exists for the external Lync Server 2013 Web Services URL on your Front End pool. Or • If you choose to use HTTP for the initial Autodiscover request and do not update subject alternative name lists on the certificates, configure a new web publishing rule or reconfigure an existing publishing rule for port 80 HTTP.	Local administrator	Configuring the Reverse Proxy for Mobility
Test your mobility deployment for Lync 2010 Mobile using the Mcx Mobility Service	Run **Test-CsMcxP2PIM** to test sending an instant message from one person to another. See the Lync Server Management Shell cmdlet documentation for Test-CsMcxP2PIM for a complete list of options.	CsAdministrator	Verifying Your Mobility Deployment
Test your mobility deployment for Lync 2013 Mobile clients using the UCWA Web components	Use the **Test-CsUcwaConference** cmdlet to test and verify that pre-defined test users or a pair of actual users can use UCWA to create and participate in a conference. See the Lync Server Management Shell cmdlet documentation for Test-CsUcwaConference for a complete list of options.	CsAdministrator	Verifying Your Mobility Deployment

Configure for push notifications	• For Lync Server 2013 Edge Servers, add a Lync Server online hosting provider and configure hosting provider federation. • For Lync Server 2010 Edge Servers, add a Lync Server online hosting provider and configure hosting provider federation. • For Office Communications Server 2007 R2 Edge Servers, add a federated partner. • If you want to support push notifications over a Wi-Fi network, configure a firewall rule outbound for TCP port 5223. • Use the **Set-CsPushNotificationConfiguration** cmdlet to enable push notifications to the Apple Push Notification Service (APNS) and Microsoft Push Notification Service (MPNS). This feature is disabled by default. • Use the **Test-CsFederatedPartner** cmdlet to test the federation configuration and the **Test-CsMCXPushNotification** cmdlet to test push notifications. **Note:** Push notifications are used for Lync 2010 Mobile clients on Apple devices and Windows Phone Push notification is required for Lync 2013 Mobile clients on Windows Phone	RtcUniversalServerAdmins	Configuring for Push Notifications

	only		
Configure mobility policy	Use the **Set-CsMobilityPolicy** cmdlet to allow or disallow: • Call via Work • Enable IP Audio and IP Video • Require WiFi for IP Audio and/or IP Video	CsAdministrator	Configuring Mobility Policy

1.4 Deployment

Deployment

Microsoft Lync Server 2013 >

Topic Last Modified: *2012-10-18*

Deployment of Lync Server 2013 communications software includes preparing Active Directory Domain Services (AD DS), deploying the Front End Servers and other core Lync Server 2013 internal components, and then deploying any additional server roles and features that your organization may require, such as external user access and Enterprise Voice.

This documentation describes three scenarios for deploying Lync Server 2013:

- New Deployment of Lync Server 2013, Enterprise Edition
- New Deployment of Lync Server 2013, Standard Edition
- New Deployment of Lync Server 2013 Standard Edition or Enterprise Edition into an existing Lync Server 2010 Standard Edition or Enterprise Edition deployment

For information about deploying Lync Server 2013 in an existing Microsoft Office Communications Server 2007 or Microsoft Office Communications Server 2007 R2 environment, see the Migration documentation.

- Deploying Lync Server 2013
- Deploying External User Access
- Deploying Enterprise Voice
- Deploying Monitoring
- Deploying Archiving
- Configuring Dial-in Conferencing
- Configuring Video
- Deploying Branch Sites
- Deploying Persistent Chat Server
- Deploying Clients and Devices
- Planning and Deploying Unified Contact Store
- Managing Server-to-Server Authentication (Oauth) and Partner Applications
- Updating From the Evaluation Version of Lync Server 2013
- Deploying Remote Call Control
- Deploying Mobility
- Configuring Integration with Office Web Apps Server and Lync Server 2013
- Health Configuration in Lync Server 2013

1.4.1 Deploying Lync Server 2013

Deploying Lync Server 2013

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-10-18*

Your deployment process for Lync Server 2013 is determined by the Lync Server topology and components you decide to install, including whether you want to deploy a Front End pool or a Standard Edition server. The topics in this section help you determine what environment you want to deploy and guide you through the deployment process.

- Deployment Overview
- System Requirements
- Preparing the Infrastructure and Systems
- Defining and Configuring the Topology
- Finalizing and Implementing the Topology Design
- Setting Up Front End Servers and Front End Pools
- Deploying Lync Server 2013 Standard Edition into an Existing Lync Server 2013 Enterprise
- Adding Server Roles
- Setting Up Kerberos Authentication

1.4.1.1 Deployment Overview

Deployment Overview

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2013-03-12*

The main difference between Lync Server 2013 Enterprise Edition and Lync Server 2013 Standard Edition is that Standard Edition does not support the high availability features included with Enterprise Edition. For high availability, you need to deploy multiple Front End Servers to a pool and then you can mirror the server running SQL Server. With Enterprise Edition you can choose to collocate or define a stand-alone Mediation Server. The Monitoring Server and Archiving Server can use a stand-alone server running SQL Server. Or, they can have instances of SQL Server running on the database server for the Front End Servers and pools.

Servers running Lync Server 2013 Standard Edition are intended for smaller organizations and remote locations, which are geographically removed from the organization’s main deployment. Two Standard Edition server servers paired together for failover in case of disaster can support up to 5,000 users. You cannot pool Standard Edition servers like you can Front End Servers in Enterprise Edition. Also, the SQL Server database that Standard Edition uses is a collocated server running SQL Server Express that is designed to handle Standard Edition server workloads. This is not to say that all roles must reside on a Standard Edition server. You can have stand-alone Mediation Servers and Edge Servers. The SQL Server database for the Central Management store and for the purposes of Lync Server 2013 must reside on the Standard Edition server collocated with the server running SQL Server. The Monitoring Server and Archiving Server use a stand-alone server with the SQL Server database.

1.4.1.2 System Requirements

System Requirements

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2012-06-20*

This section discusses the system requirements for deploying Lync Server 2013 and all of the associated components.

- Administrator Rights and Permissions Required for Setup and Administration
- System Requirements for Servers Running Lync Server 2013
- System Requirements for SQL Server
- System Requirements for Administration Tools
- DNS Requirements

1.4.1.2.1 Administrator Rights and Permissions Required for Setup and Administration

Administrator Rights and Permissions Required for Setup and Administration

Deployment > Deploying Lync Server 2013 > System Requirements >

Topic Last Modified: *2012-06-29*

Setup and deployment of Lync Server 2013 requires that the person installing and deploying the software be a member of local or domain-level groups. Administrative tools for Lync Server 2013 can require additional permissions.

- Group Membership Requirements
- Delegate Setup Permissions

1.4.1.2.1.1 Group Membership Requirements

Group Membership Requirements

Deploying Lync Server 2013 > System Requirements > Administrator Rights and Permissions Required for Setup and Administration >

Topic Last Modified: *2012-10-05*

The following table summarizes the group or groups that a person should belong to in order to successfully install, manage, and troubleshoot Lync Server 2013.

Lync Server 2013 Executable	Group Membership Required
Setup.exe – Executable that starts the installation of the Lync Server 2013 administrative tools.	Member of the Local Administrators group on the computer from which the executable is run. Member of Domain Users group to read information in Active Directory Domain Services (AD DS). This level of permission is required because the automatic installation of required MSI packages on the local computer requires privileges that allow reading from and writing to protected local computer resources such as Program Files directories, and protected registry such as the Local Machine hive. **Tip:**

	You can also delegate setup permissions to users or groups to whom you do not want to grant membership in the Domain Admins group. For details, see Granting Setup Permissions in the Deployment documentation.
Deploy.exe – Called by setup.exe, deploy.exe is responsible for the deployment of the software components for the server roles.	Member of the Local Administrators group on the computer from which the executable is run. Member of Domain Users group to read information in AD DS. This level of permission is required because the automatic installation of required MSI packages on the local computer requires privileges that allow reading from and writing to protected local computer resources such as Program Files directories, and protected registry such as the Local Machine hive. Membership in RtcUniversalReadOnlyAdmins group is necessary to read the Central Management store. **Note:** If you are running the Windows Vista operating system or Windows 7 operating system, you will be prompted by User Account Control (UAC) to proceed with installation. If you are logged on with a standard user account, you will need someone who is a member of the Local Administrators group to provide credentials when prompted for an account with permissions to install the software.
Bootstrapper.exe – Called by setup.exe, bootstrapper.exe is responsible for deployment and configuration of server roles.	Member of the Local Administrators group on the computer from which the executable is run. Member of the RTCUniversalServerAdmins group to run Bootstrapper.exe. Member of Domain Users group to read information in AD DS. This level of permission is required because the automatic installation of required MSI packages on the local computer requires privileges that allow reading from and writing to protected local computer resources such as Program Files directories, and protected registry such as the Local Machine hive.
TopologyBuilder – Wizard-driven user interface to create, view, adjust, and validate Lync Server 2013 topologies.	Member of the Local Administrators group on the computer from which the executable is run to view the topology. Member of the RTCUniversalServerAdmins group to change configuration settings. Member of the RTCUniversalServerAdmins group and Domain Admins group, or member of the RTCUniversalServerAdmins group (only if the group has been granted delegate setup permissions), to publish the topology. For details about delegating setup permissions to allow members of the RTCUniversalServerAdmins group to publish the topology without being members of the Domain Admins group, see Granting Setup Permissions in the Deployment documentation.
AdminUIHost – Web-based graphical user interface for managing Lync	Member of CsAdministrator group or member of another role-based access control (RBAC) role to

Server 2013.	which the specific administrative task is assigned. Lync Server 2013 Control Panel implements configuration changes by running Lync Server 2013 Management Shell cmdlets. For a list of predefined roles and the cmdlets members are permitted to run, see Planning for Role-Based Access Control in the Planning documentation.
PowerShell.exe with the Lync Server 2013 module loaded – Command-line administrative tool with cmdlets specific to management of Lync Server 2013.	Member of CsAdministrator group or member of another RBAC role to which the specific cmdlet has been assigned. For a list of predefined roles and the cmdlets members are permitted to run, see Planning for Role-Based Access Control in the Planning documentation. Or, member of one or more of the following groups, depending on the cmdlet: • RTCUniversalServerAdmins • RTCUniversalUserAdmins • RTCUniversalReadOnlyAdmins

1.4.1.2.1.2 Delegate Setup Permissions

Delegate Setup Permissions

Deploying Lync Server 2013 > System Requirements > Administrator Rights and Permissions Required for Setup and Administration >

Topic Last Modified: *2012-10-01*

If you do not want to grant membership in the Domain Admins group to users or groups who are deploying Lync Server 2013, you can enable members of the RTCUniversalServerAdmins group to run the **Enable-CsTopology** Windows PowerShell cmdlet on servers running Lync Server 2013. By default, members of the RTCUniversalServerAdmins group do not have the ability to run this cmdlet. You grant administrator rights and permissions to run **Enable-CsTopology** on servers running Lync Server by using the **Grant-CsSetupPermission** cmdlet and specifying an organizational unit (OU) where computer objects for the server running Lync Server 2013 are located.

Note:

Enable-CsTopology is the key cmdlet to allow the RTCUniversalServerAdmins group members to set up and deploy Lync Server 2013.

⊟To add the ability to run Enable-CsTopology to the RTCUniversalServerAdmins group

1. Log on to a server as a member of the Domain Admins group for the domain on which the delegated user will run **Enable-CsTopology**.
2. Open the Lync Server 2013 Management Shell. The Lync Server 2013 Management Shell is automatically installed on each Front End Server or any computer where the Lync Server 2013 administrative tools have been installed. For details about the Lync Server 2013 Management Shell, see Lync Server Management Shell in the Operations documentation.
3. Run the following cmdlet from the Lync Server 2013 Management Shell:

```
Grant-CsSetupPermission -ComputerOU <DN of the OU> -Domain <Domain FQD
```

Note:

If the OU is not top level, you must provide the full domain name.

In the following example, the OU is “Lync Servers,” which is in the contoso.com domain.

```
Grant-CsSetupPermission -ComputerOU "OU=Lync Servers" -Domain contoso.
```

1.4.1.2.2 System Requirements for Servers Running Lync Server 2013

System Requirements for Servers Running Lync Server 2013

Deployment > Deploying Lync Server 2013 > System Requirements >

Topic Last Modified: *2013-03-12*

Standard Edition and Enterprise Edition servers share the same software requirements.

Servers running Lync Server 2013, Enterprise Edition are intended for large organizations as the main organizational deployment. Enterprise Edition server is designed to scale to approximately 80,000 homed users per pool. Servers running Lync Server 2013, Standard Edition are intended for smaller organizations and remote locations from the main organization deployment. One pair of Standard Edition servers can support up to 5,000 users.. For details on the differences between Standard Edition servers and Enterprise Edition servers, see Deployment Overview.

Operating System Installation

Important:

Lync Server 2013 is available only in a 64-bit edition, which requires 64-bit hardware and a 64-bit edition of the Windows Server operating system. A 32-bit edition of Lync Server 2013 is not available with this release.

Standard Edition and Enterprise Edition server can use any of the following:

- Windows Server 2008 R2 SP1 or latest service pack
- Windows Server 2012

Install the operating system software on the Standard Edition Server or Enterprise Edition Front End Server. Apply all updates in order to bring the operating system up to the latest update and required update level consistent with your organization’s standards. For more details about the operating requirements, see Server and Tools Operating System Support in the Supportability documentation.

Additional Software for Lync Server 2013

In addition to the updates required for the operating system, Lync Server 2013 requires operating system roles, features, and software to operate. For details about the additional software that must be installed prior to publishing your topology and installing Lync Server 2013, see Additional Software Requirements in the Planning documentation.

Additional Software Necessary for All Server Roles

On all server roles, you must also make sure that Windows PowerShell command-line interface 3.0 and Microsoft .NET Framework 4.5 are installed.

Additionally, Windows PowerShell command-line interface 3.0 and Microsoft .NET Framework 4.5 are required on any computer where you will run the Lync Server administrative tools.

Windows PowerShell 3.0

Lync Server 2013 requires you to install Windows PowerShell 3.0 on each computer that will take part in your Lync Server topology. For details about installing Windows PowerShell 3.0, see Installing Windows PowerShell 3.0.

Note:
On Windows Server 2008 R2 with SP1, Windows PowerShell command-line interface 3.0 cannot be installed before installing Microsoft .NET Framework 4.5.

Microsoft .NET Framework 4.5

When you install Microsoft .NET Framework 4.5 on servers that will run Lync Server 2013 and Windows Server 2012, you must perform one additional step. After .NET Framework 4.5 is installed, use Server Manager to install HTTP Activation.

To Install .NET 4.5 HTTP Activation on Windows Server 2012

1. From the **Start** menu, click **Programs**, then click **Administrative Tools**, then click **Server Manager**.
2. In Server Manager, under **Features Summary**, choose **Add Features**.
3. Expand **.NET Framework 4.5**.
4. Select **WCF Activation** if it isn't already selected. Then select **HTTP Activation**.
5. Click **Next** and follow the prompts to finish the installation.

1.4.1.2.3 System Requirements for SQL Server

System Requirements for SQL Server

Deployment > Deploying Lync Server 2013 > System Requirements >

Topic Last Modified: *2012-09-13*

Before you deploy Enterprise Edition server, install Microsoft SQL Server 2008 R2 or Microsoft SQL Server 2012 on a dedicated computer that meets the hardware requirements. For details about hardware requirements, see Server Hardware Platforms in the Supportability documentation. For details about software requirements, see Database Software Support in the Supportability documentation.

Before you create the Front End pool, you must also configure Windows Firewall to allow Lync Server 2013 access to SQL Server over specific ports by defining ports for the server using SQL Server Configuration Manager and opening ports in Windows Firewall with Advanced Security.

1.4.1.2.4 System Requirements for Administration Tools

System Requirements for Administration Tools

Deployment > Deploying Lync Server 2013 > System Requirements >

Topic Last Modified: *2012-06-29*

The following topics describe the requirements for installing the administration tool and publishing a topology.

- Administrative Tools Software Requirements

- Requirements to Publish a Topology

1.4.1.2.4.1 Administrative Tools Software Requirements

Administrative Tools Software Requirements

Deploying Lync Server 2013 > System Requirements > System Requirements for Administration Tools >

Topic Last Modified: *2013-02-21*

This topic describes the software required to install and use Lync Server 2013 administrative tools in addition to the operating system requirements.

Microsoft .NET Framework 4.5

The 64-bit edition of Microsoft .NET Framework 4.5 is required for Lync Server 2013.

Windows PowerShell 3.0

Windows PowerShell 3.0 is required for running any component of Microsoft Lync Server 2013. For more information, see Installing Windows PowerShell 3.0.

Windows Installer Version 4.5

Lync Server 2013 uses Windows Installer technology to install, uninstall, and maintain various server roles. Windows Installer version 4.5 is available as a redistributable component for the Windows Server operating system. Windows Installer 4.5 ships with Windows Server 2012 and Windows Server 2008 R2, meaning that you do not need to download the utility for any computer that is running Lync Server 2013. (Lync Server 2013 can only be installed on computers running Windows Server 2012 or Windows Server 2008 R2.)

However, if you want to install Lync Server Management Shell or Lync Server Topology Builder on an administrator workstation you might need to download Windows Installer 4.5. That utility ships with Windows 7 and Windows 2008 R2 but not with any previous versions of the Windows operating system. You can download Windows Installer 4.5 from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?linkid=197395.

Microsoft Silverlight 5 browser plug-in

Lync Server 2013 Control Panel is a web-based tool and requires that you install the latest version of Microsoft Silverlight 5 browser plug-in. When you start Lync Server 2013 Control Panel, if this software is not installed or if an earlier version is installed, Lync Server 2013 Control Panel prompts you to install the required version.

⊟See Also

Concepts

Server and Tools Operating System Support

Other Resources

Administrative Tools Infrastructure Requirements
Administrator Rights and Permissions Required for Setup and Administration

1.4.1.2.4.2 Requirements to Publish a Topology

Requirements to Publish a Topology

See Also

Deploying Lync Server 2013 > System Requirements > System Requirements for Administration Tools >

Topic Last Modified: *2013-02-21*

This topic describes the infrastructure and software requirements that are specific to publishing a topology, whether by using Topology Builder or the Lync Server 2013 Management Shell command-line interface. These requirements are in addition to the general operating system, software, and permissions requirements applicable to all Lync Server 2013 administrative tools. Make sure that you satisfy all administrative tools requirements before you publish a topology.

- You must run Topology Builder on a computer that is joined to the same domain or forest of the Lync Server 2013 deployment you are creating so that Active Directory Domain Services (AD DS) preparation steps are already completed, enabling you to use the administrative tools on that computer to successfully publish your topology.
- The computers defined in the topology must be joined to the domain, except for Edge Servers, and in AD DS. However, the computers do not need to be online when you publish the topology.
- The file share for the pool must be created and available to remote users.
- In order to publish an Enterprise Edition Front End pool, the SQL Server-based Back End Server must be joined to the domain in which you are deploying the servers, online, and configured with the appropriate firewall rules to make it available to remote users. For details about specifying firewall exceptions, see Understanding Firewall Requirements for SQL Server. For other details about configuring SQL Server, see Configure SQL Server for Lync Server 2013.

Note:

Standard Edition server has a collocated database that will accept the published configuration. You must first run the **Prepare first Standard Edition server** setup task in the Lync Server Deployment Wizard.

Tasks

Publish the Topology
Delegate Setup Permissions

Concepts

Administrative Tools Software Requirements
Server and Tools Operating System Support

Other Resources

Administrator Rights and Permissions Required for Setup and Administration

1.4.1.2.5 DNS Requirements

DNS Requirements

Deployment > Deploying Lync Server 2013 > System Requirements >

Topic Last Modified: *2012-06-29*

The following topics describe the DNS requirements for a Front End pool and Standard Edition Server.

- DNS Requirements for Front End Pool
- DNS Requirements for a Standard Edition Server

1.4.1.2.5.1 DNS Requirements for Front End Pool

DNS Requirements for Front End Pool

Deploying Lync Server 2013 > System Requirements > DNS Requirements >

Topic Last Modified: *2012-11-07*

To successfully complete this procedure, you should be logged on to the server or domain minimally as a member of the Domain Admins group or a member of the DnsAdmins group.

You need to configure the required Domain Name System (DNS) records prior to publishing your topology in Topology Builder. Additionally, some of the fully qualified domain names (FQDNs) used in the configuration of a Lync Server 2013 deployment are logical and not physical server FQDNs, so additional DNS configuration is required prior to publishing.

⚠**Warning:**

Lync Server 2013 does not support single-labeled domains. For example, a forest with a root domain named **contoso.local** is supported, but a root domain named **local** is not supported. For details, see Microsoft Knowledge Base article 300684, "Information about configuring Windows for domains with single-label DNS names," at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=300684.

◆**Important:**

The name you specify must be identical to the computer name configured on the server. By default the computer name of a computer that is not joined to a domain is a short name, not an FQDN. Topology Builder uses FQDNs, not short names. **Use only standard characters** (including A–Z, a–z, 0–9, and hyphens) when assigning FQDNs of your servers running Lync Server, Edge Servers, and pools. Do not use Unicode characters or underscores. Nonstandard characters in an FQDN are often not supported by external DNS and public certification authorities (CAs) (when the FQDN must be assigned to the SN in the certificate).

Prior to operating the topology after it has been deployed, ensure that the following Active Directory and DNS records are created (as your needs for specific features dictate):

- Each server role that will exist in the topology is published as an Active Directory object (joining the computer to the domain will accomplish this).
- A DNS A Record exists for each server.
- A DNS SRV Record exists for each SIP domain if you plan to use automatic logon for clients in the form of _sipinternaltls_tcp.<*SIP domain*>. If you will use manual configuration for clients, this record is not necessary.
- A DNS A Record for each configured simple URL, of which there are typically four: meet, dialin, lwa, and scheduler. Additionally, there is the admin simple URL which is a special URL for access to the Lync Server 2013 Control Panel.
- The server running SQL Server must be joined to the domain, and reachable by the computer that Topology Builder is publishing from.

The table follows the reference architectures presented in the Planning section. For details, see Scenarios for External User Access in the Planning documentation.

DNS Records Required for the Front End pool

Location	Type	FQDN	Maps to/Comments
Internal DNS	A	pool01.contoso.net	Pool01 (DNS load balancing). Requires a DNS A record for the IP address of each Front End Server within the pool,

			mapping to the pool FQDN.
Internal DNS	A	pool01.contoso.net	Pool01 (virtual IP (VIP) of hardware load balancer).
Internal DNS	A	fe01.contoso.net fe02.contoso.net fe03.contoso.net …	Pool01 Front End Server (NODE 1). Pool01 Front End Server (NODE 2). Pool01 Front End Server (NODE 3). …
Internal DNS	A	fe02.contoso.net	Pool01 Front End Server (NODE 2).
Internal DNS	A	lsweb.contoso.net	Pool01 (VIP) for client-to-server web traffic.
Internal DNS	A	sqlbe.contoso.net	Pool01 Back End Server running SQL Server 2008 R2.
Internal DNS	A	sip.contoso.com	Required for Lync Phone Edition, or automatic logon of clients without DNS SRV records, and for strict domain matching. Not required in all cases.
Internal DNS	A	sip.fabrikam.com	Assumes a second SIP domain. Required for Lync Phone Edition, automatic logon of clients without DNS SRV records, and for strict domain matching. Not required in all cases.
Internal DNS	A	dialin.contoso.com	Simple URL for dial-in conferencing published internally – Front End Server (or Director, if installed) responds to simple URL queries.
Internal DNS	A	meet.contoso.com	Simple URL for conferences published internally – Front End Server (or Director, if installed)

			responds to simple URL queries.
Internal DNS	A	admin.contoso.com admin	Optional record, simple URL for Lync Server 2013 Control Panel published internally - Front End Server (or Director, if installed) responds to simple URL queries. Host name only (no domain name) is recommended.

Note:
VIP = Virtual IP address for hardware load balancer

DNS SRV Records for the Front End pool

Location	**Type**	**FQDN**	**Target FQDN**	**Port**	**Maps to/ Comments**
Internal DNS	SRV	_sipinternaltls._tcp.contoso.com	pool01.contoso.com	5061	Required for automatic configuration of Lync 2013 clients to work internally.
Internal DNS	SRV	_sipinternaltls._tcp.fabrikam.com	pool01.fabrikam.com	5061	Required for automatic configuration of Lync 2013 clients to work internally.
Internal DNS	SRV	_ntp._udp.contoso.com	dc01.contoso.com	123	Network Time Protocol (NTP) source required for devices running Lync Phone Edition. Internally, this should point to the domain controller. If the domain controller is not defined, it will try to use the NTP server time.windows.com.

1.4.1.2.5.2 DNS Requirements for a Standard Edition Server

DNS Requirements for a Standard Edition Server

See Also

Deploying Lync Server 2013 > System Requirements > DNS Requirements >

Topic Last Modified: *2013-02-22*

This section describes the Domain Name System (DNS) records that are required for deployment of Standard Edition servers.

DNS Records for Standard Edition Servers

The following table specifies DNS requirements for Lync Server 2013 Standard Edition server deployment.

Deployment scenario	DNS requirement
Standard Edition server	An internal A record that resolves the fully qualified domain name (FQDN) of the server to its IP address.
Automatic client sign-in	For each supported SIP domain, an SRV record for _sipinternaltls._tcp.<domain> over port 5061 that maps to the FQDN of the Standard Edition server that authenticates and redirects client requests for sign-in. For details, see DNS Requirements for Automatic Client Sign-In.
Device Update Web service discovery by unified communications (UC) devices	An internal A record with the name ucupdates-r2.<SIP domain> that resolves to the IP address of the Standard Edition server hosting Device Update Web service. In the situation where a UC device is turned on, but a user has never logged into the device, the A record allows the device to discover the server hosting Device Update Web service and obtain updates. Otherwise, devices obtain the server information though in-band provisioning the first time a user logs in. For details, see Device Update Web Service in the Operations documentation.
A reverse proxy to support HTTP traffic	An external A record that resolves the external web farm FQDN to the external IP address of the reverse proxy. Clients and UC devices use this record to connect to the reverse proxy. For details, see Determine DNS Requirements in the Planning documentation.

⊟See Also

Concepts

DNS Requirements for Automatic Client Sign-In
Determine DNS Requirements

Other Resources

Device Update Web Service

1.4.1.3 Preparing the Infrastructure and Systems

Preparing the Infrastructure and Systems

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2013-02-21*

Deployment of Lync Server 2013 requires the use of Topology Builder to define and publish the topology design. To identify the components required for your topology, you use Topology Builder to create and save a topology design. Prior to publishing your topology in Topology Builder, you do the following:

- Acquire and install the hardware for each component in the topology design that you created and saved by using Topology Builder, including all required computers (servers running Lync Server 2013, database servers, servers running Internet Information Services (IIS), and reverse proxy servers, as appropriate), network adapters, hardware load balancers, and storage devices (such as file servers). For details about how to define a topology that specifies the components needed for your deployment, see Defining and Configuring the Topology. For details about hardware requirements for servers, see Supported Hardware in the Supportability documentation.
- Make sure that the networking infrastructure meets requirements. For details, see Network Infrastructure Requirements in the Planning documentation.
- Set up Active Directory Domain Services (AD DS). To publish and enable the topology, you need the internal servers to be represented by computer accounts in AD DS. This is accomplished by joining the computers to AD DS. For details about preparing AD DS, see Preparing Active Directory Domain Services for Lync Server 2013.
- Create a file share. Standard Edition servers can host the file share for the required file, while in an Enterprise deployment the file share cannot be hosted on the front end server. The permissions and group memberships required for deploying and setting the access control list (ACL) on the folder and the share must be set correctly for Topology Builder to complete successfully. You should make sure that the person running Topology Builder has the following permissions and group memberships:
  - Member of Local Administrators
  - Member of Domain Users
  - Full Control on share and folder of file store
- For Enterprise Edition, install and configure SQL Server. For SQL Server setup to succeed the SQL Server-based server must be online and the person publishing the topology be a local admin on the SQL Server and must be a member of the SQL Server sysadmin group on the SQL Server instance.

After you complete all of the preparation tasks as described in this topic, but prior to publishing the topology, you also need to perform the other preparation tasks, including installing the Windows operating systems and other prerequisite software, setting up IIS, and configuring DNS. For details about these tasks, see System Requirements for Servers Running Lync Server 2013, Configure IIS, and Preparing the Infrastructure and Systems. Additionally, you should familiarize yourself with the clients and client requirements. For details, see Deploying Clients and Devices.

- Hardware Setup
- Software Setup
- Preparing Active Directory Domain Services for Lync Server 2013
- Configure SQL Server for Lync Server 2013
- Configure DNS Records for a Front End Pool or Standard Edition Server

- Install Lync Server Administrative Tools

1.4.1.3.1 Hardware Setup

Hardware Setup

Deployment > Deploying Lync Server 2013 > Preparing the Infrastructure and Systems >

Topic Last Modified: *2013-02-21*

Setting up the hardware and other components required in the infrastructure that you need to implement your topology requires that, prior to publishing your topology in Topology Builder, you do the following:

- Install the hardware for each component in the topology design that you created and saved by using Topology Builder, including all required computers (servers running Lync Server 2013, database servers, servers running Internet Information Services (IIS), and reverse proxy servers, as appropriate), network adapters, hardware load balancers, and storage devices (such as file servers). Confirm that you have followed the recommendations for the number and speed for network adapters. If you will be using hardware load balancers, make sure that you have the proper information from the vendor to configure them for use with Lync Server 2013. If you will be using a file server or other server to house the file share required by Lync Server, make sure that the server is available and ready for the configuration of the file share. For details about how to define a topology that specifies the components needed for your deployment, see Defining and Configuring the Topology. For details about hardware requirements for servers, see Supported Hardware in the Supportability documentation.
- Make sure that the networking infrastructure meets requirements. For details, see Network Infrastructure Requirements in the Planning documentation.
- Set up Active Directory Domain Services (AD DS). Setting up AD DS includes preparing AD DS and defining all components that you want to deploy in AD DS. For details about preparing AD DS, see Preparing Active Directory Domain Services for Lync Server 2013 in the Deployment documentation.
- Set up the required permissions for creating the file share. Permissions for use of file shares by Lync Server 2013 are automatically configured by Topology Builder when you publish your topology. However, the user account used to publish the topology must have full control (read/write/modify) on the file share in order for Topology Builder to configure the required permissions. To make sure that the file share can be managed properly during the Topology Builder publishing process, the user or domain group that the user is a member of should be made a member of the local Administrators group on the machine where the file share is located. In a multi-domain scenario, Domain A user or group should be made a member of the local Administrators group on the machine in Domain B where the file share will be located.
  For details about updating using file shares in a Distributed File System (DFS), see Configure File Storage.

⚠**Warning:**
The file share for Lync Server 2013, Enterprise Edition cannot be located on the Front End Server.

- Install and set up the hardware load balancer for Web Services. With Domain Name System (DNS) load balancing deployed, you still need to also use hardware load balancers for these pools, but only for HTTP/HTTPS traffic. The hardware load balancer is used for HTTPS traffic from clients over ports 443 and 80. Although you still need hardware load balancers for these pools, their setup and administration will be primarily for HTTP/HTTPS traffic, which the administrators of the hardware load balancers are accustomed to.

After you complete all of the preparation tasks as described in this topic, but prior to publishing the topology, you also need to:

- Install Operating Systems and Prerequisite Software on Servers
- Configure IIS
- Configure SQL Server for Lync Server 2013
- Configure DNS Records for a Front End Pool or Standard Edition Server

1.4.1.3.2 Software Setup

Software Setup

Deployment > Deploying Lync Server 2013 > Preparing the Infrastructure and Systems >

Topic Last Modified: *2012-06-29*

This section details the software setup that is required after you have setup the hardware in your environment.

- Install Operating Systems and Prerequisite Software on Servers
- Configure File Storage
- Request Certificates in Advance (Optional)
- Configure IIS
- Installing Windows PowerShell 3.0

1.4.1.3.2.1 Install Operating Systems and Prerequisite Software on Servers

Install Operating Systems and Prerequisite Software on Servers

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Software Setup >

Topic Last Modified: *2012-10-21*

After you have set up the hardware and system infrastructure, you need to install the appropriate Windows operating systems and updates, in addition to all other prerequisite software on each server that you are deploying. This includes each Lync Server 2013 server role and any additional infrastructure servers or servers running SQL Server that are required for your deployment.

Note:

This section describes installation of operating systems and prerequisite software for internal servers. If you are deploying Edge Servers to support external user access, you also need to install operating systems and prerequisite software for those servers, including Edge Servers and reverse proxy servers. For details about preparing servers to support external user access, see Preparing for Installation of Servers in the Perimeter Network in the Deployment documentation.

Install Windows Operating Systems on Servers

On each server that you are deploying, install the appropriate Windows operating system as follows:

- **Servers running Lync Server 2013** For details about the operating system requirements for servers running Lync Server 2013, see Server and Tools Operating System Support in the Supportability documentation.
- **Database servers** For details about operating system requirements for

database servers, including the back-end database, Archiving database, and Monitoring database, see the SQL Server documentation. For SQL Server 2012, see the SQL Server 2012 Books Online at http://go.microsoft.com/fwlink/p/?linkId=218015.

Note:

If you are installing Lync Server 2013 on Windows Server 2008 R2 with SP1, you must first install the update described in the Microsoft Knowledge Based article 2646886, "FIX: Heap corruption occurs when a module calls the InsertEntityBody method in IIS 7.5", at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=2646886.

Install Windows Update on Servers

Install the following updates from Windows Update on each server:

- **Windows Update for servers running Lync Server 2013** For details about the updates from Windows Update that are required for servers running Lync Server 2013, see Additional Software Requirements in the Planning documentation.
- **Database servers** For details about the updates from Windows Update that are required for database servers, including the back-end database, Archiving database, and Monitoring database, see the SQL Server 2012 documentation. For SQL Server 2012, see the SQL Server 2012 Books Online at http://go.microsoft.com/fwlink/p/?linkId=218015.

Install Other Prerequisite Software on Servers

Lync Server 2013 requires the installation of the following additional software on servers:

- **Prerequisite software for servers running Lync Server 2013** The additional software prerequisites for servers running Lync Server 2013 depend on the server role being deployed. For details about the specific software requirements for each server, see Additional Software Requirements in the Planning documentation.
- **Windows Identity Foundation** Lync Server 2013 requires the installation of Windows Identity Foundation in order to support server-to-server authentication scenarios. To verify that it has already been installed on your computer, go to Control Panel, click **Programs and Features**, **View installed updates**, and look under **Microsoft Windows**. For details about installing Windows Identity Foundation, see http://go.microsoft.com/fwlink/p/?linkId=204657.
- **Microsoft .NET Framework 4.5** The 64-bit edition of Microsoft .NET Framework 4.5 is required for Lync Server 2013.
- **Prerequisite software for database servers** For details about the Windows Update required for database servers, including the back-end database, Archiving database, and Monitoring database, see the SQL Server 2012 documentation at http://go.microsoft.com/fwlink/p/?linkId=218015.

  Note:

  Lync Server 2013 automatically installs Microsoft SQL Server 2012 Express on each Standard Edition server and each server running Lync Server 2013 on which the local configuration store is located.
- **Windows Desktop Experience** All Front End Servers and Standard Edition servers where conferencing will be deployed must have the Windows Media Format Runtime installed, which is installed as part of the Windows desktop experience, except for Windows Server 2012. Windows Server 2012 requires Microsoft Media Foundation. The Windows Media Format Runtime is required to run the Windows Media Audio (.wma) files that the Call Park, Announcement, and Response Group applications play for announcements and music.

We recommend that you install Windows desktop experience before you install Lync Server 2013. If Lync Server 2013 does not find this software on the server, it will prompt you to install it, and then you must restart the server to complete installation.

1.4.1.3.2.2 Installing Windows PowerShell 3.0

Installing Windows PowerShell 3.0

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Software Setup >

Topic Last Modified: *2013-02-21*

Lync Server 2013 requires the 5/31/2012 version of Windows PowerShell 3.0 on each computer that will take part in your Lync Server topology. When the final version of Lync Server 2013 is released, it is expected that Windows PowerShell 3.0 will ship with the product, and, if necessary, be installed at the same time that you install Lync Server itself. For the Lync Server 2013 release, however, you will need to download and install Windows PowerShell 3.0 yourself.

The 5/31/2012 release of Windows PowerShell 3.0 can be found in the Microsoft Downloads Center at (http://go.microsoft.com/fwlink/p/?LinkId=268538). You should download the file Windows6.1-KB2506143-x64.msu from the Downloads Center and then save a copy of that file to each computer where you need to install Windows PowerShell 3.0. It is also recommended that you uninstall any previous version of Windows PowerShell 3.0 before installing the 5/31/2012 release. To uninstall a previous version of Windows PowerShell 3.0 complete the following procedure on each computer where the previous version has been installed:

1. In the Windows Control Panel, click **Uninstall a Program**.
2. In Programs and Features, click **View installed updates**.
3. In the **Uninstall an update** pane, in the **Microsoft Windows** section, locate the update titled **Microsoft Windows Management Framework 3.0 Beta (KB2506143)**.
4. Right-click **Microsoft Windows Management Framework 3.0 Beta (KB2506143)** and then click **Uninstall**.
5. In the **Uninstall an update** dialog box, click **Yes**.

Note that you will need to restart the computer after the update has been uninstalled.

After the computer has restarted, you can install the 5/31/2012 release of Windows PowerShell 3.0 by completing the following procedure on each computer where Lync Server 2013 will be installed:

1. Double-click the file **Windows6.1-KB2506143-x64.msu**.
2. In the **Windows Update Standalone Installer** dialog box, click **Yes** when asked if you want to install the update.
3. In the Download and Install Update wizard, on the **Read these license terms** page, click **I Accept**.
4. On the **Installation complete** page, click **Restart Now** to immediately restart your computer. (Your computer must be restarted in order for the updates to take effect.) If you prefer not to immediately restart your computer, click **Close**. As noted, you will still need to restart the computer before Windows PowerShell 3.0 is fully installed.

After the computer has restarted you can verify that Windows PowerShell 3.0 has been installed by completing the following check:

1. Click **Start**, click **All Programs**, click **Accessories**, click **Windows PowerShell**, and then click **Windows PowerShell**.
2. In the Windows PowerShell console, type the following command at the command prompt and then press ENTER:

```
Get-Host | Select-Object Version
```

3. If Windows PowerShell 3.0 has been installed you will see output that looks like this:

```
Version
-------
3.0
```

Assuming your computer meets all the other prerequisites you can now install Lync Server 2013.

1.4.1.3.2.3 Configure File Storage

Configure File Storage

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Software Setup >

Topic Last Modified: *2012-09-13*

Lync Server 2013 supports using file shares on a Distributed File System (DFS). For details about DFS for Windows Server 2008, see the DFS Step-by-Step Guide for Windows Server 2008 at http://go.microsoft.com/fwlink/p/?linkId=202835.To use a DFS, Lync Server 2013 requires the following:

- Namespaces are domain based
- All namespace servers are running a minimum of Windows 2008

Lync Server 2013 setup requires that permissions on shared folder allow full access to Administrator. Lync Server 2013 will then use NTFS file permissions to ACL the folders. Inherited DFS share permissions will not be used to restrict access.

For more details about File Share requirements, see File Storage Support in the Supportability documentation.

The following procedure describes how to correctly configure shared folder permissions using the DFS Namespace Wizard (as described in DFS setup guide).

⊟To configure shared folder permissions

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree of the DFS Management snap-in, right-click the namespace server (for example filesrv1.contoso.com), and then click **Edit Settings**.
3. Select **Shared Folder Permissions**.
4. Select **Use Custom Permissions**.
5. For the Administrator group, select the following under **Allow**:
   - **Full Control**
   - **Change**
   - **Read**
6. Click **Apply**, and then click **OK**.

1.4.1.3.2.4 Request Certificates in Advance (Optional)

Request Certificates in Advance (Optional)

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Software Setup >

Topic Last Modified: *2013-02-21*

Certificates are required for all internal servers that are running Lync Server 2013, including each Enterprise Edition Front End Server, Standard Edition server, Director, Edge Server and stand-alone Mediation Server. Although an internal enterprise certification authority (CA) is recommended for internal servers, you can also use a public CA. For details about certificate requirements and about the use of a public CA, see Certificate Requirements for Internal Servers in the Planning documentation.

Lync Server 2013 setup includes the Certificate Wizard, which facilitates the tasks of requesting, assigning, and installing certificates during deployment. If you want to request certificates prior to installing servers (for instance, to save time during actual deployment of servers), you can do so by using a computer on which the Lync Server 2013 administrative tools are installed or by using a certificate request procedure defined in your organization, as long as you make sure that the certificates are exportable and contain all the required subject alternative names. Requesting certificates in advance is optional. If you do not request them in advance, you must request them as part of the setup of each server that requires a certificate.

This Deployment documentation provides procedures for using the Certificate Wizard to request certificates as part of the setup process, as described in the Configure Certificates for Servers, Configure Certificates for the Director, and Install the Files for Mediation Server sections of this Deployment documentation. If you request certificates in advance, you must modify the certificate deployment procedures in those sections as appropriate to importing and assigning the certificates instead of requesting them at the time of deployment.

Note:

Lync Server 2013 includes support for SHA-256 certificates for connections from clients running the Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7 operating systems, and Lync Phone Edition. To support external access using SHA-256, the external certificate is issued by a public CA using SHA-256.

1.4.1.3.2.5 Configure IIS

Configure IIS

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Software Setup >

Topic Last Modified: *2011-12-16*

Configuring Internet Information Services (IIS) for Lync Server 2013 involves installing the correct components to support the Web Services needed by Lync Server 2013. For details about installing IIS, see IIS Configuration. If you have a policy to run the Security Configuration Wizard on servers before putting them into service or as a typical part of your maintenance, see Re-Activate Server After Security Configuration Wizard Closes Ports in IIS for information about a side effect of running the wizard that will close ports on a Lync Server 2013 IIS configuration.

In This Section

- IIS Configuration
- Re-Activate Server After Security Configuration Wizard Closes Ports in IIS

IIS Configuration

See Also

Preparing the Infrastructure and Systems > Software Setup > Configure IIS >

Topic Last Modified: *2013-02-25*

To successfully complete this procedure, you should be logged on to the server minimally as a local administrator and a domain user.

Before you configure and install the Front End Server for Lync Server 2013, Standard Edition or the first Front End Server in a pool, you install and configure the server role and Web Services for Internet Information Services (IIS).

Important:

If your organization requires that you locate IIS and all Web Services on a drive other than the system drive, you can change the installation location path for the Lync Server 2013 files in the Setup dialog box when you initially install the Lync Server 2013 Administrative tools. You install the Administrative tools before installing IIS. If you install the Setup files to this path, including OCSCore.msi, the rest of the Lync Server 2013 files will be deployed to this drive as well. For dtails, see Install Lync Server Administrative Tools. For details about how to relocate the INETPUB deployed by Windows Server Manager when installing IIS, see http://go.microsoft.com/fwlink/p/?linkId=216888.

The following table indicates the required IIS 7.5 role services.

IIS 7.5 Role Services

Role Heading	Role Service
Common HTTP features installed	Static content
Common HTTP features installed	Default document
Common HTTP features installed	HTTP errors
Application development	ASP.NET Windows Server 2012 also requires ASP.NET4.5
Application development	.NET extensibility
Application development	Internet Server API (ISAPI) extensions
Application development	ISAPI filters
Health and diagnostics	HTTP logging
Health and diagnostics	Logging tools
Health and diagnostics	Tracing
Security	Anonymous authentication (installed and enabled by default)
Security	Windows authentication
Security	Client Certificate Mapping authentication
Security	Request filtering
Performance	Static content compression Dynamic content compression
Management Tools	IIS Management Console
Management Tools	IIS Management Scripts and Tools

On the Windows Server 2008 R2 SP1 x64 operating system, you can use Windows PowerShell 2.0. You must first import the ServerManager module, and then install the IIS 7.5 role and role services.

```
Import-Module ServerManager
```

```
Add-WindowsFeature Web-Server, Web-Static-Content, Web-Default-Doc, Web-Scripting
 Web-Asp-Net, Web-Log-Libraries, Web-Http-Tracing, Web-Stat-Compression, Web-Dyn-
 Web-ISAPI-Filter, Web-Http-Errors, Web-Http-Logging, Web-Net-Ext, Web-Client-Aut
 Web-Mgmt-Console
```

Note:

Anonymous authentication is installed by default with the IIS server role. You can manage anonymous authentication after the installation of IIS. For details, see "Enable Anonymous Authentication (IIS 7)" at http://go.microsoft.com/fwlink/p/?linkId=203935.

The following table indicates the required IIS 8.0 role services for Windows Server 2012.

IIS 8.0 Role Services

Role Heading	Role Service
Web Server (IIS)	Web Server
Common HTTP Features	Default Document
Common HTTP Features	Directory Browsing
Common HTTP Features	HTTP Errors
Common HTTP Features	Static content
Common HTTP Features	HTTP Redirection
Health and Diagnostics	HTTP Logging
Health and Diagnostics	Logging Tools
Health and Diagnostics	Request Monitor
Health and Diagnostics	Tracing
Security	Request Filtering
Security	Basic Authentication
Security	Client Certificate Mapping Authentication
Security	Windows Authentication
Application Development	.Net Extensibility 3.5
Application Development	.Net Extensibility 4.5
Application Development	ASP.Net 3.5
Application Development	ASP.Net 4.5
Application Development	ISAPI Extensions
Application Development	ISAPI Filters
Application Development	Server Side Includes
Management Tools	IIS Management Console

Management Tools	IIS 6 Metabase compatibility
Management Tools	IIS Management Scripts and Tools
.Net 3.5 Framework Features	.Net 3.5 Framework
.Net 4.5 Framework Features	.Net Framework 4.5
.Net 4.5 Framework Features	ASP.Net 4.5
.Net 4.5 Framework Features	HTTP Activation
.Net 4.5 Framework Features	TCP Port Sharing
Background Intelligent Transfer Service	IIS Server Extensions
Ink and Handwriting Services	Ink and Handwriting Services
Media Foundation	Media Foundation
User Interfaces and Infrastructure	Graphical Management Tools and Infrastructure
User Interfaces and Infrastructure	Desktop Experience
User Interfaces and Infrastructure	Server Graphical Shell
Windows Identity Foundation 3.5	Windows Identity Foundation 3.5
Windows Process Activation Service	Process Model
Windows Process Activation Service	Configuration APIs

In Windows Server 2012, you can use Windows PowerShell 3.0 to install the IIS Requirements. Using the ServerManager module in Windows PowerShell 3.0, type:

```
Import-Module ServerManager
```

```
Add-WindowsFeature Web-Server, Web-Static-Content, Web-Default-Doc, Web-Http-Erro
 Web-Net-Ext, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Http-Logging, Web-Log-Librarie
 Web-Http-Tracing, Web-Basic-Auth, Web-Windows-Auth, Web-Client-Auth, Web-Filteri
 Web-Dyn-Compression, NET-Framework-45-Core, NET-WCF-HTTP-Activation45, Web-Asp-N
 Web-Scripting-Tools, Web-Mgmt-Console Web-Mgmt-Compat, Windows-Identity-Foundati
 BITS -Source D:\sources\sxs
```

Important:

New to Windows Server 2012 is the –Source parameter that defines where the Windows Server 2012 source media can be found. The media can be defined as a DVD drive (for example, D:\Sources\Sxs), or to a network share that the media files have been copied (for example, \\fileserver\windows2012\sources\Sxs).

Concepts

IIS Requirements for Front End Pools and Standard Edition Servers

Re-Activate Server After Security Configuration Wizard Closes Ports in IIS

Preparing the Infrastructure and Systems > Software Setup > Configure IIS >

Topic Last Modified: *2012-10-01*

Some Lync Server 2013 roles run Web Services on Internet Information Services (IIS) port

4443. Running the Lync Server Deployment Wizard, Bootstrapper.exe, or using the **Enable-CsComputer** cmdlet creates an exception in the firewall and opens the port. If you then run the Windows Server 2008 R2 Security Configuration Wizard (or other hardening scripts), port 4443 will be blocked, and external clients will not be able to contact Web Services. To reopen the port you can either modify the firewall exception directly or re-activate the server.

⊟To re-activate the server by using the Deployment Wizard

1. On the Lync Server Deployment Wizard page, click **Run** next to **Step 2: Setup or Remove Lync Server Components**.
2. On **Setup Lync Server components** page, click **Next**.
3. On the **Executing Commands** page, when the task status is shown as completed, click **Finish**.

> **Note:**
> You can also use bootstrapper.exe or **Enable-CsComputer** to re-activate the server.

1.4.1.3.3 Preparing Active Directory Domain Services for Lync Server 2013

Preparing Active Directory Domain Services for Lync Server 2013

Deployment > Deploying Lync Server 2013 > Preparing the Infrastructure and Systems >

Topic Last Modified: *2013-02-21*

Before you deploy and operate Lync Server 2013, you must prepare Active Directory Domain Services (AD DS) by extending the schema and then creating and configuring objects. The schema extensions add the Active Directory classes and attributes that are required by Lync Server.

The topics in this section describe how to prepare AD DS for deploying Lync Server and how to assign setup and organizational unit (OU) permissions. For details about the schema changes required for Lync Server, see Active Directory Schema Extensions, Classes, and Attributes Used by Lync Server 2013.

- Active Directory Infrastructure Requirements
- Overview of Active Directory Domain Services Preparation
- Preparing Active Directory Domain Services
- Preparing a Locked-Down Active Directory Domain Services
- Granting Permissions

1.4.1.3.3.1 Active Directory Infrastructure Requirements

Active Directory Infrastructure Requirements

Planning > Determining Your Infrastructure Requirements > Active Directory Domain Services Requirements, Support, and Topologies >

Topic Last Modified: *2012-11-27*

Before you start the process of preparing Active Directory Domain Services (AD DS) for Lync Server 2013, make sure that your Active Directory infrastructure meets the following prerequisites:

- All domain controllers (which include all global catalog servers) in the forest where you deploy Lync Server run one of the following operating systems:

  - Windows Server 2012 operating system
  - Windows Server 2008 R2 operating system
  - Windows Server 2008 operating system
  - Windows Server 2008 Enterprise 32-Bit
  - 32-bit or 64-bit versions of the Windows Server 2003 R2 operating system
  - 32-bit or 64-bit versions of the Windows Server 2003 operating system

- All domains in which you deploy Lync Server are raised to a domain functional level of Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or at least Windows Server 2003.
- The forest in which you deploy Lync Server is raised to a forest functional level of Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or at least Windows Server 2003.

  Note:

  To change your domain or forest functional level, see "Raising domain and forest functional levels" in the TechNet Library at http://go.microsoft.com/fwlink/p/?LinkId=263775.

- A global catalog is deployed in every domain where you deploy Lync Server computers or users.

Lync Server 2013 supports the universal groups in the Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003 operating systems. Members of universal groups can include other groups and accounts from any domain in the domain tree or forest and can be assigned permissions in any domain in the domain tree or forest. Universal group support, combined with administrator delegation, simplifies the management of a Lync Server deployment. For example, it is not necessary to add one domain to another to enable an administrator to manage both.

1.4.1.3.3.2 Overview of Active Directory Domain Services Preparation

Overview of Active Directory Domain Services Preparation

See Also

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 >

Topic Last Modified: *2012-10-29*

To prepare Active Directory Domain Services (AD DS) for your Lync Server 2013 deployment, you must perform three steps in a specific sequence.

The following table describes the steps required to prepare AD DS for Lync Server.

Active Directory Preparation Steps

	Step	Description	Where run
1.	Preparing the Active Directory Schema	Extends the Active Directory schema by adding new classes and attributes that are used by Lync Server. Run once for each forest in your deployment where	Against the schema master in the root domain of each forest where Lync Server will be deployed. **Note:** You do not need to run this step in the root domain if you have permissions on

		Lync Server will be deployed.	the schema master, but you must be a member of the Schema Admins group in the root domain and a member of the Enterprise Admins group on the schema master. In a resource forest topology, run this step only in the resource forest, not in any user forests. In a central forest topology, run this step only in the central forest, not in any user forests.
2.	Preparing the Forest	Creates global settings and universal groups that are used by Lync Server. Run once for each forest in your deployment where Lync Server will be deployed.	In the root domain of each forest where Lync Server will be deployed. To run this step, you must be a member of the Enterprise Admins group. **Note:** In a resource forest topology, run this step only in the resource forest, not in any user forests. In a central forest topology, run this step only in the central forest, not in any user forests.
3.	Preparing Domains	Adds permissions on objects to be used by members of universal groups. Run once per user domain or server domain. **Note:** If you are migrating from Lync Server 2010 to Lync Server 2013, the Deployment Wizard may indicate that domain preparation is already complete. You do not need to run domain preparation again. Permissions were not	On a member server in each domain where Lync Server will be deployed. To run this step, you must be a member of the Domain Admins group.

		changed from Lync Server 2010 to Lync Server 2013.	

Lync Server 2013, like Lync Server 2010, stores much of the configuration information in the Central Management store instead of in AD DS as was the case in Office Communications Server 2007 R2. However, the following information is stored in AD DS:

- **Schema extensions**:
  - User object extensions
  - Extensions for Office Communications Server 2007 R2 classes to maintain backward compatibility
- **Data** (stored in Lync Server extended schema and in existing schema classes):
  - User SIP Uniform Resource Identifier (URI) and other user settings
  - Contact objects for applications such as Response Group and Conferencing Attendant
  - A pointer to the Central Management store
  - Kerberos Authentication Account (an optional computer object)

In Lync Server 2013, you delegate setup and administration by granting setup permissions to the RTCUniversalServerAdmins universal group so that members of that group can install and activate Lync Server 2013 on a local server (after the server has been added to the topology, published, and enabled). The delegated users must be local administrators on the computer where they are installing and activating Lync Server 2013, but they do not need to be members of the Domain Admins group. You can also grant permissions for objects in specified organizational units (OUs) so that members of the universal groups created during forest preparation can access those objects without being members of the Domain Admins group.

For new deployments of Lync Server 2013, global settings must be stored in the Configuration container. If your organization is upgrading from an earlier version and you still have global settings in the System container, the System container is still supported.

Concepts

Preparing the Active Directory Schema
Active Directory Schema Extensions, Classes, and Attributes Used by Lync Server 2013

Other Resources

Preparing the Forest
Preparing Domains

1.4.1.3.3.3 Preparing Active Directory Domain Services

Preparing Active Directory Domain Services

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 >

Topic Last Modified: *2012-10-29*

In Lync Server 2013, you can use the Lync Server Deployment Wizard to prepare Active Directory Domain Services (AD DS), or you can use Lync Server Management Shell cmdlets directly. You can also use the ldifde.exe command line tool directly on your domain controllers, as described later in this topic.

The Lync Server Deployment Wizard guides you through each Active Directory preparation task. The Deployment Wizard runs Lync Server Management Shell cmdlets. This tool is useful for environments with a single domain and single forest topology, or other similar topology.

Important:

You can deploy Lync Server in a forest or domain where domain controllers run 32-bit versions of some operating systems (for details, see Active Directory Infrastructure Requirements). However, you cannot use the Lync Server Deployment Wizard to run schema, forest, and domain preparation in these environments because the Deployment Wizard and supporting files are 64-bit only. Instead, you can use ldifde.exe and the associated .ldf files on a 32-bit domain controller to prepare the schema, forest and domain. See the section “Using Cmdlets and Ldifde.exe” later in this topic.

You can use Lync Server Management Shell cmdlets to run tasks remotely or for more complex environments.

Active Directory Preparation Prerequisites

You must run Active Directory preparation steps on a computer running Windows Server 2012 or Windows Server 2008 R2 with SP1 (64-bit). Active Directory preparation requires Lync Server Management Shell and OCSCore.

The following components are required to run Active Directory preparation tasks:

- Lync Server Core components (OCScore.msi)

  Note:

  If you plan to use Lync Server Management Shell for Active Directory preparation, you must run the Lync Server Deployment Wizard first to install Core components.

- Microsoft .NET Framework 4.5

  Note:

  For Windows Server 2012, you install and activate .NET Framework 4.5 by using Server Manager. For details, see "Microsoft .NET Framework 4.5" in Additional Software Requirements. For Windows Server 2008 R2, the file dotnetfx45.exe is provided in the \Setup\AMD64 directory of the installation media or download.

- Remote Server Administration Tools (RSAT)

  Note:

  Some RSAT tools are required if you run Active Directory preparation steps on a member server rather than on a domain controller. Install the AD DS snap-ins and command-line tools and the Active Directory Module for Windows PowerShell from the AD DS and AD LDS Tools node in Server Manager.

- Microsoft Visual C++ 11 Redistributable

  Note:

  Setup prompts you to install this prerequisite if it is not already installed on the computer. The package is supplied for you, and you will not have to acquire it separately.

- Windows PowerShell 3.0 (64-bit)

  For Windows Server 2012, Windows PowerShell 3.0 should be included with your Lync Server 2013 installation. For Windows Server 2008 R2, you need to install or upgrade to Windows PowerShell 3.0. For details, see Installing Windows PowerShell 3.0

Administrator Rights and Roles

The following table shows the administrative rights and roles required for each Active Directory preparation task.

User Rights Required for Active Directory Preparation

Procedure	Rights or roles
Schema preparation	Member of Schema Admins group for the forest root domain and administrator rights on the schema master
Forest preparation	Member of Enterprise Admins group for the forest
Domain preparation	Member of Enterprise Admins or Domain Admins group for the specified domain

Active Directory Preparation Cmdlets

The following table compares the Lync Server Management Shell cmdlets used to prepare AD DS to the LcsCmd commands used to prepare AD DS in Microsoft Office Communications Server 2007 R2.

Cmdlets Compared to LcsCmd

Cmdlets	LcsCmd
Install-CsAdServerSchema	Lcscmd /forest /action:SchemaPrep /SchemaType:Server
Get-CsAdServerSchema	Lcscmd /forest /action:CheckSchemaPrepState
Enable-CsAdForest	Lcscmd /forest /action:ForestPrep
Disable-CsAdForest	Lcscmd /forest /action:ForestUnprep
Get-CsAdForest	Lcscmd /forest /action:CheckForestPrepState
Enable-CsAdDomain	Lcscmd /domain /action:DomainPrep
Disable-CsAdDomain	Lcscmd /domain /action: DomainUnprep
Get-CsAdDomain	Lcscmd /domain /action:CheckDomainPrepState

Locked Down Active Directory Requirements

If permissions inheritance is disabled or authenticated user permissions must be disabled in your organization, you must perform additional steps during domain preparation. For details, see Preparing a Locked-Down Active Directory Domain Services.

Custom Container Permissions

If your organization uses custom containers instead of the three built-in containers (that is, Users, Computers, and Domain Controllers), you must grant read access to the custom containers for the Authenticated Users group. Read access to the containers is required for domain preparation. For details, see Preparing Domains.

Using Cmdlets and Ldifde.exe

The **Prepare Schema** step in the Lync Server Deployment Wizard and the **Install-CsAdServerSchema** cmdlet extend the Active Directory schema on domain controllers running a 64-bit operating system. If you need to extend the Active Directory schema on a domain controller running a 32-bit operating system, you can run the **Install-CsAdServerSchema** cmdlet remotely from a member server (recommended approach). If you need to run schema preparation directly on the domain controller, however, you can use the Ldifde.exe tool to import the schema files. The Ldifde.exe tool comes with most versions of the Windows operating system.

If you use Ldifde.exe to import the schema files, you must import all four files, regardless of whether you are migrating from a previous version or performing a clean installation. You must import them in the following sequence:

1. ExternalSchema.ldf
2. ServerSchema.ldf
3. BackCompatSchema.ldf
4. VersionSchema.ldf

Note:

The four .ldf files are located in \Support\Schema directory of your installation media or download.

To use Ldifde.exe to import the four schema files on a domain controller that is the schema master, use the following format:

```
ldifde -i -v -k -s <DCName> -f <Schema filename> -c DC=X <defaultNamingContext> -
```

For example:

```
ldifde -i -v -k -s DC1 -f ServerSchema.ldf -c DC=X "DC=contoso,DC=com" -j C:\Batc
```

Note:

Use the b parameter only if you are logged in as a different user. For details about the required user rights, see the "Administrator Rights and Roles" section earlier in this topic.

To use Ldifde.exe to import the four schema files on a domain controller that is not the schema master, use the following format:

```
ldifde -i -v -k -s <SchemaMasterFQDN> -f <Schema filename> -c DC=X <rootDomainNam
```

For details about using Ldifde, see Microsoft Knowledge Base article 237677, "Using LDIFDE to import and export directory objects to Active Directory," at http://go.microsoft.com/fwlink/p/?linkId=132204.

In This Section

- Preparing the Active Directory Schema
- Preparing the Forest
- Preparing Domains

Preparing the Active Directory Schema

See Also

Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 > Preparing Active Directory Domain Services >

Topic Last Modified: *2012-08-27*

Before you begin preparing Active Directory Domain Services (AD DS), you can open the schema files by using a text editor, such as Windows Notepad, or see Active Directory Schema Extensions, Classes, and Attributes Used by Lync Server 2013 to review all the Active Directory Domain Services (AD DS) schema extensions that will be modified for Lync Server 2013. Lync Server uses four schema files:

- ExternalSchema.ldf, which is used for interoperability with Microsoft Exchange Server
- ServerSchema.ldf, which is the primary Lync Server 2013 schema file
- BackCompatSchema.ldf, which is used for interoperability with any components from prior releases
- VersionSchema.ldf, which is used for version information of the prepared schema

All .ldf files are installed during schema preparation, regardless of whether you are migrating from a previous release or performing a clean installation. These schema files are installed in the sequence shown in the preceding list and are located in the \Support \schema folder on the installation media.

The Lync Server schema extensions are replicated across all domains, which impacts network traffic. Run schema preparation at a time when network usage is low.

Note:

If you need to add support for Microsoft® Office Communicator Mobile 2007 R2 for Java and Microsoft® Office Communicator Mobile for Nokia 1.0 mobile clients to your Lync Server 2013 deployment, you need to prepare the Active Directory schema for Microsoft Office Communications Server 2007 R2 during installation of Lync Server 2013. For the necessary software and documentation, see http://go.microsoft.com/fwlink/p/?linkId=207172.

ADSI Edit

Active Directory Service Interfaces Editor (ADSI Edit) is an AD DS administration tool that you can use to verify schema preparation and replication.

ADSI Edit is installed by default when you install the AD DS role to make a server a domain controller. For Windows Server 2008 and Windows Server 2008 R2, ADSI Edit (adsiedit.msc) is included with the Remote Server Administration Tools (RSAT). You can also install RSAT on domain member servers or stand-alone servers. The RSAT package is copied to these servers by default when you install Windows, but it is not installed by default. You install individual tools by using Server Manager. ADSI Edit is included under **Role Administration Tools**, **Active Directory Domain Services Tools**, **Active Directory Domain Controller Tools**.

For Windows Server 2003, ADSI Edit is included with the Support Tools. The Support Tools are available from the Windows Server 2003 CD in the \SUPPORT\TOOLS folder, or you can download them from "Windows Server 2003 Service Pack 2 32-bit Support Tools" at http://go.microsoft.com/fwlink/p/?linkId=125770. Instructions for installing the Support Tools from the product CD are available from "Install Windows Support Tools" at http://go.microsoft.com/fwlink/p/?linkId=125771. Adsiedit.dll is automatically registered when you install the support tools. If, however, you copied the files to your computer, you must run the **regsvr32** command to register the adsiedit.dll file before you can run the tool.

In This Section

- Running Schema Preparation

- Verifying Schema Replication

See Also

Other Resources

Preparing the Forest
Preparing Domains

Running Schema Preparation

See Also

Preparing Active Directory Domain Services for Lync Server 2013 > Preparing Active Directory Domain Services > Preparing the Active Directory Schema >

Topic Last Modified: *2012-10-29*

You can use Setup or Lync Server Management Shell cmdlets to prepare the Active Directory schema. The cmdlet that extends the Active Directory schema is **Install-CsAdServerSchema**.

Note:
The schema preparation cmdlet (**Install-CsAdServerSchema**) must access the schema master, which requires that the remote registry service is running and that the remote registry key is enabled. If the remote registry service cannot be enabled on the schema master, you can run the cmdlet locally on the schema master. For details about registry remote access, see Microsoft Knowledge Base article 314837, "How to Manage Remote Access to the Registry," at http://go.microsoft.com/fwlink/p/?linkId=125769.

After you complete schema preparation, manually verify that the schema partition has been replicated before proceeding to forest preparation. For details, see Verifying Schema Replication.

To use Setup to prepare the schema of the current forest

1. Log on to a server in your forest as a member of the Schema Admins group and with administrator rights on the schema master.
2. From the Lync Server 2013 installation folder or media, run Setup.exe to start the Deployment Wizard.
3. If you are prompted to install the Microsoft Visual C++ Redistributable, click **Yes**.
4. The Lync Server 2013 Setup dialog box prompts you for a location to install the Lync Server files. Choose the default location or **Browse** to a location of your choice, and then click **Install**.
5. On the License Agreement page, check **I accept the terms in the license agreement**, and then click **OK**.
6. The installer installs the Lync Server Core Components.
7. When the Deployment Wizard is ready, click **Prepare Active Directory**, and then wait for the deployment state to be determined.
8. At **Step 1: Prepare Schema**, click **Run**.
9. On the **Prepare Schema** page, click **Next**.
10. On the **Executing Commands** page, look for **Task status: Completed**, and then click **View Log**.
11. Under the **Action** column, expand **Schema Prep**, look for the **<Success>** Execution Result at the end of each task to verify that schema preparation completed successfully, close the log, and then click **Finish**.
12. Wait for Active Directory replication to complete or force replication.
13. Manually verify that the schema changes replicated to all other domain controllers. For details, see Verifying Schema Replication.

To use cmdlets to prepare the schema of the current forest

1. Log on to a computer in the forest as a member of the Schema Admins group and with administrator rights on the schema master.
2. Install Lync Server Core components as follows:
   2.a. From the Lync Server 2013 installation folder or media, run Setup.exe to start the Lync Server Deployment Wizard.
   2.b. If you are prompted to install the Microsoft Visual C++ Redistributable, click **Yes**.
   2.c. The Lync Server 2013 Setup dialog box prompts you for a location to install the Lync Server files. Choose the default location or **Browse** to a location of your choice, and then click **Install**.
   2.d. On the License Agreement page, check **I accept the terms in the license agreement**, and then click **OK**. The installer installs the Lync Server 2013 Core Components.
3. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
4. Run:

   ```
   Install-CsAdServerSchema [-Ldf <directory where the .ldf file is locat
   ```

   If you do not specify the Ldf parameter, the default value is the Lync Server 2013 installation path that is read from the registry.
   For example:

   ```
   Install-CsAdServerSchema -Ldf "C:\Program Files\Microsoft Lync Server
   ```

5. Use the following cmdlet to verify that schema preparation ran to completion.

   ```
   Get-CsAdServerSchema
   ```

   This cmdlet returns a value of **SCHEMA_VERSION_STATE_CURRENT** if schema preparation was successful.
6. Wait for Active Directory replication to complete or force replication.
7. Manually verify that the schema changes replicated to all other domain controllers. For details, see Verifying Schema Replication.

Tasks

Verifying Schema Replication

Concepts

Preparing the Active Directory Schema

Verifying Schema Replication

See Also

Preparing Active Directory Domain Services for Lync Server 2013 > Preparing Active Directory Domain Services > Preparing the Active Directory Schema >

Topic Last Modified: *2012-10-29*

Before you run forest preparation, manually verify that the schema partition has been replicated.

⊟To manually verify schema replication

1. Log on to a domain controller as a member of the Enterprise Admins group.
2. Open ADSI Edit by clicking **Start**, clicking **Administrative Tools**, and then clicking **ADSI Edit**.

   Tip:
   Alternatively, you can run **adsiedit.msc** from the command line.

3. In the Microsoft Management Console (MMC) tree, if it is not already selected, click **ADSI Edit**.
4. On the **Action** menu, click **Connect to**.
5. In the **Connection Settings** dialog box under **Select a well known Naming**

Context, select **Schema**, and then click **OK**.

6. Under the schema container, search for CN=ms-RTC-SIP-SchemaVersion. If this object exists, and the value of the **rangeUpper** attribute is 1150 and the value of the **rangeLower** attribute is 3, then the schema was successfully updated and replicated. If this object does not exist or the values of the **rangeUpper** and **rangeLower** attributes are not as specified, then the schema was not modified or has not replicated.

Tasks

Running Schema Preparation

Concepts

Preparing the Active Directory Schema

Preparing the Forest

Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 > Preparing Active Directory Domain Services >

Topic Last Modified: *2013-02-21*

Forest preparation creates Active Directory global settings and objects and Active Directory universal groups for use by Lync Server 2013, and grants suitable access permissions on the Active Directory objects. For a description of the universal groups and the global settings and objects created by forest preparation, see Changes Made by Forest Preparation.

Forest preparation also creates objects that contain property sets and display specifiers that are used by Lync Server 2013, and stores them in the Configuration container.

◆**Important:**
Make sure that schema preparation changes have replicated to all domain controllers before performing the forest preparation procedure. If replication is not completed, an error occurs.

If you are performing a new Lync Server deployment, you must store global settings in the Configuration container. If you are upgrading from an earlier version and you still store global settings in the System container, you can continue to use the System container.

You must be a member of the Enterprise Admins or Domain Admins group for the forest root domain to perform this procedure.

- Running Forest Preparation
- Using Cmdlets to Reverse Forest Preparation

Running Forest Preparation

See Also

Preparing Active Directory Domain Services for Lync Server 2013 > Preparing Active Directory Domain Services > Preparing the Forest >

Topic Last Modified: *2012-10-29*

You can use Setup or Lync Server Management Shell cmdlets to prepare the forest. The cmdlet that prepares the forest is **Enable-CsAdForest**.

After you prepare the forest, you must verify that global settings have been replicated before running domain preparation.

⊟To use Setup to prepare the forest

1. Log on to a computer that is joined to a domain as a member of the Enterprise Admins group for the forest root domain.
2. From the Lync Server 2013 installation folder or media, run Setup.exe to start the Deployment Wizard.
3. Click **Prepare Active Directory**, and then wait for the deployment state to be determined.
4. At **Step 3: Prepare Current Forest**, click **Run**.
5. On the **Prepare Forest** page, click **Next**.

> **Note:**
> Forest Preparation allows you to choose where to place the Universal Groups for Lync Server 2013. Choose a location that is consistent with the requirements of your organization.

6. On the **Executing Commands** page, look for **Task status: Completed**, and then click **View Log**.
7. Under the **Action** column, expand **Forest Prep**, look for a **<Success>** Execution Result at the end of each task to verify that forest preparation completed successfully, close the log, and then click **Finish**.
8. Wait for Active Directory replication to complete, or force replication to all domain controllers listed in the **Active Directory Sites and Services** snap-in for the forest root domain controller, before running domain preparation. Force replication between the domain controllers in all Active Directory sites to cause replication within the sites to occur within minutes.

To use cmdlets to prepare the forest

1. Log on to a computer that is joined to a domain as a member of the Domain Admins group in the forest root domain.
2. Install Lync Server Core components as follows:
   2.a. From the Lync Server 2013 installation folder or media, run Setup.exe to start the Lync Server Deployment Wizard.
   2.b. If you are prompted to install the Microsoft Visual C++ Redistributable, click **Yes**.
   2.c. The Lync Server 2013 Setup dialog box prompts you for a location to install the Lync Server files. Choose the default location or **Browse** to a location of your choice, and then click **Install**.
   2.d. On the License Agreement page, check **I accept the terms in the license agreement**, and then click **OK**. The installer installs the Lync Server 2013 Core Components.
3. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
4. Run:

```
Enable-CsAdForest [-GroupDomain <FQDN of the domain in which to create
```

   For example:

```
Enable-CsAdForest -GroupDomain domain1.contoso.com
```

   If you do not specify the GroupDomain parameter, the default value is the local domain. If universal groups were created previously in a domain that is not the default domain, you must specify the GroupDomain parameter explicitly.
5. Wait for Active Directory replication to complete, or force replication to all domain controllers listed in the **Active Directory Sites and Services** snap-in for the forest root domain controller, before running domain preparation.
6. Verify that forest preparation was successful. Run:

```
Get-CsAdForest
```

   This cmdlet returns a value of **LC_FORESTSETTINGS_STATE_READY** if forest preparation was successful.

Tasks

Using Cmdlets to Reverse Forest Preparation

Other Resources

Preparing the Forest

Using Cmdlets to Reverse Forest Preparation

See Also

Preparing Active Directory Domain Services for Lync Server 2013 > Preparing Active Directory Domain Services > Preparing the Forest >

Topic Last Modified: *2012-10-29*

Use the **Disable-CsAdForest** cmdlet to reverse the forest preparation step.

Caution:

If you run the **Disable-CsAdForest** cmdlet in an environment where you also have a previous version of Lync Server deployed, the global settings for the previous version will also be deleted.

⊟To use cmdlets to reverse forest preparation

1. Log on to a computer that is joined to a domain as a member of the Domain Admins group in the forest root domain.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

```
Disable-CsAdForest [-Force] [-GroupDomain <FQDN of the domain in which
```

```
Disable-CsAdForest -Force -GroupDomain contoso.net
```

The Force parameter specifies whether to force running the task. If this parameter is not present, the command will not run if even one domain in the forest is still prepared for Lync Server 2013. If the Force parameter is specified, the action will continue regardless of the state of other domains in the forest.

If you do not specify the GroupDomain parameter, the default value is the local domain.

Tasks

Running Forest Preparation

Other Resources

Preparing the Forest

Preparing Domains

Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 > Preparing Active Directory Domain Services >

Topic Last Modified: *2012-10-29*

Domain preparation is the final step in preparing Active Directory Domain Services (AD DS) for Lync Server 2013. The domain preparation step adds the necessary access control entries (ACEs) to universal groups that grant permissions to host and manage users within the domain. Domain preparation creates ACEs on the domain root and three built-in containers: User, Computers, and Domain Controllers.

You can run domain preparation on any computer in the domain where you are deploying

Lync Server. You must prepare every domain that will host Lync Server or users.

If permissions inheritance is disabled or authenticated user permissions are disabled in your organization, you must perform additional steps during domain preparation. For details, see Preparing a Locked-Down Active Directory Domain Services.

If your organization uses organizational units (OU) instead of the three built-in containers (that is, Users, Computers, and Domain Controllers), you must grant read access to the OUs for the Authenticated Users group. Read access to the containers is required for domain preparation. If the Authenticated Users group does not have read access to the OU, run the **Grant-CsOuPermission** cmdlet as illustrated in the following code examples to grant read permissions for each OU.

```
Grant-CsOuPermission -ObjectType <User | Computer | InetOrgPerson | Contact | App
```

```
Grant-CsOuPermission -ObjectType "user","contact",inetOrgPerson" -OU "ou=Redmond,
```

For details about the **Grant-CsOuPermission** cmdlet, see the Lync Server Management Shell documentation.

Tip:

For details about the ACEs created on the domain root and in the Users, Computers, and Domain Controllers containers, see Changes Made by Domain Preparation.

- Running Domain Preparation
- Using Cmdlets to Reverse Domain Preparation

Running Domain Preparation

See Also

Preparing Active Directory Domain Services for Lync Server 2013 > Preparing Active Directory Domain Services > Preparing Domains >

Topic Last Modified: *2012-10-29*

You can use Setup or Lync Server Management Shell cmdlets to prepare domains. The cmdlet that prepares a domain is **Enable-CsAdDomain**.

Domain preparation is the final step in preparing Active Directory Domain Services (AD DS) for Lync Server 2013.

⊟To use Setup to prepare domains

1. Log on to any server in the domain as a member of the Domain Admins group.
2. From the Lync Server 2013 installation folder or media, run Setup.exe to start the Lync Server Deployment Wizard.
3. Click **Prepare Active Directory**, and then wait for the deployment state to be determined.
4. At **Step 5: Prepare Current Domain**, click **Run**.
5. On the **Prepare Domain** page, click **Next**.
6. On the **Executing Commands** page, look for **Task status: Completed**, and then click **View Log**.
7. Under the **Action** column, expand **Domain Prep**, look for a **<Success>** Execution Result at the end of each task to verify that domain preparation completed successfully, close the log, and then click **Finish**.
8. Wait for Active Directory replication to complete or force replication to all the domain controllers listed in the Active Directory Sites and Services snap-in for the forest root domain controller.

⊟To use cmdlets to prepare the domain

1. Log on to any server in the domain as a member of the Domain Admins group.
2. Install Lync Server Core components as follows:
   - 2.a. From the Lync Server 2013 installation folder or media, run Setup.exe to start the Lync Server Deployment Wizard.
   - 2.b. If you are prompted to install the Microsoft Visual C++ Redistributable, click **Yes**.
   - 2.c. The Lync Server 2013 Setup dialog box prompts you for a location to install the Lync Server files. Choose the default location or **Browse** to a location of your choice, and then click **Install**.
   - 2.d. On the License Agreement page, check **I accept the terms in the license agreement**, and then click **OK**. The installer installs the Lync Server 2013 Core Components.
3. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
4. Run:

```
Enable-CsAdDomain [-Domain <DomainFQDN>]
```

For example:

```
Enable-CsAdDomain -Domain domain1.contoso.net
```

If you do not specify the Domain parameter, the default is the local domain.

5. Verify that domain preparation was successful. Run:

```
Get-CsAdDomain [-Domain <Domain FQDN>] [-DomainController <Domain cont
```

For example:

```
Get-CsAdDomain -Domain domain1.contoso.net - GlobalSettingsDomainContr
```

Note:
The parameter GlobalSettingsDomainController allows you to indicate where global settings are stored. If your settings are stored in the System container (which is typical with upgrade deployments that have not had the global settings migrated to the Configuration container), you define a domain controller in the root of your Active Directory forest. If the global settings are in the Configuration container (which is typical with new deployments or upgrade deployments where the settings have been migrated to the Configuration container), you define any domain controller in the forest. If you do not specify this parameter, the cmdlet assumes that the settings are stored in the Configuration container and refers to any domain controller in AD DS.

If you do not specify the **Domain** parameter, the default is the local domain. This cmdlet returns a value of **LC_DOMAINSETTINGS_STATE_READY** if domain preparation was successful.

Tasks

Using Cmdlets to Reverse Domain Preparation

Other Resources

Preparing Domains

Using Cmdlets to Reverse Domain Preparation

See Also

Preparing Active Directory Domain Services for Lync Server 2013 > Preparing Active Directory Domain Services > Preparing Domains >

Topic Last Modified: *2012-10-29*

Use the **Disable-CsAdDomain** cmdlet to reverse the domain preparation step.

To use cmdlets to reverse domain preparation

1. Log on to any server in the domain as a member of the Domain Admins group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

   ```
   Disable-CsAdDomain [-Domain <Fqdn>] [-DomainController <Fqdn>] [-Force
   [-GlobalCatalog <Fqdn>] [-GlobalSettingsDomainController <Fqdn>]
   ```

   For example:

   ```
   Disable-CsAdDomain -Domain domain1.contoso.net -GlobalSettingsDomainCo
   ```

   If the Force parameter is present, domain preparation is rolled back, even if one or more Front End Servers or A/V Conferencing Servers in the domain are activated. If the Force parameter is not present, domain preparation rollback is terminated if any Front End Servers or A/V Conferencing Servers in the domain are activated.

   > **Note:**
   >
   > The parameter GlobalSettingsDomainController allows you to indicate where global settings are stored. If your settings are stored in the System container (which is typical with upgrade deployments that have not had the global setting migrated to the Configuration container), you define a domain controller in the root of your Active Directory forest. If the global settings are in the Configuration container (which is typical with new deployments or upgrade deployments where the settings have been migrated to the Configuration container), you define any domain controller in the forest. If you do not specify this parameter, the cmdlet assumes that the settings are stored in the Configuration container and refers to any domain controller in AD DS.

Tasks

Running Domain Preparation

Other Resources

Preparing Domains

1.4.1.3.3.4 Preparing a Locked-Dow n Active Directory Domain Services

Preparing a Locked-Down Active Directory Domain Services

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 >

Topic Last Modified: *2012-05-14*

Organizations often lock down Active Directory Domain Services (AD DS) to help mitigate security risks. However, a locked-down Active Directory environment can limit the permissions that Lync Server 2013 requires. Properly preparing a locked-down Active Directory environment for Lync Server 2013 involves some additional considerations and steps.

Two common ways in which permissions are limited in a locked-down Active Directory environment are as follows:

- Authenticated user access control entries (ACEs) are removed from containers.
- Permissions inheritance is disabled on containers of User, Contact, InetOrgPerson, or Computer objects.

In This Section

- Authenticated User Permissions Are Removed
- Permissions Inheritance Is Disabled on Computers, Users, or InetOrgPerson Containers

Authenticated User Permissions Are Removed

Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 > Preparing a Locked-Down Active Directory Domain Services >

Topic Last Modified: *2013-02-21*

In a locked-down Active Directory environment, authenticated user access control entries (ACEs) are removed from the default Active Directory containers, including the Users, Configuration or System, and organizational units (OUs) where User and Computer objects are stored. Removing authenticated user ACEs prevents read access to Active Directory information. However, removing the ACEs creates issues for Lync Server 2013 because it depends on read permissions to these containers to allow users to run domain preparation.

In this situation, membership in the Domain Admins group, which is required to run domain preparation, server activation, and pool creation, no longer grants read access to Active Directory information stored in the default containers. You must manually grant read-access permissions on various containers in the forest root domain to check that the prerequisite forest preparation procedure is complete.

To enable a user to run domain preparation, server activation, or pool creation on any non-forest root domain, you have the following options:

- Use an account that is a member of the Enterprise Admins group to run domain preparation.
- Use an account that is a member of the Domain Admins group and grant this account read-access permissions on each of the following containers in the forest root domain:
  - Domain
  - Configuration or System

If you do not want to use an account that is a member of the Enterprise Admins group to run domain preparation or other Setup tasks, explicitly grant the account you want to use read access on the relevant containers in the forest root.

⊟To give users read-access permissions on containers in the forest root domain

1. Log on to the computer joined to the forest root domain with an account that is a member of the Domain Admins group for the forest root domain.
2. Run adsiedit.msc for the forest root domain.

   If authenticated user ACEs were removed from the Domain, Configuration, or System container, you must grant read-only permissions to the container, as described in the following steps.
3. Right-click the container, and then click **Properties**.
4. Click the **Security** tab.

5. Click **Advanced**.
6. On the **Permissions** tab, click **Add**.
7. Type the name of the user or group receiving permissions by using the following format: `domain\account name`, and then click **OK**.
8. On the **Objects** tab, in **Applies To**, click **This Object Only**.
9. In **Permissions**, select the following Allow ACEs by clicking the **Allow** column: **List Content**, **Read All Properties**, and **Read Permissions**.
10. Click **OK** twice.
11. Repeat these steps for any of the relevant containers listed in Step 2.

Permissions Inheritance Is Disabled on Computers, Users, or InetOrgPerson Containers

Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 > Preparing a Locked-Down Active Directory Domain Services >

Topic Last Modified: *2012-06-19*

In a locked-down Active Directory Domain Services (AD DS), Users and Computer objects are often placed in specific organizational units (OUs) with permissions inheritance disabled to help secure administrative delegation and to enable use of Group Policy objects (GPOs) to enforce security policies.

Domain preparation and server activation set the access control entries (ACEs) required by Lync Server 2013. When permissions inheritance is disabled, the Lync Server security groups cannot inherit these ACEs. When these permissions are not inherited, Lync Server security groups cannot access settings, and the following two issues arise:

- To administer Users, InetOrgPersons, and Contacts, and to operate servers, the Lync Server security groups require ACEs set by the domain preparation procedure on each user's property sets, real-time communications (RTC), RTC User Search, and Public Information. When permissions inheritance is disabled, security groups do not inherit these ACEs and cannot manage servers or users.
- To discover servers and pools, servers running Lync Server rely on ACEs set by activation on computer-related objects, including the Microsoft Container and Server object. When permissions inheritance is disabled, security groups, servers, and pools do not inherit these ACEs and cannot take advantage of these ACEs.

To address these issues, Lync Server provides the **Grant-CsOuPermission** cmdlet. This cmdlet sets required Lync Server ACEs directly on a specified container and organizational units and the objects within the container or organizational unit.

Set Permissions for User, InetOrgPerson, and Contact Objects after Running Domain Preparation

In a locked-down Active Directory environment where permissions inheritance is disabled, domain preparation does not set the necessary ACEs on the containers or organizational units holding Users or InetOrgPerson objects within the domain. In this situation, you must run the **Grant-CsOuPermission** cmdlet on each container or OU that has User or InetOrgPerson objects for which permissions inheritance is disabled. If you have a central forest topology, you must also perform this procedure on the containers or OUs that hold contact objects. For details about central forest topologies, see Supported Active Directory Topologies in the Supportability documentation. The ObjectType parameter specifies the object type. The OU parameter specifies the organizational unit.

This cmdlet adds the required ACEs directly on the specified containers or OUs and the User or InetOrgPerson objects within the container.

You need user rights equivalent to Domain Admins group membership to run this cmdlet. If the authenticated user ACEs have also been removed in the locked-down environment, you must grant this account read-access ACEs on the relevant containers or OUs in the forest root domain as described in Authenticated User Permissions Are Removed or use an account that is a member of the Enterprise Admins group.

To set required ACEs for User, InetOrgPerson, and Contact objects

1. Log on to a computer joined to the domain with an account that is a member of the Domain Admins group or that has equivalent user rights.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

   ```
   Grant-CsOuPermission -ObjectType <User | Computer | InetOrgPerson | Co
   -OU <DN name for the OU container relative to the domain root containe
   ```

   If you do not specify the Domain parameter, the default value is the local domain.

   For example:

   ```
   Grant-CsOuPermission -ObjectType "User" -OU "cn=Redmond,dc=contoso,dc=
   ```

4. In the log file, look for **<Success>** Execution Result at the end of each task to verify that the permissions were set, and then close the log window. Or, you can run the following command to determine whether the permissions were set:

   ```
   Test-CsOuPermission -ObjectType <type of object>
   -OU <DN name for the OU container relative to the domain root containe
   [-Domain <Domain FQDN>] [-Report <fully qualified path and name of fil
   ```

   For example:

   ```
   Test-CsOuPermission -ObjectType "User" -OU "cn=Redmond,dc=contoso,dc=n
   ```

Set Permissions for Computer Objects after Running Domain Preparation

In a locked-down Active Directory environment where permissions inheritance is disabled, domain preparation does not set the necessary ACEs on the containers or OUs that hold Computer objects within the domain. In this situation, you must run the **Grant-CsOuPermission** cmdlet on each container or OU that has computers running Lync Server where permissions inheritance is disabled. The ObjectType parameter specifies the object type.

This procedure adds the required ACEs directly on the specified containers.

You need user rights equivalent to Domain Admins group membership to run this cmdlet. If the authenticated user ACEs have also been removed, you must grant this account read-access ACEs on the relevant containers in the forest root domain as described in Authenticated User Permissions Are Removed or use an account that is a member of the Enterprise Admins group.

To set required ACEs for computer objects

1. Log on to the domain computer with an account that is a member of the Domain Admins group or that has equivalent user rights.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

3. Run:

```
Grant-CsOuPermission -ObjectType <Computer>
-OU <DN name for the computer OU container relative to the domain root
[-Domain <Domain FQDN>][-Report <fully qualified path and name of outp
```

   If you do not specify the Domain parameter, the default value is the local domain.
   For example:

```
Grant-CsOuPermission -ObjectType "Computer" -OU "ou=Lync Servers,dc=li
```

4. In the example log file C:\Logs\OUPermissions.xml, you would look for **<Success>** Execution Result at the end of each task and verify that there are no errors, and then close the log. You can run the following cmdlet to test permissions:

```
Test-CsOuPermission -ObjectType <type of object>
-OU <DN name for the OU container relative to the domain root containe
```

   For example:

```
Test-CsOuPermission -ObjectType "user","contact" -OU "cn=Bellevue,dc=c
```

> **Note:**
> If you run domain preparation on the forest root domain in a locked-down Active Directory environment, be aware that Lync Server requires access to the Active Directory Schema and Configuration containers.
> If the default authenticated user permission is removed from the Schema or the Configuration containers in AD DS, only members of the Schema Admins group (for Schema container) or Enterprise Admins group (for Configuration container) are permitted to access the given container. Because Setup.exe, Lync Server Management Shell cmdlets, and Lync Server Control Panel require access to these containers, Setup and installation of the administrative tools will fail unless the user running the installation has user rights equivalent to Schema Admins and Enterprise Admins group membership.
> To remedy this situation, you must grant RTCUniversalGlobalWriteGroup group Read, Write access to the Schema and Configuration containers.

1.4.1.3.3.5 Granting Permissions

Granting Permissions

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 >

Topic Last Modified: *2012-10-15*

For setup, you can grant permissions to the RTCUniversalServerAdmins universal group for a specific Active Directory organizational unit (OU), enabling members of the RTCUniversalServerAdmins group in that OU to install Lync Server 2013 in the specified domain. When you grant permissions for an OU, the following permissions are granted:

- Read
- Write
- ReadSPN
- WriteSPN

For administration, you can add permissions to specified OUs so that members of the RTC universal groups created by forest preparation can access the OUs without needing to be members of the Domain Admins group. The permissions added to the specified OU are the same permissions that the **Enable-CsAdDomain** cmdlet adds to the computers and users OU containers.

In This Section

- Granting Setup Permissions
- Granting Organizational Unit Permissions

Granting Setup Permissions

Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 > Granting Permissions >

Topic Last Modified: *2012-08-27*

You can use the **Grant-CsSetupPermission** cmdlet to add Read, Write, ReadSPN, and WriteSPN permissions to the RTCUniversalServerAdmins group for a specified Active Directory organizational unit (OU). Then members of the RTCUniversalServerAdmins group in that OU can install servers running Lync Server 2013 in the specified domain without being members of the Domain Admins group.

Use the **Test-CsSetupPermission** cmdlet to verify the permissions you set up by using the **Grant-CsSetupPermission** cmdlet.

You can use the **Revoke-CsSetupPermission** cmdlet to remove permissions that you granted by using the **Grant-CsSetupPermission** cmdlet.

To grant setup permissions

1. Log on to a computer running Lync Server 2013 in the domain where you want to grant setup permissions. Use an account that is a member of the Domain Admins group or the Enterprise Admins group if the OU is in a different child domain.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

```
Grant-CsSetupPermission -ComputerOu <DN of the OU or container where t
```

You can specify the ComputerOu parameter as relative to the default naming context of the specified domain (for example, CN=computers). Alternatively, you can specify this parameter as the full OU distinguished name (DN) (for example, "CN=computers,DC=Contoso,DC=com"). In the latter case, you must specify an OU DN that is consistent with the domain you specify.

If you do not specify the Domain parameter, the default value is the local domain.

To verify setup permissions

1. Log on to a computer running Lync Server 2013 in the domain where you want to verify setup permissions that you granted by using the **Grant-CsSetupPermission** cmdlet. Use an account that is a member of the Domain Admins group or the Enterprise Admins group if the OU is in a different child domain.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

```
Test-CsSetupPermission -ComputerOu <DN of the OU or container where th
```

You can specify the ComputerOu parameter as relative to the default naming context of the specified domain (for example, CN=computers). Alternatively, you can specify this parameter as the full OU distinguished name (DN) (for example, "CN=computers,DC=Contoso,DC=com"). In the latter case, you must specify an OU DN that is consistent with the domain you specify.

If you do not specify the Domain parameter, the default value is the local domain.

⊟To revoke setup permissions

1. Log on to a computer running Lync Server 2013 in the domain where you want to revoke setup permissions that were granted by the **Grant-CsSetupPermission** cmdlet. Use an account that is a member of the Domain Admins group or the Enterprise Admins group if the OU is in a different child domain.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

   ```
   Revoke-CsSetupPermission -ComputerOu <DN of the OU or container where
   ```

   You can specify the ComputerOu parameter as relative to the default naming context of the specified domain (for example, CN=computers). Alternatively, you can specify this parameter as the full OU distinguished name (DN) (for example, "CN=computers,DC=Contoso,DC=com"). In the latter case, you must specify an OU DN that is consistent with the domain you specify.

   If you do not specify the Domain parameter, the default value is the local domain.

Granting Organizational Unit Permissions

Preparing the Infrastructure and Systems > Preparing Active Directory Domain Services for Lync Server 2013 > Granting Permissions >

Topic Last Modified: *2012-05-14*

You can use the **Grant-CsOuPermission** cmdlet to grant permissions to objects in specified organizational units (OUs) so that members of the RTC universal groups created by forest preparation can access them without being members of the Domain Admins group. The permissions added to the specified OU are the same permissions that the **Enable-CsAdDomain** cmdlet adds to the computers and users containers during domain preparation.

Use the **Test-CsOuPermission** cmdlet to verify the permissions you set up by using the **Grant-CsOuPermission** cmdlet.

You can use the **Revoke-CsOuPermission** cmdlet to remove permissions that you granted by using the **Grant-CsOuPermission** cmdlet.

⊟To grant OU permissions

1. Log on to a computer running Lync Server 2013 in the domain where you want to grant OU permissions. Use an account that is a member of the Domain Admins group or the Enterprise Admins group if the OU is in a different child domain.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

   ```
   Grant-CsOuPermission -ObjectType <User | Computer | InetOrgPerson | Co
   ```

If you do not specify the Domain parameter, the default value is the local domain.

To verify OU permissions

1. Log on to a computer running Lync Server 2013 in the domain where you want to verify OU permissions that you granted by using the **Grant-CsOuPermission** cmdlet. Use an account that is a member of the Domain Admins group or the Enterprise Admins group if the OU is in a different child domain.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

```
Test-CsOuPermission -ObjectType <User | Computer | InetOrgPerson | Con
```

If you do not specify the Domain parameter, the default value is the local domain.

To revoke OU permissions

1. Log on to a computer running Lync Server 2013 in the domain where you want to revoke OU permissions that were granted by the **Grant-CsOuPermission** cmdlet. Use an account that is a member of the Domain Admins group or the Enterprise Admins group if the OU is in a different child domain.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

```
Revoke-CsOuPermission -ObjectType <User | Computer | InetOrgPerson | C
```

If you do not specify the Domain parameter, the default value is the local domain.

1.4.1.3.4 Configure SQL Server for Lync Server 2013

Configure SQL Server for Lync Server 2013

Deployment > Deploying Lync Server 2013 > Preparing the Infrastructure and Systems >

Topic Last Modified: *2012-10-01*

The topics in this section discuss how to deploy and configure SQL Server to use in an Enterprise deployment of Lync Server. Standard Edition servers use a collocated SQL Server Express version of SQL Server that is right sized for the workloads of a Standard Edition server.

The Lync Server 2013 Central Management store holds user data for all Enterprise Edition servers within a pool, and is designed to be located on a SQL Server -based Back End Server. As a centralized repository, the Central Management store cannot be installed on the same computer as any other Lync Server 2013 role. The Central Management store cannot reside on an Enterprise Edition server in the pool. The Central Management store is created automatically when you publish the topology for the first time and select to create the databases. The computer that you designate as the Back End Server must already be running SQL Server database software in order for the installation to succeed.

- SQL Server Data and Log File Placement
- Configure SQL Server
- Deployment Permissions for SQL Server

- Database Installation Using Lync Server Management Shell
- Understanding Firewall Requirements for SQL Server

1.4.1.3.4.1 SQL Server Data and Log File Placement

SQL Server Data and Log File Placement

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Configure SQL Server for Lync Server 2013 >

Topic Last Modified: *2013-02-21*

During the planning and deployment of Microsoft SQL Server 2012 or Microsoft SQL Server 2008 R2 SP1 for your Lync Server 2013 Front End pool, an important consideration is the placement of data and log files onto physical hard disks for performance. The recommended disk configuration is to implement a 1+0 RAID set using 6 spindles. Placing all database and log files that are used by the Front End pool and associated server roles and services (that is, Archiving and Monitoring Server, Lync Server Response Group service, Lync Server Call Park service) onto the RAID drive set using the Lync Server Deployment Wizard will result in a configuration that has been tested for good performance. The database files and what they are responsible for is detailed in the following table.

Note:

If your policies and SQL Server configurations require a more specialized installation, the database and log files can be installed to any pre-defined location using the Lync Server Management Shell. See Database Installation Using Lync Server Management Shell for more details.

Data and Log Files for Central Management Store

Central Management store database files	Data file or log purpose
Xds.ldf	Transaction log file for the Central Management store
Xds.mdf	Maintains the configuration of the current Lync Server 2013 topology, as defined and published by Topology Builder
Lis.mdf	Location Information service data file
Lis.ldf	Transaction log for the Location Information service data file

Data and Log files for User, Conferencing, and Address Book

Core Lync Server 2013 database files	Data file or log purpose
Rtc.mdf	Persistent user data (for example, access control lists (ACLs), contacts, scheduled conferences)
Rtc.ldf	Transaction log for Rtc data
Rtcdyn.mdf	Maintains transient user data (presence runtime data)
Rtcdyn.ldf	Transaction log for Rtcdyn data
Rtcab.mdf	Real-time communications (RTC) address book database is the SQL Server repository

	where Address Book service information is stored
Rtcab.ldf	Transaction log for Address Book Service
Rtclocal.mdb	Hosts the conference directory
Rtcxds.mdf	Maintains the backup for user data
Rtcxds.ldf	Transaction log for Rtcxds data

Data and Log Files for Call Park and Response Group

Application database	**Data file or log purpose**
Cpsdyn.mdf	Dynamic information database for the Call Park application
Cpsdyn.ldf	Transaction log for Call Park application data file
Rgsconfig.mdf	Lync Server Response Group service data file for the configuration of the services
Rgsconfig.ldf	Transaction log file for the Response Group application configuration
Rgsdyn.mdf	Response Group service data file for runtime operations
Rgsdyn.ldf	Transaction log for the Response Group service runtime data file

Data and Log Files for Archiving and Monitoring Server

Archiving and Monitoring database files	**Data file or log purpose**
LcsCdr.mdf	Data store for the call detail recording (CDR) process of the Monitoring Server
LcsCdr.ldf	Transaction log for call detail recording (CDR) data
QoEMetrics.mdf	Quality of Experience data file stored from the Monitoring Server
QoEMetrics.ldf	Transaction log for Monitoring data
Lcslog.mdf	Data file for the retention of instant messaging and conferencing data on an Archiving Server
Lcslog.ldf	Transaction log for Archiving data

In this topic, references are made to disk and to RAID set. Note that in the configuration of SQL Server resources, referring to a disk means a single hardware device. A hard disk drive with two partitions, one holding log files and the other partition holding data files, is not the same as two disks, each dedicated to either log or data files.

In reference to RAID sets, there are a number of different RAID technologies from various vendors. And, with the proliferation of storage area networks (SAN), RAID sets dedicated to a single system are rarer. You should consult with your RAID or SAN vendor to determine what the best configuration is for your disk layout when configuring for SQL

Server performance with Lync Server 2013.

Note also that not all disk drives are created equally; some perform better than others. Even drives from the same manufacturer can vary in performance because of rotational speed, hardware cache size, and other factors.

1.4.1.3.4.2 Configure SQL Server

Configure SQL Server

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Configure SQL Server for Lync Server 2013 >

Topic Last Modified: *2012-10-01*

For each database that you deploy, you can use a single SQL Server instance for all databases for your Lync Server 2013 deployment that can be collocated on a database server. For details about database collocation, see Supported Server Collocation in the Supportability documentation.

Additionally, each SQL Server instance must be installed and available prior to completing the steps in Topology Builder that set up the databases, or manually creating the databases with Windows PowerShell cmdlets. For details about SQL Server supportability, see Hardware Setup.

⊟To install Microsoft SQL Server 2012

- See the Microsoft SQL Server 2012 documentation at: http://go.microsoft.com/fwlink/p/?linkId=218015.

1.4.1.3.4.3 Deployment Permissions for SQL Server

Deployment Permissions for SQL Server

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Configure SQL Server for Lync Server 2013 >

Topic Last Modified: *2012-10-01*

Microsoft SQL Server 2012 has specific requirements when installing and deploying Lync Server 2013. Because Windows and SQL Server define their security differently, logging in as an administrator in the Active Directory domain does not implicitly grant permissions for SQL Server. You must also be a member of the sysadmin entity on the SQL Server-based server you are configuring.

Permissions Required for Database and Lync Server Installation

The following options detail three permissions and group membership associations for installation of Lync Server 2013 files and SQL Server databases. Choose the scenario that best meets the requirements of your organization.

Permissions and Group Membership Associations

SQL Server or Lync Server 2013 role	Role-Typical SQL Server permissions	Role-typical Lync Server 2013	Permissions outcome

	and group membership	**permissions and group membership**	
Lync Server 2013 administrator	Must be granted membership of sysadmins SQL Server security group and member of the SQL Server local Administrators group	Must be a member of the RTCUniversalServerAdmins group	Lync Server 2013 administrator has the proper permissions to install both Lync Server 2013 and SQL Server databases.
SQL Server administrator	SQL Server sysadmin group member (or equivalent) and member of the SQL Server local Administrators group	Must be a member of the RTCUniversalServerReadOnly group	SQL Server administrator has the proper permissions to install both Lync Server 2013 and SQL Server databases.
Both administrators sharing installation duties	SQL Server administrator is member of sysadmins group (or equivalent) and member of the SQL Server local Administrators group	Lync Server 2013 administrator is member of RTCUniversalServerAdmins	The Lync Server 2013 administrator can install Lync Server 2013, but cannot install the databases. The SQL Server administrator uses the Lync Server Management Shell and Windows PowerShell cmdlets provided by the Lync Server 2013 administrator to install the databases. The Lync Server 2013 Management Shell used by the SQL Server administrator is installed on the Front End Server. This eliminates the need to install the Lync Server 2013 administrative tools on the SQL Server-based server.

1.4.1.3.4.4 Database Installation Using Lync Server Management Shell

Database Installation Using Lync Server Management Shell

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Configure SQL Server for Lync Server 2013 >

Topic Last Modified: *2013-02-06*

Separation of roles and responsibilities between server administrators and SQL Server administrators can result in delays in implementation. Lync Server 2013 uses role-based access control (RBAC) to mitigate these difficulties. In some instances, the SQL Server administrator must manage the installation of databases on the SQL Server-based server outside RBAC. The Lync Server 2013 Management Shell provides a way for the SQL Server administrator to run Windows PowerShell cmdlets designed to configure the databases with the correct data and log files. For details, see Deployment Permissions for SQL Server.

Important:

The following procedure assumes that at a minimum the Lync Server 2013 OCSCore.msi, SQL Server Native Client (sqlncli.msi) Microsoft SQL Server 2012 Management Objects, CLR Types for Microsoft SQL Server 2012 and Microsoft SQL Server 2012 ADOMD.NET are installed. The OCSCore.msi is located on the installation media in the \Setup\AMD64 \Setup directory. The remaining components are located in \Setup\amd64. Additionally, Active Directory preparation for Lync Server 2013 has been successfully completed.

Install-CsDatabase is the Windows PowerShell cmdlet you use to install the databases. The **Install-CsDatabase** cmdlet has a large number of parameters, only a few of which are discussed here. For details about the possible parameters, see the Lync Server 2013 Management Shell documentation.

Warning:

To avoid performance and possible time-out issues, always use fully qualified domain names (FQDNs) when referring to SQL Server-based servers. Avoid using host name-only references. For example, use sqlbe01.contoso.net, but avoid using SQLBE01.

For installing databases, **Install-CsDatabase** uses three primary methods for placing the databases onto the prepared SQL Server-based server:

- Run **Install-CsDatabase** without DatabasePaths or UseDefaultSqlPath. The cmdlet uses a built in algorithm to determine the best placement for the log and data files. The algorithm only works for stand-alone SQL Server implementations.
- Run **Install-CsDatabase** with the DatabasePaths parameter. The built-in algorithm to optimize log and data file locations is not used if the DatabasePaths parameter is defined. Using this parameter allows you to define the locations where log and data files will be deployed.
- Run **Install-CsDatabase** with UseDefaultSqlPaths. This option does not use the built-in algorithm to optimize the log and data file locations. Log and data file are deployed according to the defaults set by the SQL Server administrator. These paths are typically set for the purpose of automatic administration of log and data files on the SQL Server in advance, and are not associated with the setup of Lync Server 2013.
- The DatabasePathMap parameter can also be used to explicitly specify a location for each database and its respective log file.

To use Windows PowerShell cmdlets to configure the SQL Server Central Management store

1. On any computer, log on with administrative credentials for creating the databases on the SQL Server-based server. For details, see Deployment Permissions for SQL Server.
2. Open the Lync Server 2013 Management Shell. If you have not adjusted the execution policy for Windows PowerShell, you must adjust the policy to allow Windows PowerShell scripts to run. For details, see “Examining the Execution Policy” at http://go.microsoft.com/fwlink/p/?linkId=203093.
3. Use the **Install-CsDatabase** cmdlet to install the Central Management store.

```
Install-CsDatabase -CentralManagementDatabase -SqlServerFqdn <fully qu
-SqlInstanceName <named instance> -DatabasePaths <logfile path>,<datab
-Report <path to report file>
```

```
Install-CsDatabase -CentralManagementDatabase -SqlServerFqdn sqlbe.con
```

> **Tip:**
> The Report parameter is optional but is useful if you are documenting the installation process.

4. **Install-CsDatabase –DatabasePaths** can use up to six path parameters, each defining the paths for the drives as defined in SQL Server Data and Log File Placement. By the logical rules of the database configuration in Lync Server 2013, drives are parsed out into buckets of two, four, or six. Depending on your SQL Server configuration and the number of buckets, you will supply two paths, four paths, or six paths.

   If you have three drives, the log gets priority and the data files are distributed after. An example for a SQL Server-based server configured with six drives:

   ```
   Install-CsDatabase -ConfiguredDatases -SqlServerFqdn sqlbe.contoso.net
   ```

5. When the database installation completes, you can close Lync Server 2013 Management Shell or proceed to the installation of the Lync Server 2013 configured databases defined in Topology Builder.

To use Windows PowerShell cmdlets to configure the SQL Server topology configured databases

1. To install the Topology Builder configured databases for Lync Server 2013, the Lync Server 2013 administrator must publish the topology. For details, see Publish the Topology in the Deployment documentation.
2. On any computer, log on with administrative credentials for creating the databases on the SQL Server-based server. See the topic, Deployment Permissions for SQL Server.

   > **Important:**
   > To be able to configure the SQL Server-based databases, make sure the SQL Server administrator account used to run the steps described here is also a member of the sysadmins group (or equivalent) on the server running SQL Server and holding the Central Management Server role. This is especially important to check for any additional Lync Server 2013 pools which require SQL Server database installation or configuration. For example, if you are deploying a second pool (pool02) but the Central Management Server role is held by pool01. The SQL Server sysadmin group (or equivalent) must have permissions on both SQL Server-based databases.

3. Open Lync Server 2013 Management Shell, if it’s not already open.
4. Use the **Install-CsDatabase** cmdlet to install the Topology Builder configured databases.

   ```
   Install-CsDatabase -ConfiguredDatabases -SqlServerFqdn <fully qualifie
    -DatabasePaths <logfile path>,<database file path> -Report <path to r
   ```

   ```
   Install-CsDatabase -ConfiguredDatabases -SqlServerFqdn sqlbe.contoso.n
   -Report "C:\Logs\InstallDatabases.html"
   ```

   > **Tip:**
   > The Report parameter is optional but is useful if you are documenting the installation process.

5. When the database installation completes, close Lync Server 2013 Management Shell.

To use Windows PowerShell cmdlets to configure the SQL Server topology using the DatabasePathMap parameter

1. To install databases for Lync Server 2013, the Lync Server administrator must create the paths and deploy the databases files and log files according to a predefined set of rules.
2. On any computer, log on with administrative credentials for creating the

databases on the SQL Server-based server. See the topic, Deployment Permissions for SQL Server.

Important:
To be able to configure the SQL Server-based databases, make sure the SQL Server administrator account used to run the steps described here is also a member of the sysadmins group (or equivalent) on the server running SQL Server and holding the Central Management Server role. This is especially important to check for any additional Lync Server pools which require SQL Server database installation or configuration. For example, if you are deploying a second pool (pool02) but the Central Management Server role is held by pool01. The SQL Server sysadmin group (or equivalent) must have permissions on both SQL Server-based databases.

3. Open Lync Server Management Shell, if it's not already open.
4. Use the **Install-CsDatabase** cmdlet with the DatabasePathMap parameter and a PowerShell hash table to install the Topology Builder configured databases.
5. In the example code, the paths defined for the databases can be determined in a granular manner by using the –DatabasePathsMap parameter and a defined hash table as follows (the example uses "C:\CSData" for all database (.mdf) files, and "C:\CSLogFiles" for all log (.ldf) files. Folder will be created as needed by Install-CsDatabase):

```
$pathmap = @{
"BackendStore:BlobStore:DbPath"="C:\CsData";"BackendStore:BlobStore:Lo
"BackendStore:RtcSharedDatabase:DbPath"="C:\CsData";"BackendStore:RtcS
"ABSStore:AbsDatabase:DbPath"="C:\CsData";"ABSStore:AbsDatabase:LogPat
"ApplicationStore:RgsConfigDatabase:DbPath"="C:\CsData";"ApplicationSt
"ApplicationStore:RgsDynDatabase:DbPath"="C:\CsData";"ApplicationStore
"ApplicationStore:CpsDynDatabase:DbPath"="C:\CsData";"ApplicationStore
"ArchivingStore:ArchivingDatabase:DbPath"="C:\CsData";"ArchivingStore:
"MonitoringStore:MonitoringDatabase:DbPath"="C:\CsData";"MonitoringSto
"MonitoringStore:QoEMetricsDatabase:DbPath"="C:\CsData";"MonitoringSto
}
Install-CsDatabase -ConfigureDatabases -SqlServerFqdn sqlbe01.contoso.
```

6. Because the database and log files are explicitly named with their location on the destination database server, you can define specific locations for each service type's actual database and log location. The following example puts databases for each specific service type on separate disks, and associated log files on another. For example:
   - All RTC databases to "D:\RTCDatabase"
   - All RTC log files to "E:\RTCLogs"
   - All application store databases to "F:\CPSDatabases"
   - All application store logs to "G:\CPSLogs"
   - All response group store databases to "H:\RGSDatabases"
   - All response group store logs to "I:\RGSLogs"
   - All address book store databases to "J:\ABSDatabases"
   - All address book store log files to "K:\ABSLogs"
   - All archiving store databases to "L:\ArchivingDatabases"
   - All archiving store logs to "M:\ArchivingLogs"
   - All monitoring store databases to "N:\MonitoringDatabases"
   - All monitoring store log files to "O:\MonitoringLogfiles"

```
$pathmap = @{
"BackendStore:BlobStore:DbPath"="D:\RTCDatabase";"BackendStore:BlobSto
"BackendStore:RtcSharedDatabase:DbPath"="D:\RTCDatabase";"BackendStore
"ABSStore:AbsDatabase:DbPath"="J:\ABSDatabases";"ABSStore:AbsDatabase:
"ApplicationStore:RgsConfigDatabase:DbPath"="H:\RGSDatabases";"Applica
"ApplicationStore:RgsDynDatabase:DbPath"="H:\RGSDatabases";"Applicatio
"ApplicationStore:CpsDynDatabase:DbPath"="F:\CPSDatabases";"Applicatio
"ArchivingStore:ArchivingDatabase:DbPath"="M:\ArchivingLogs";"Archivin
"MonitoringStore:MonitoringDatabase:DbPath"="N:\MonitoringDatabases";"
"MonitoringStore:QoEMetricsDatabase:DbPath"="N:\MonitoringDatabases";"
}
Install-CsDatabase -ConfigureDatabases -SqlServerFqdn sqlbe01.contoso.
```

Using the –DatabasePathMap parameter, you can define any logical drive letter mapping combination that provides the best solution for your SQL Server performance and placement requirements.

If you configure your database data files and log files by using the **DatabasePathMap** method, you will need to make a slight change to your normal process when using Topology Builder. Typically, you would define your topology choices, publish the topology, and choose to deploy the database selections.

If you have used **DatabasePathMap** you have already accomplished the third part of the Topology Builder process. In the case of having a completely configured database server in advance of running Topology Builder, you would still define all of your server roles and options, but deselect the option to create the databases.

1.4.1.3.4.5 Understanding Firewall Requirements for SQL Server

Understanding Firewall Requirements for SQL Server

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Configure SQL Server for Lync Server 2013 >

Topic Last Modified: *2013-02-21*

For a Standard Edition deployment, firewall exceptions are created automatically during Lync Server 2013 Setup. However, for Enterprise Edition deployments, you must configure the firewall exceptions manually on the SQL Server Back End Server. The TCP/IP protocol allows for a given port to be used once for a given IP address. This means that for the SQL Server-based server you can assign the default database instance the default TCP port 1433. For any other instances you will need to use the SQL Server Configuration Manager to assign unique and unused ports. This topic covers:

- Requirements for a firewall exception when using the default instance
- Requirements for a firewall exception for the SQL Server Browser service
- Requirements for static listening ports when using named instances

Requirements for a Firewall Exception When Using the Default Instance

If you are using the SQL Server default instance for any database when deploying Lync Server 2013, the following firewall rule requirements are used to help ensure communication from the Front End pool to the SQL Server default instance.

Protocol	Port	Direction
TCP	1433	Inbound to SQL Server

Requirements for a Firewall Exception for the SQL Server Browser Service

The SQL Server Browser service will locate database instances and communicate the port that the instance (named or default) is configured to use.

Protocol	Port	Direction

UDP	1434	Inbound

Requirements for Static Listening Ports When Using Named Instances

When using named instances in the SQL Server configuration for databases supporting Lync Server 2013, you configure static ports by using SQL Server Configuration Manager. After the static ports have been assigned to each named instance, you create exceptions for each static port in the firewall.

Protocol	Port	Direction
TCP	Statically defined	Inbound

SQL Server Documentation

Microsoft SQL Server 2012 documentation provides detailed guidance on how to configure firewall access for databases. For details about Microsoft SQL Server 2012, see “Configuring the Windows Firewall to Allow SQL Server Access” at http://go.microsoft.com/fwlink/p/?linkId=218031.

1.4.1.3.5 Configure DNS Records for a Front End Pool or Standard Edition Server

Configure DNS Records for a Front End Pool or Standard Edition Server

Deployment > Deploying Lync Server 2013 > Preparing the Infrastructure and Systems >

Topic Last Modified: *2012-10-01*

Lync Server 2013 uses the Domain Name System (DNS) to register and maintain records for proper domain name to IP address resolution. You need to configure required DNS records for your deployment prior to operating the Standard Edition server or Front End pool. The following links will provide guidance on what records need to be created to allow for the proper operation of Lync Server 2013.

- Configure DNS for Load Balancing
- Configure DNS Host Records
- Create and Verify DNS SRV Records

1.4.1.3.5.1 Configure DNS for Load Balancing

Configure DNS for Load Balancing

See Also

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Configure DNS Records for a Front End Pool or Standard Edition Server >

Topic Last Modified: *2012-10-01*

To successfully complete this procedure, you should be logged on to the server or domain minimally as a member of the Domain Admins group or a member of the DnsAdmins group.

Domain Name System (DNS) Load Balancing balances the network traffic that is unique to

Lync Server 2013, such as SIP traffic and media traffic. DNS load balancing is supported for Front End pools, Edge pools, Director pools, and stand-alone Mediation pools. A pool that is configured to use DNS load balancing must have two fully qualified domain names (FQDNs) defined: the regular pool FQDN that is used by DNS load balancing (for example, pool1.contoso.com) and that resolves to the physical IPs of the servers in the pool, and another FQDN for the pool's Web Services (for example, web1.contoso.net), which resolves to the virtual IP address of the pool. For details about DNS Load Balancing, see DNS Load Balancing in the Planning documentation.

Note:

Hardware load balancing is still required for client to server HTTPS traffic.

Before you can use DNS load balancing, you must do the following:

1. Override the internal Web Services pool FQDN.

   ⚠Warning:

   If decide to override the Internal web services with a self-defined FQDN, each FQDN must be unique from any other Front End pool, Director or a Director pool.

2. Create DNS A host records to resolve the pool FQDN to the IP addresses of all the servers in the pool.
3. Enable IP Address randomization or, for Windows Server DNS, enable round robin.

   Note:

   Round robin should be enabled by default.

⊟To override internal Web services FQDN

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. From the console tree, expand the Enterprise Edition Front End pools node.
3. Right-click the pool, click **Edit Properties**, and then click **Web Services**.
4. Below **Internal web services**, select the **Override FQDN** check box.
5. Type the pool FQDN that resolves to the physical IP addresses of the servers in the pool.
6. Below **External web services**, type the external pool FQDN that resolves to the virtual IP addresses of the pool, and then click **OK**.
7. From the console tree, click **Lync Server 2013**, and then in the **Actions** pane, click **Publish Topology**.

⊟To create DNS Host (A) Records for all internal pool servers

1. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **DNS**.
2. In **DNS Manager**, click the DNS Server that manages your records to expand it.
3. Click **Forward Lookup Zones** to expand it.
4. Right-click the DNS domain that you need to add records to, and then click **New Host (A or AAAA)**.
5. In the **Name** box, type the name of the host record (the domain name will be automatically appended).
6. In the IP Address box, type the IP address of the individual Front End Server and then select **Create associated pointer (PTR) record** or **Allow any authenticated user to update DNS records with the same owner name**, if applicable.
7. Continue creating records for all member Front End Servers that will participate in DNS Load Balancing.

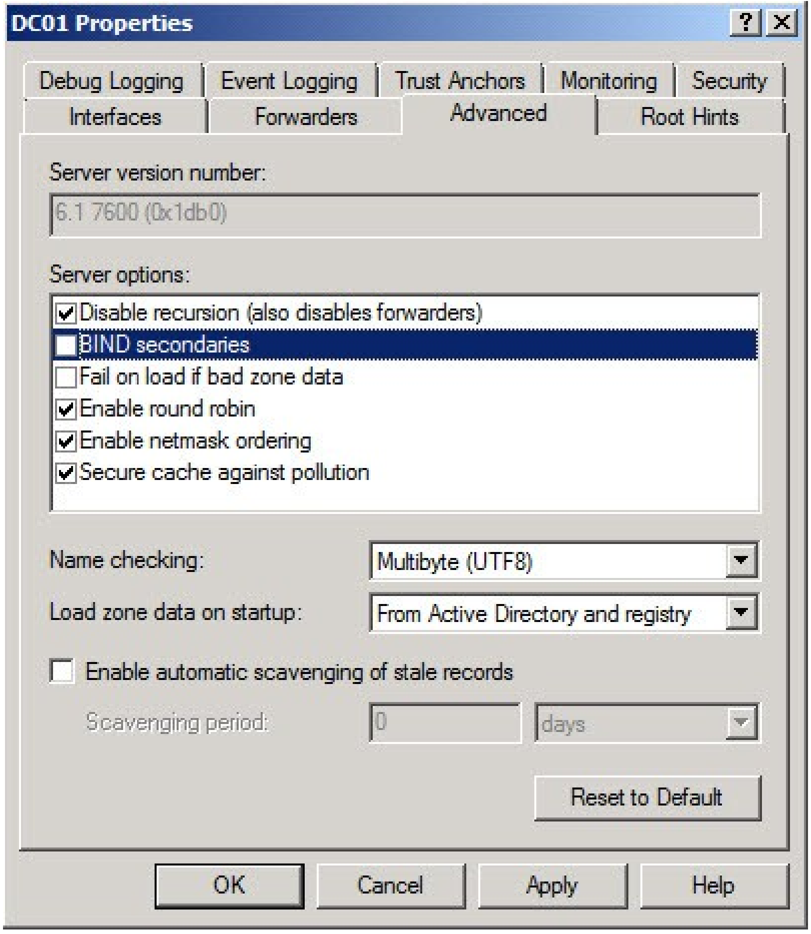
   For example, if you had a pool named pool1.contoso.com and three Front End Servers, you would create the following DNS entries:

FQDN	Type	Data
Pool1.contoso.com	Host (A)	192.168.1.1
Pool1.contoso.com	Host (A)	192.168.1.2
Pool1.contoso.com	Host (A)	192.168.1.3

For details about creating DNS Host (A) records, see Configure DNS Host Records.

⊟To enable round robin for Windows Server

1. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **DNS**.
2. Expand **DNS**, right-click the DNS server you want to configure, and then click **Properties**.
3. Click the **Advanced** tab, select **Enable round robin** and **Enable netmask ordering**, and then click **OK**.



DC01 Properties

Server version number: 6.1 7600 (0x1db0)

Server options:

☑ Disable recursion (also disables forwarders)
☐ BIND secondaries
☐ Fail on load if bad zone data
☑ Enable round robin
☑ Enable netmask ordering
☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

Note:
This feature should be enabled by default.

Concepts

DNS Load Balancing

1.4.1.3.5.2 Configure DNS Host Records

Configure DNS Host Records

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Configure DNS Records for a Front End Pool or Standard Edition Server >

Topic Last Modified: *2012-10-01*

To successfully complete this procedure, you should be logged on to the server or domain at minimum as a member of the Domain Admins group or a member of the DnsAdmins group.

⊟To configure DNS Host A records

1. On the Domain Name System (DNS) server, click **Start**, click **Administrative Tools**, and then click **DNS**.
2. In the console tree for your domain, expand **Forward Lookup Zones**, and then right-click the domain in which Lync Server 2013 will be installed.
3. Click **New Host (A or AAAA)**.
4. Click **Name**, type the host name for the pool (the domain name is assumed from the zone that the record is defined in and does not need to be entered as part of the A record).
5. Click **IP Address**, type the virtual IP (VIP) of the load balancer for the Front End pool.

   Important:
   In deployments that use a Director pool, the host (A) records for the simple URLs should point to the VIP of the Director load balancer.

   Note:
   If you deploy only one Enterprise Edition server or Director that is connected to the topology without a load balancer, or if you deploy a Standard Edition server, type the IP address of the Enterprise Edition server, Standard Edition server, or Director. A load balancer is required if you deploy more than one Enterprise Edition server or Director in a pool. Load balancers are not used with Standard Edition servers.
6. Click **Add Host**, and then click **OK**.
7. To create an additional A record, repeat steps 4 and 5.
8. When you are finished creating all the A records that you need, click **Done**.

1.4.1.3.5.3 Create and Verify DNS SRV Records

Create and Verify DNS SRV Records

Deploying Lync Server 2013 > Preparing the Infrastructure and Systems > Configure DNS Records for a Front End Pool or Standard Edition Server >

Topic Last Modified: *2013-02-21*

To successfully complete this procedure, you should be logged on to the server or domain minimally as a member of the Domain Admins group or a member of the DnsAdmins group.

This topic describes how to configure the Domain Name System (DNS) records that you are required to create in Lync Server 2013 deployments and those required for automatic client sign in. When you create a Front End pool, Setup creates Active Directory objects and settings for the pool, including the pool fully qualified domain name (FQDN). Similar objects and settings are created for a Standard Edition server. For clients to be able to connect to the pool or Standard Edition server, the FQDN of the pool or Standard Edition server must be registered in DNS. You must create DNS SRV records in your internal DNS for every SIP domain. This procedure assumes that your internal DNS has zones for your SIP user domains.

⊟To configure a DNS SRV record

1. On the DNS server, click **Start**, click **Administrative Tools**, and then click **DNS**.
2. In the console tree for your SIP domain, expand **Forward Lookup Zones**, and then right-click the SIP domain in which Lync Server 2013 will be installed.
3. Click **Other New Records**.
4. In **Select a resource record type**, click **Service Location (SRV)**, and then click **Create Record**.
5. Click **Service**, and then type **_sipinternaltls**.
6. Click **Protocol**, and then type **_tcp**.
7. Click **Port Number**, and then type **5061**.
8. Click **Host offering this service**, and then type the FQDN of the pool or Standard Edition server.
9. Click **OK**, and then click **Done**.

⊟To verify the creation of a DNS SRV record

1. Log on to a client computer in the domain with an account that is a member of the Authenticated Users group or has equivalent permissions.
2. Click **Start**, and then click **Run**.
3. In the **Open** box, type **cmd**, and then click **OK**.
4. At the command prompt, type **nslookup**, and then press ENTER.
5. Type **set type=srv**, and then press ENTER.
6. Type **_sipinternaltls._tcp.contoso.com**, and then press ENTER. The output displayed for the Transport Layer Security (TLS) record is as follows:

   Server: *<dns server>*.contoso.com

   Address: *<IP address of DNS server>*

   Non-authoritative answer:

   _sipinternaltls._tcp.contoso.com SRV service location:

   priority = 0

   weight = 0

   port = 5061

   svr hostname = poolname.contoso.com (or Standard Edition server A record)

   poolname.contoso.com internet address = *<virtual IP Address of the load balancer>* or *<IP address of a single Enterprise Edition server for pools with only one Enterprise Edition server>* or *<IP address of the Standard Edition server>*
7. When you are finished, at the command prompt, type **exit**, and then press ENTER.

⊟To verify that the FQDN of the Front End pool or Standard Edition server can be resolved

1. Log on to a client computer in the domain.
2. Click **Start**, and then click **Run**.
3. In the **Open** box, type **cmd**, and then click **OK**.
4. At the command prompt, type **nslookup** *<FQDN of the Front End pool>* or *<FQDN of the Standard Edition server>*, and then press ENTER.
5. Verify that you receive a reply that resolves to the appropriate IP address for the FQDN.

1.4.1.3.6 Install Lync Server Administrative Tools

Install Lync Server Administrative Tools

See Also

Topic Last Modified: *2013-02-21*

This topic describes how to install the administrative tools you need to use to deploy and manage Lync Server 2013. The administrative tools are installed by default on each server running Lync Server 2013. Additionally, you can install the administrative tools on other computers, such as dedicated administrative consoles. We strongly recommend that you install the administrative tools on a computer that is in the same domain or forest as the Lync Server 2013 deployment you are creating because by doing so you make sure that Active Directory Domain Services (AD DS) preparation steps are already complete, which enables you to use the administrative tools on that computer later to publish your topology.

Make sure that you review infrastructure, operating system, software, and administrator rights requirements before you install or use the Lync Server 2013 administrative tools. For details about infrastructure requirements, see Administrative Tools Infrastructure Requirements. For details about operating system and software requirements to install the Lync Server 2013 administrative tools, see Server and Tools Operating System Support, Additional Software Requirements, and Additional Server Support and Requirements. For details about the user rights and permissions required to install and use the tools, see Administrator Rights and Permissions Required for Setup and Administration.

Important:
If your organization requires that you locate Internet Information Services (IIS) and all Web Services on a drive other than the system drive, you can change the installation location path for the Lync Server files in the Setup dialog box. If you install the Setup files to this path, including OCSCore.msi, the rest of the Lync Server 2013 files will be deployed to this drive as well.

To install the Lync Server 2013 administrative tools

1. Log on as a local administrator (minimum requirement) to the computer where you want to install the administrative tools. If you are logged on as an a standard user on the Windows Vista or Windows 7 operating systems, and User Account Control (UAC) is enabled, you will be prompted for the local administrator or a domain equivalent user name and password.
2. Locate the installation media on your computer, and then double-click \Setup \amd64\Setup.exe.
3. If you are prompted to install the Microsoft Visual C++ 2008 distributable, click **Yes**.
4. On the **Microsoft Lync Server 2013 Installation Location** page, click **OK**. Change this path to another location or drive if you need to have the files installed to another location.

Important:
If your organization requires that you locate Internet Information Services (IIS) and all Web Services on a drive other than the system drive, you can change the installation location path for the Lync Server 2013 files in the Setup dialog box. If you install the Setup files to this path, including OCSCore.msi, the rest of the Lync Server 2013 files will be deployed to this drive too.

5. On the **End User License Agreement** page, review the license terms, click **I accept**, and then click **OK**. This step is required before you can continue.
6. On the **Microsoft Lync Server 2013 – Deployment Wizard** page, click **Install Administrator Tools**.
7. When the installation successfully completes, click **Exit**.

Tasks

Open Lync Server Administrative Tools

Concepts

Lync Server Administrative Tools

1.4.1.4 Designing the Topology by Using the Planning Tool

Designing the Topology by Using the Planning Tool

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2013-03-04*

The Microsoft Lync Server 2013, Planning Tool is a wizard driven, interview-like tool that asks questions about the Lync Server 2013 topology that you are designing. The Planning Tool uses the information supplied, coupled with preferred practices for topology design and capacity, to present a recommended topology based on the answers supplied. You can download the Planning Tool from the Microsoft Downloads Center (http://go.microsoft.com/fwlink/?LinkID=282725).

Ultimately, the goal of the Planning Tool is to ease the potential complexity of designing a complete Lync Server 2013 topology. The tool also provides contextual references to planning and deployment documentation inside the tool, provided that an Internet connection is available to connect to the Microsoft TechNet website.

After customizing the topology with the infrastructure’s TCP/IP addresses and fully qualified domain names (FQDNs), the Planning Tool makes available a series of reports that cover Domain Name System (DNS) naming, firewall rules, certificates, and more.

The Planning Tool also provides the ability to export information in two formats:

- Microsoft Excel
- Microsoft Visio

The following topics introduce and detail the Planning Tool.

- Installing the Planning Tool
- Installing Optional Software
- Navigating the Planning Tool
- Create the Initial Design
- Reviewing the Administrator Reports

⊟See Also

Other Resources

Deploying Lync Server 2013
Planning for Front End Servers, Instant Messaging, and Presence

1.4.1.4.1 Install the Planning Tool

Installing the Planning Tool

See Also

Deployment > Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool >

Topic Last Modified: *2013-02-21*

Before you begin designing and planning your Lync Server 2013 infrastructure by using the Microsoft Lync Server 2013, Planning Tool, you must first install the Planning Tool. The Planning Tool does not need to be deployed to a workstation or server that is part of the domain or infrastructure where you plan to install Lync Server 2013. The Readme file that accompanies the Planning Tool details important information about installing and using the tool. Some of the information in the Readme file is duplicated here for clarity.

◆**Important:**
The Planning Tool requires installation by a user with administrator rights and permissions on the computer on which the tool is to be installed.

The supported operating systems for installation and operation of the Planning Tool are:

- Windows 8
- Windows Server 2012
- Windows 7, 32-bit edition
- Windows 7, 64-bit edition using Windows on Win32 (WOW)
- Windows Server 2008 R2, using WOW

Additionally, the Planning Tool requires Microsoft .NET Framework 4.5.

After the preinstallation requirements are met, you can then install the Planning Tool.

⊟To install the Planning Tool

1. Log on to the local computer as a member of the Administrators group.
2. Using Windows Explorer or a command window, locate the directory where you downloaded the Planning Tool installation files.
3. Locate the LyncPlanningTool.msi. In Windows Explorer, double-click the file. In the command window, type the name of the file, and then press **Enter** to run the file.
4. On the Welcome page of the **Microsoft Lync Server 2013, Planning Tool Setup Wizard**, click **Next**.
5. Review the **End-User License Agreement**, select **I accept the terms in the License Agreement** if you choose to accept the terms of use in the license agreement, and then click **Next**.
6. Choose where to install the Planning Tool files. The default location is C:\Program Files (x86)\Microsoft Lync Server 2013\Planning Tool. If you want to change the installation location, click **Change**. On **Change destination folder**, browse or type the location to install the files, click **OK**, and then click **Next**.
7. The installer is now ready to install the Planning Tool. Click **Install** to begin the installation process.
8. The installation will start, and the progress will be displayed. After the installation is successfully completed, click **Finish**.
9. The Planning Tool is ready for use.

Concepts

Installing Optional Software

1.4.1.4.2 Installing Optional Software

Installing Optional Software

See Also

Deployment > Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool >

Topic Last Modified: *2013-02-21*

The Microsoft Lync Server 2013, Planning Tool is designed to export to Microsoft Excel and Microsoft Visio. While these applications are not required for the operation of the Planning Tool, they do add significant value to the deployment and documentation of your design.

Optional Software

Microsoft Excel

Exporting your design to Microsoft Excel creates a report that displays seven tabs in the spreadsheet:

- Summary – Displays information on site configuration, including user count, capacity settings, and server profile information.
- Hardware Profile – Displays a report on the recommended hardware configurations for servers that are specified in the topology, including CPU, memory, disk, and network interface. The quantity and recommended specifications for the server components are also included. In addition, each server is defined by site to provide a complete representation of server requirements by site.
- Ports Requirements – Displays a report of all ports that are enabled, and the association to Domain Name System load balancing (DNS LB) and hardware load balancers (HLB). You should use this report to plan your firewall and DNS LB and HLB configurations.
- Summary Report – Displays the general summary of the settings that are required to set up your Edge Server network.
- Certificates Report – Displays the subject name and subject alternate names that are required for the certificates needed to get the Edge Servers running.
- Firewall Report – Displays the source and destination ports and IP addresses for both External and Internal interfaces.
- DNS Report – Displays the fully qualified domain name (FQDN) and IP/VIP addresses required for each DNS entry that you create.

Microsoft Visio

Exporting your design to Microsoft Visio creates a diagram for use in your documentation purposes of your configured topology and infrastructure. The imported diagram can be edited and rearranged to meet your documentation needs. The typical Visio diagram will include:

Note:

If your design is large enough to require more than three Front End Servers, an additional page will be created for the Front End pool, Front End Servers, the computer running SQL Server, IP addresses, and FQDNs.

- Global Topology – Diagram of configured Lync Server 2013 sites.
- Site Name tab – Displays the site configuration topology with Edge Server, firewall, public switched telephone network (PSTN) with gateways, and the internal server deployment. Internal deployment consists of configured servers and pools, including the Front End pools, SQL Server-based servers, Active Directory Domain Services (AD DS), Directors, Exchange Unified Messaging (UM) servers, Exchange Mailbox Servers, Office Web Apps Servers, Mediation Servers, and Persistent Chat Servers.
- Edge Network Diagram – Diagram detailing the Edge Server configuration with associated IP addresses and FQDNs. DNS load balancing and hardware load balancers are also included. Additionally, Directors and the Front End Server or Front End pool are displayed, with associated DNS LB or HLB and the assigned IP address (the Planning Tool supports both IPv4 and IPv6 addresses) and FQDN.

See Also

Tasks

Installing the Planning Tool

1.4.1.4.3 Navigating the Planning Tool

Navigating the Planning Tool

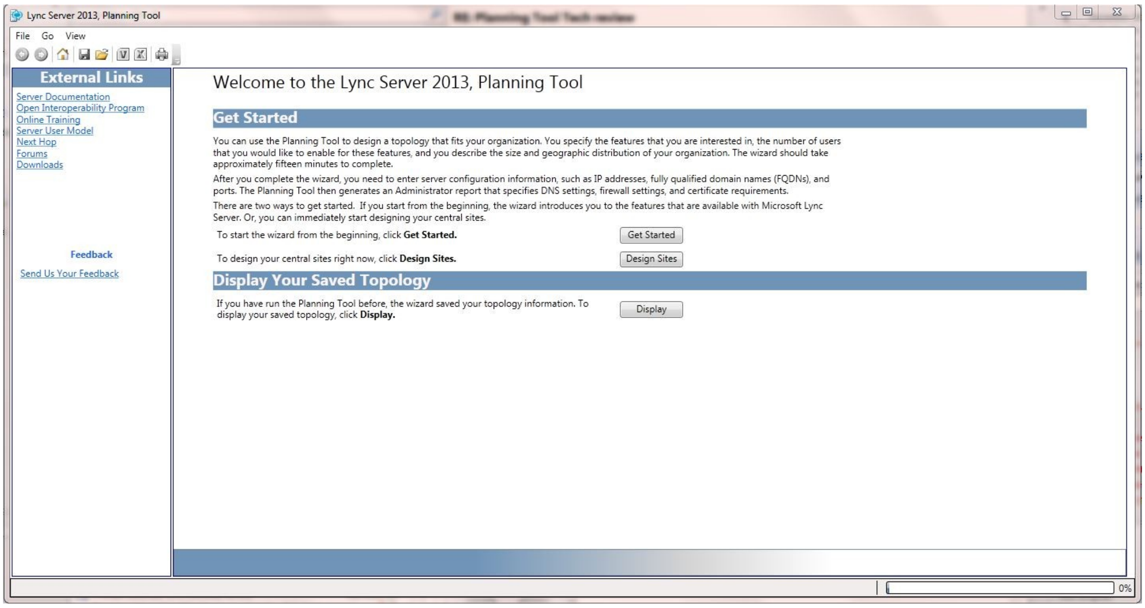
See Also

Deployment > Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool >

Topic Last Modified: *2013-02-21*

You navigate the Microsoft Lync Server 2013, Planning Tool by using a combination of a toolbar, page-specific buttons and links, and context-specific panes. The context-specific panes provide design information for planning and capacity that is relevant to the selection options on a specific page.

On starting the Planning Tool, a designer first sees the **Welcome to the Planning Tool for Microsoft Lync Server 2013** page.



Welcome to the Lync Server 2013, Planning Tool

Get Started

You can use the Planning Tool to design a topology that fits your organization. You specify the features that you are interested in, the number of users that you would like to enable for these features, and you describe the size and geographic distribution of your organization. The wizard should take approximately fifteen minutes to complete.

After you complete the wizard, you need to enter server configuration information, such as IP addresses, fully qualified domain names (FQDNs), and ports. The Planning Tool then generates an Administrator report that specifies DNS settings, firewall settings, and certificate requirements.

There are two ways to get started. If you start from the beginning, the wizard introduces you to the features that are available with Microsoft Lync Server. Or, you can immediately start designing your central sites.

To start the wizard from the beginning, click **Get Started.**

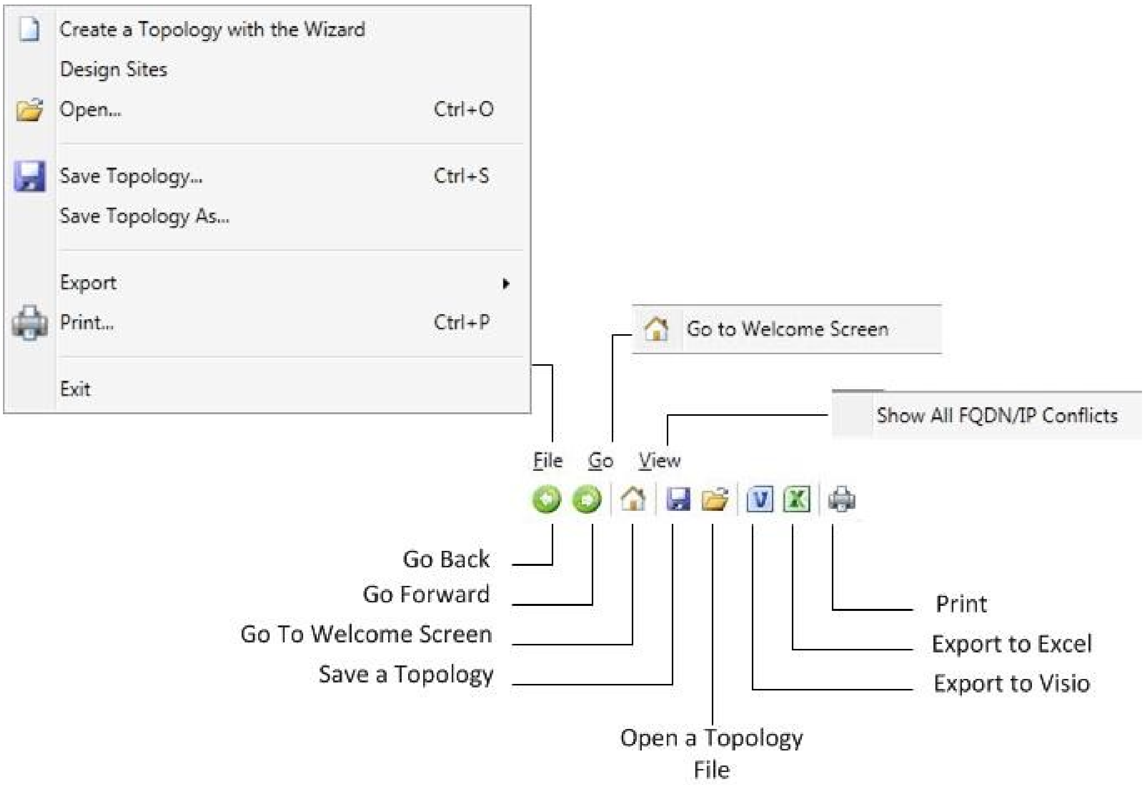
To design your central sites right now, click **Design Sites.**

Display Your Saved Topology

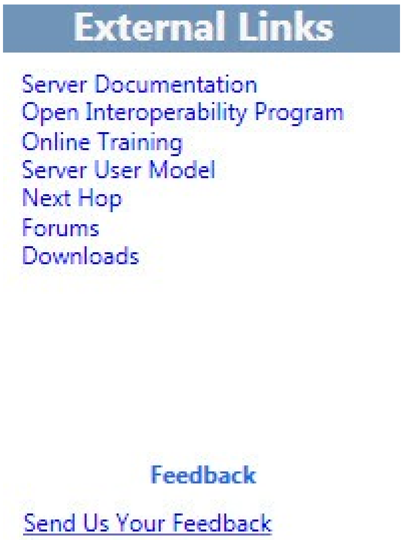
If you have run the Planning Tool before, the wizard saved your topology information. To display your saved topology, click **Display.**

On the Welcome page, the designer chooses **Get Started**, **Design Sites**, or **Display**. For details, see Create the Initial Design.

At the top of the Planning Tool is a toolbar that provides easy access to frequently used functions. The toolbar is displayed here for reference, and each function will be discussed in related topics.

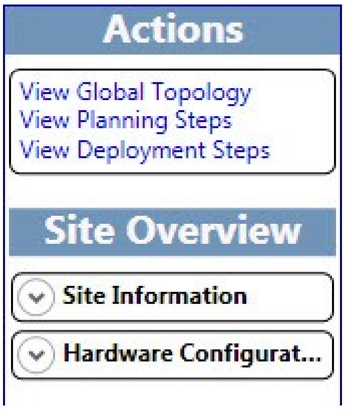


The Planning Tool has an External Links section on the left side of the tool. From here, the designer has easy access to planning and deployment information, and other technical resources such as training, technical blogs, forums, and other downloadable resources. Also in the External Links section is a Feedback link to the Lync Server 2013 Planning Tool team.



A context-sensitive Actions pane is displayed on many pages in the Planning Tool. The Actions pane gives the designer easy access to main sections of the topology. The links available in the Actions pane change based on the detail level in your topology. The Actions pane is available after you have completed the interview questions and displayed your topology. Included in the Actions pane is the Overview section, which displays numbers that the designer has entered as part of the interview process. The overview is contextually related to the displayed information.

Additionally, hardware information is displayed in the overview under the Actions pane. The hardware configuration displays a list of hardware requirements that the current topology recommends.



Tasks

Create the Initial Design

Concepts

Editing the Design

Other Resources

Reviewing the Administrator Reports

1.4.1.4.4 Create the Initial Design

Create the Initial Design

See Also

Deployment > Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool >

Topic Last Modified: *2013-02-21*

After you have finished installing the Lync Server 2013, Planning Tool, you are ready to start the Planning Tool and begin designing the proposed Lync Server 2013 infrastructure.

Note:
The Planning Tool is a wizard-driven tool with detailed guides to inform your decision-making process in designing your sites and topology. This topic is intended not as an exhaustive guide, but simply to help get you started using the Planning Tool in your design sessions.

To get started using the Planning Tool and create the initial design

1. Start the Lync Server 2013, Planning Tool: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Planning Tool**.
2. After the Planning Tool has started, the **Welcome to the Planning Tool for Microsoft Lync Server 2013** page appears. Choose one of the following options to begin your design:
   - **Option 1: Get Started** Clicking **Get Started** provides a specific series of interview questions with relevant selections to define the criteria. After you have finished the initial **Get Started** interview section, you proceed into **Design Sites** to define your site architecture. To complete this option,

proceed to step 3.

- **Option 2: Design Sites** Clicking **Design Sites** at the Welcome page bypasses the interview questions presented in the **Get Started** section. The information that would have been gathered by responding to the interview questions in **Get Started** section is set to default values with this option. By clicking **Design Sites**, the experienced designer can bypass the initial interview and change the default values, as needed, on the **Central Sites** start page. To complete this option, skip over steps 3-5 and start at step 6.
- **Option 3: Display Your Saved Topology** If you have already completed and saved a topology through previous use of the Planning Tool, you can skip over most of these steps and start by opening and displaying the topology. You can also make changes and updates to the topology, resave it, and then export it to Microsoft Excel or Microsoft Visio. To complete this option, skip over steps 3-12 and start at step 13.

3. Click **Get Started** to begin designing your Lync Server 2013 topology.
4. Answer each section by selecting the appropriate criteria for your design, and then click **Next** to proceed to the next Wizard page. Click **Back** to make changes on previous pages.

Tip:

Each page has a description of the selection criteria, and recommendations based on preferred practices and capacity planning. If you require additional details, click **Learn more** to read detailed information from the Lync Server 2013 Planning documentation on the Microsoft TechNet website. You must have Internet connectivity to access the Microsoft TechNet website.

5. Select the appropriate options for your design. After the initial criteria are defined, a page will confirm that your Features Overview is complete.
6. Click **Design Sites** to define your central site.

Note:

Each Lync Server 2013 topology will have at least one central site. Your design may have a single central site, a central site with a number of branch sites, a number of central sites, or a number of central sites with branch sites associated with each central site.

7. In **Site Name**, type the name that will identify this central site.
8. In **Site Homed Users**, type the expected number of on-premises concurrent users who will be homed in this central site.
9. In **Cloud Homed Users**, type the expected number of online concurrent users who will be homed in this central site.
10. Modify the selections for Online Collaboration, Users, Voice, Additional Deployment Options, or Server Applications, as needed.

Important:

At this point in the design, you can only select or clear options for your deployment. However, you can configure more options in a later phase of the Planning Tool. There are also options that are unavailable and cannot be cleared. In addition, you may have to clear one option in order to clear another. For example, if you clear the **Enterprise Voice** option under Voice, then the **Response Group**, **Announcement**, and **Call Park** options under Server Applications (all of which are features of Enterprise Voice) are also cleared.

11. After defining a site name and number of users, click **Next**.
12. The following pages ask for information about SIP domains, conference settings, voice settings and infrastructure, Exchange UM, external user access, Persistent Chat settings, client settings, collocation options, and branch sites. Answer these questions as appropriate.
13. The final question asks if you want to create another central site. If you select **Yes**, then the Planning Tool returns to the Central Sites page. If you select **No**, click **Next**, and then click **Draw** to display the high-level Global

Topology view.
14.To view an existing topology, click **Display**.
15.Click the .xml file that represents the previously saved topology, and then click **Open**.
16.The Planning Tool displays the Global Topology page. You can now begin editing, updating, or changing the topology by using the tools available in the Planning Tool.

Concepts

Editing the Design

1.4.1.4.5 Editing the Design

Editing the Design

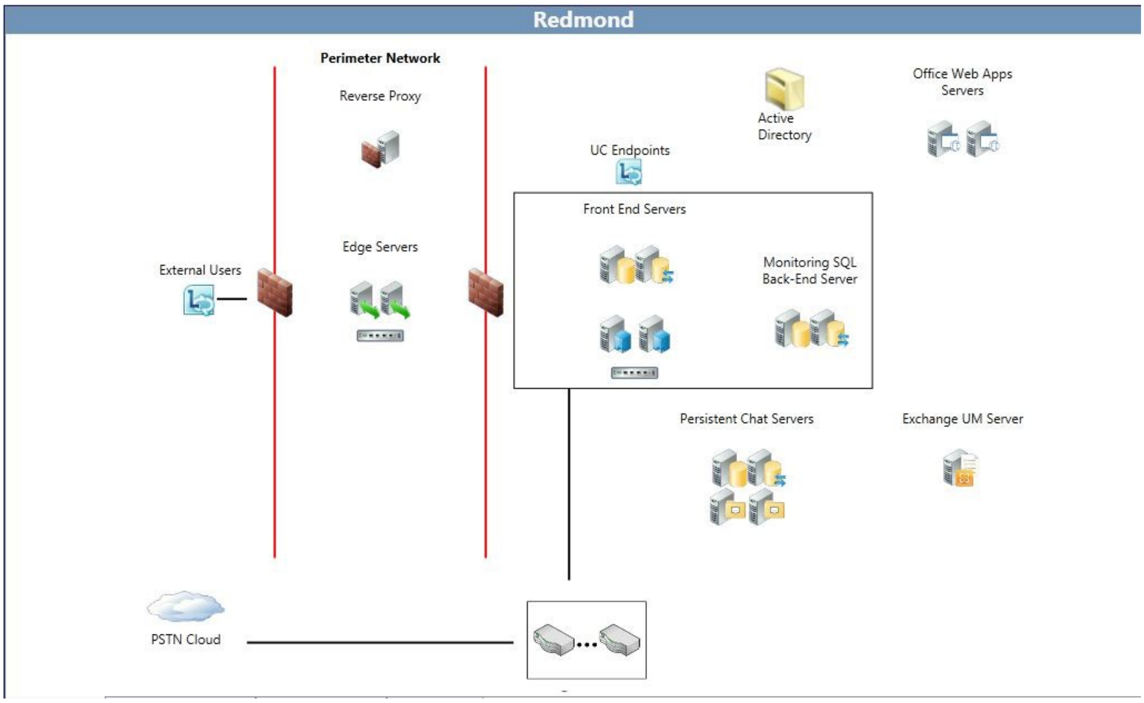
See Also

Deployment > Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool >

Topic Last Modified: *2013-02-21*

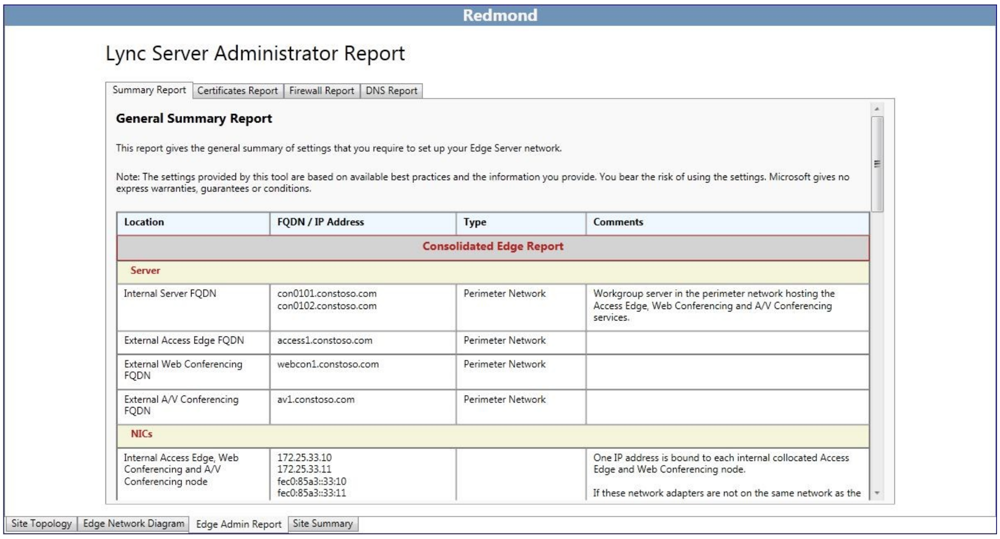
After completing the initial interview questions, you can edit the fully qualified domain name (FQDN) and IP addresses for the site. To do this, on the **Global Topology** page, double-click the site that you want to edit.

The Planning Tool displays the site topology for the selected site. At the bottom of the site page are four tabs:



- Site Topology – The currently displayed page with a visual overview of the topology as recommended.
- Edge Network Diagram – The Edge Network Diagram page is where the designer does most of the work in the Planning Tool. The diagram displays the network configuration for a recommended Lync Server 2013 topology, with editable entries for IP addresses and FQDNs for servers, pool, and both hardware and Domain Name System (DNS) load balancers.

- Edge Admin Report – The Edge Admin Report contains a total of four reports:



Lync Server Administrator Report

General Summary Report

This report gives the general summary of settings that you require to set up your Edge Server network.

Note: The settings provided by this tool are based on available best practices and the information you provide. You bear the risk of using the settings. Microsoft gives no express warranties, guarantees or conditions.

Location	FQDN / IP Address	Type	Comments
Consolidated Edge Report			
Server			
Internal Server FQDN	con0101.constoso.com con0102.constoso.com	Perimeter Network	Workgroup server in the perimeter network hosting the Access Edge, Web Conferencing and A/V Conferencing services.
External Access Edge FQDN	access1.constoso.com	Perimeter Network	
External Web Conferencing FQDN	webcon1.constoso.com	Perimeter Network	
External A/V Conferencing FQDN	av1.constoso.com	Perimeter Network	
NICs			
Internal Access Edge, Web Conferencing and A/V Conferencing node	172.25.33.10 172.25.33.11 fec0:85a3::33:10 fec0:85a3::33:11		One IP address is bound to each internal collocated Access Edge and Web Conferencing node. If these network adapters are not on the same network as the

  - Summary Report – A general report of settings for the Edge network configuration. If you edit the values on the **Edge Network Diagram** page to the topology TCP/IP and FQDN values of that will be used in the actual deployment, those addresses and names will be represented here. Otherwise, the default text will appear.
  - Certificate Report – The certificate report will list the subject name and subject alternative names for the certificates that are required for the topology.
  - Firewall Report – The firewall report lists information necessary to configure perimeter firewalls in the infrastructure. This includes the IP addresses (either the default or edited values), server role, source IP and port, destination IP and port, transport protocol, application protocol, and relevant notes.
  - DNS Report – The DNS Report lists relevant information for the DNS entries that you must create. The record type, FQDN, IP address, and comments necessary for the proper operation are included.
- Site Summary – The site summary presents an overview of the selections that you made by either answering the initial interview questions or filling in the values in **Design Sites**. Capacity information is also presented.

Note:

The information on the Site Summary page is customized for each design and may not contain all sections or information detailed here.

Concepts

Editing the Network Configuration Diagram

1.4.1.4.5.1 Editing the Netw ork Configuration Diagram

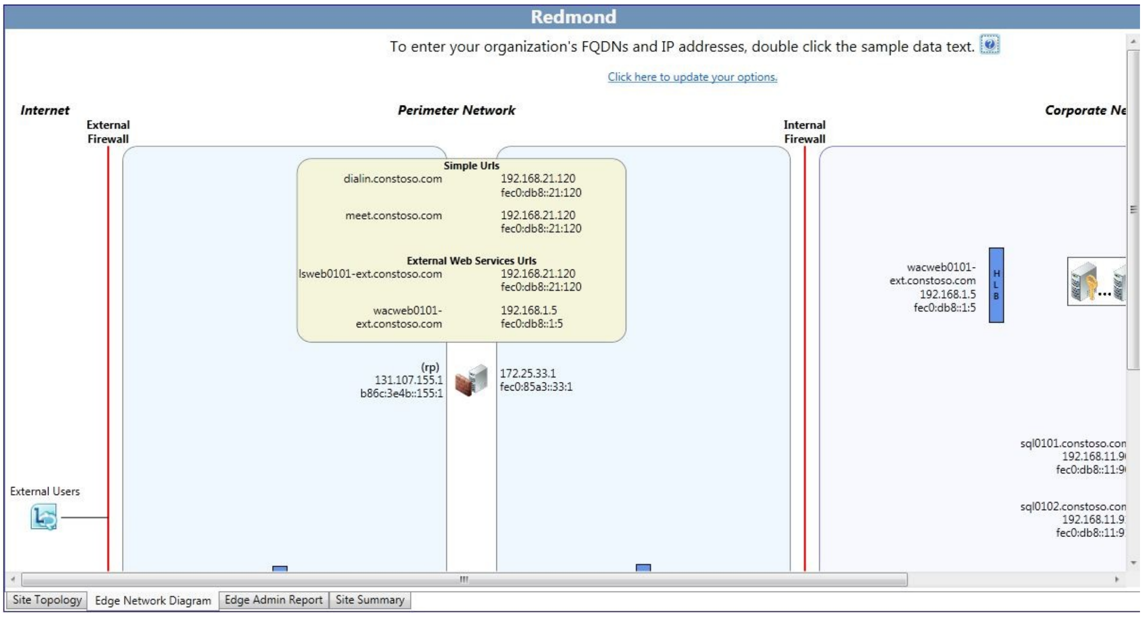
Editing the Network Configuration Diagram

See Also

Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool > Editing the Design >

Topic Last Modified: *2013-02-21*

Most of the work that a designer does in the Lync Server 2013, Planning Tool consists of defining the entries for the IP addresses and fully qualified domain names (FQDNs) for the entries on the network diagram. The information that is entered on this page carries over into the reports and other information contained in the Planning Tool.



To enter your organization's FQDNs and IP addresses, double click the sample data text.

The Planning Tool creates a network diagram with default text for IP addresses and FQDNs.

To edit the network diagram and input values:

1. Choose a section of the network to begin working on. For example, double-click the text, **access1.contoso.com**. In the dialog box that opens, type the actual FQDN of the server access1.contoso.com and the actual IP address, replacing the 131.107.155.3.
2. Click **OK** to save the entries.
3. Continue to edit IP addresses and FQDNs, providing virtual IP addresses for hardware load balancers or server entries for Domain Name System (DNS) load balancing for servers in pools.

A helpful feature of the Planning Tool is that it can incrementally assign a range of IP addresses and server host names, rather than requiring the designer to edit each separate server in a pool. For example:

1. Double-click the pooled Front End Servers. When the dialog box opens, select **Do you want to use the IPs and FQDN as starting points for all equivalent servers in this cluster?**.
2. For example, the starting value for the first server is fe0101.contoso.com and an IP address of 192.168.21.122.
3. Type **fe0.contoso.com** in **Front End Server FQDN**, type **192.168.21.131** in **Front End Server IP address**, and then click **OK**.
4. The auto-increment feature updates all servers in the pool to fe01 through fe06, and all IP address from 192.168.21.131 to 136.

After you have completed all edits, save the topology by completing the following steps:

To save the Planning Tool design, click **File**, and then click **Save Topology** or **Save Topology As**. If a **Save Planning Tool As** dialog box appears, type a name for the file in

File name, and then click **Save**.

Concepts

Editing the Design

1.4.1.4.6 Reviewing the Administrator Reports

Reviewing the Administrator Reports

Deployment > Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool >

Topic Last Modified: *2013-02-21*

The Administrator Reports are detailed information for deployment and operations. The reports are generated based on the selections marked in **Design Sites**. The designer can further add value to the Administrator Reports by editing the network diagrams and defining the complete IP addresses and fully qualified domain names (FQDNs) for servers, pools, and load balancers.

- Reviewing the Summary Report
- Reviewing the Certificates Report
- Reviewing the Firewall Report
- Reviewing the DNS Report

1.4.1.4.6.1 Reviewing the Summary Report

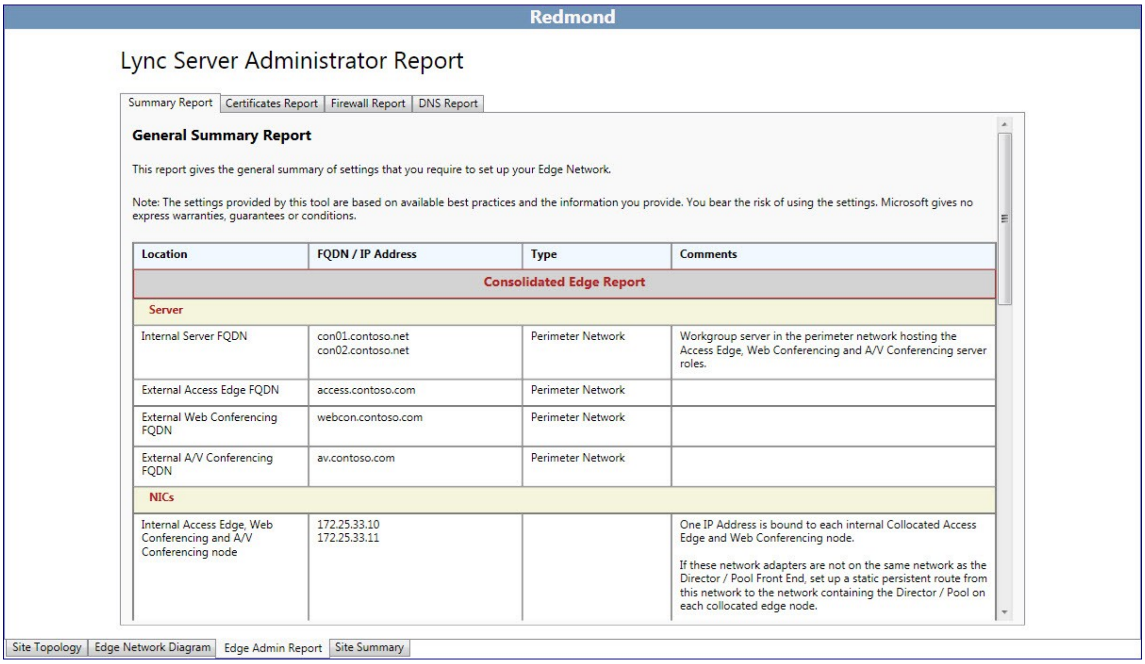
Reviewing the Summary Report

See Also

Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool > Reviewing the Administrator Reports >

Topic Last Modified: *2013-02-21*

The Lync Server Administrator Report is the first of four valuable reports that document your design in detail. The information in this report, and the other three associated reports, is excellent documentation for your Information Technology Teams:



Lync Server Administrator Report

General Summary Report

This report gives the general summary of settings that you require to set up your Edge Network.

Note: The settings provided by this tool are based on available best practices and the information you provide. You bear the risk of using the settings. Microsoft gives no express warranties, guarantees or conditions.

Location	FQDN / IP Address	Type	Comments
Consolidated Edge Report			
Server			
Internal Server FQDN	con01.contoso.net con02.contoso.net	Perimeter Network	Workgroup server in the perimeter network hosting the Access Edge, Web Conferencing and A/V Conferencing server roles.
External Access Edge FQDN	access.contoso.com	Perimeter Network	
External Web Conferencing FQDN	webcon.contoso.com	Perimeter Network	
External A/V Conferencing FQDN	av.contoso.com	Perimeter Network	
NICs			
Internal Access Edge, Web Conferencing and A/V Conferencing node	172.25.33.10 172.25.33.11		One IP Address is bound to each internal Collocated Access Edge and Web Conferencing node. If these network adapters are not on the same network as the Director / Pool Front End, set up a static persistent route from this network to the network containing the Director / Pool on each collocated edge node.

- Certificates Report
- Firewall Report
- DNS Report

The Summary Report lists general configuration information associated with your Edge network. The location, fully qualified domain name (FQDN) and IP address, type of network, and comments specific to a given role are documented.

The designer and each of the teams that will deploy, manage, and maintain the infrastructure should review the summary report for accuracy and to make sure that errors are at a minimum.

Other Resources

Reviewing the Administrator Reports

1.4.1.4.6.2 Reviewing the Certificates Report

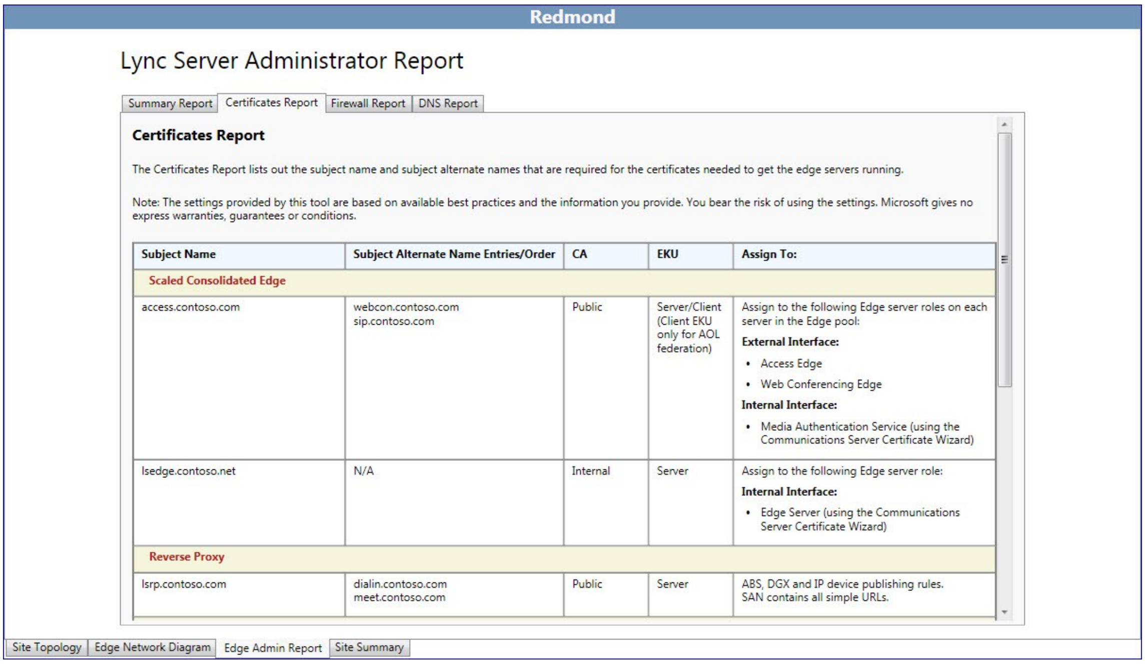
Reviewing the Certificates Report

See Also

Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool > Reviewing the Administrator Reports >

Topic Last Modified: *2013-02-21*

The Certificates Report contains all certificates that are required in the recommended Lync Server 2013 deployment. The Planning Tool accounts for the subject names and subject alternative names that are entered. Default text that is left unedited may represent a potential challenge for the team responsible for requesting and issuing the certificates. Certificate information also contains information about where the certificate can typically be issued from. If the infrastructure does not have an internal public key infrastructure (PKI) in place, all certificates can be requested through a public certificate provider. Extended key usages (EKU) and Assign To fields in the report are very helpful in understanding what the purpose and location for each certificate should be.



Redmond

Lync Server Administrator Report

Certificates Report

The Certificates Report lists out the subject name and subject alternate names that are required for the certificates needed to get the edge servers running.

Note: The settings provided by this tool are based on available best practices and the information you provide. You bear the risk of using the settings. Microsoft gives no express warranties, guarantees or conditions.

Subject Name	Subject Alternate Name Entries/Order	CA	EKU	Assign To:
Scaled Consolidated Edge				
access.contoso.com	webcon.contoso.com sip.contoso.com	Public	Server/Client (Client EKU only for AOL federation)	Assign to the following Edge server roles on each server in the Edge pool: **External Interface:** • Access Edge • Web Conferencing Edge **Internal Interface:** • Media Authentication Service (using the Communications Server Certificate Wizard)
lsedge.contoso.net	N/A	Internal	Server	Assign to the following Edge server role: **Internal Interface:** • Edge Server (using the Communications Server Certificate Wizard)
Reverse Proxy				
lsrp.contoso.com	dialin.contoso.com meet.contoso.com	Public	Server	ABS, DGX and IP device publishing rules. SAN contains all simple URLs.

Carefully review, and be sure to understand, the use and purpose of each certificate in the deployment. If there is a question about what a certificate does, determine which server or service is talking to what. Certificates in Lync Server 2013 are used for two primary purposes:

- Mutual Transport Layer Security (MTLS) – The computers involved in the communication each present a certificate that proves their identity to another computer. This is known as server authentication. Communication cannot begin until each computer trusts the other computer's identity.
- Encryption – Encryption (Secure Sockets Layer, or SSL, and Transport Layer Security, or TLS) is a critical means to help secure communications, help ensure privacy, and to create a trusted communications and collaboration system.

Other Resources

Reviewing the Administrator Reports

1.4.1.4.6.3 Reviewing the Firewall Report

Reviewing the Firewall Report

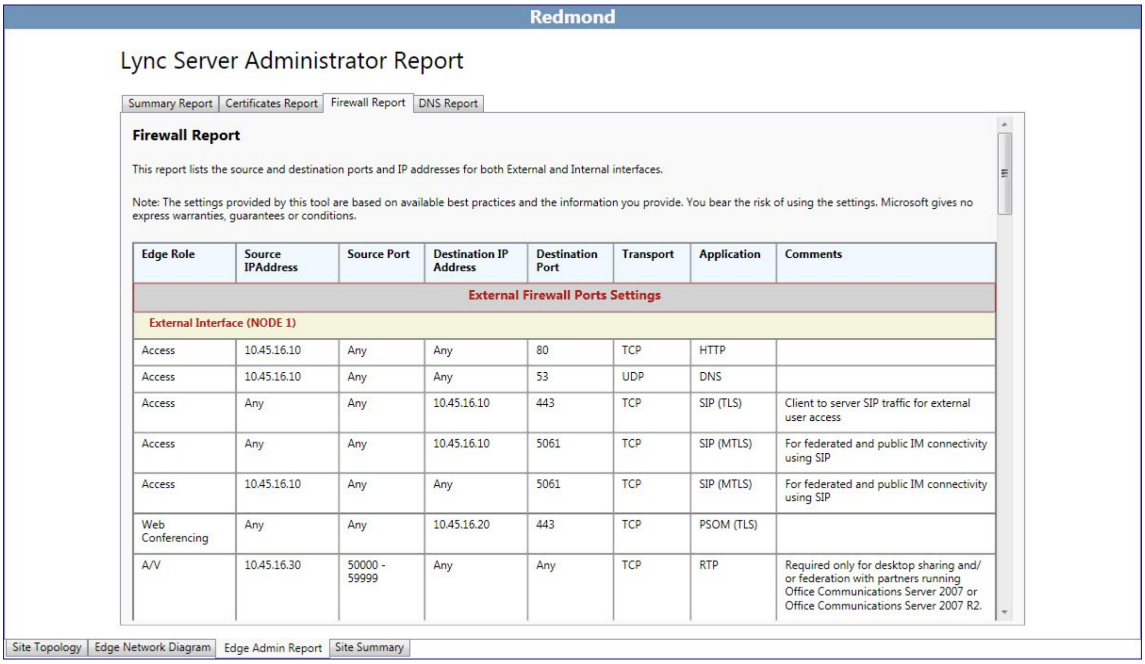
See Also

Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool > Reviewing the Administrator Reports >

Topic Last Modified: *2013-02-21*

Lync Server 2013 has a potentially complex set of firewall rules. The Planning Tool reduces this complexity by generating a report that defines in detail all firewall requirements, based on the designer's input criteria. The IT firewall administrator will be able to use this report to configure and define the necessary rules.

From the standpoint of firewall management, the report should be carefully reviewed to make sure that there are no conflicts with exiting firewall rules and that there are no policies or procedures that might be violated.



Firewall Report

This report lists the source and destination ports and IP addresses for both External and Internal interfaces.

Note: The settings provided by this tool are based on available best practices and the information you provide. You bear the risk of using the settings. Microsoft gives no express warranties, guarantees or conditions.

Edge Role	Source IPAddress	Source Port	Destination IP Address	Destination Port	Transport	Application	Comments
External Firewall Ports Settings							
External Interface (NODE 1)							
Access	10.45.16.10	Any	Any	80	TCP	HTTP	
Access	10.45.16.10	Any	Any	53	UDP	DNS	
Access	Any	Any	10.45.16.10	443	TCP	SIP (TLS)	Client to server SIP traffic for external user access
Access	Any	Any	10.45.16.10	5061	TCP	SIP (MTLS)	For federated and public IM connectivity using SIP
Access	10.45.16.10	Any	Any	5061	TCP	SIP (MTLS)	For federated and public IM connectivity using SIP
Web Conferencing	Any	Any	10.45.16.20	443	TCP	PSOM (TLS)	
A/V	10.45.16.30	50000 - 59999	Any	Any	TCP	RTP	Required only for desktop sharing and/ or federation with partners running Office Communications Server 2007 or Office Communications Server 2007 R2.

Other Resources

Reviewing the Administrator Reports

1.4.1.4.6.4 Reviewing the DNS Report

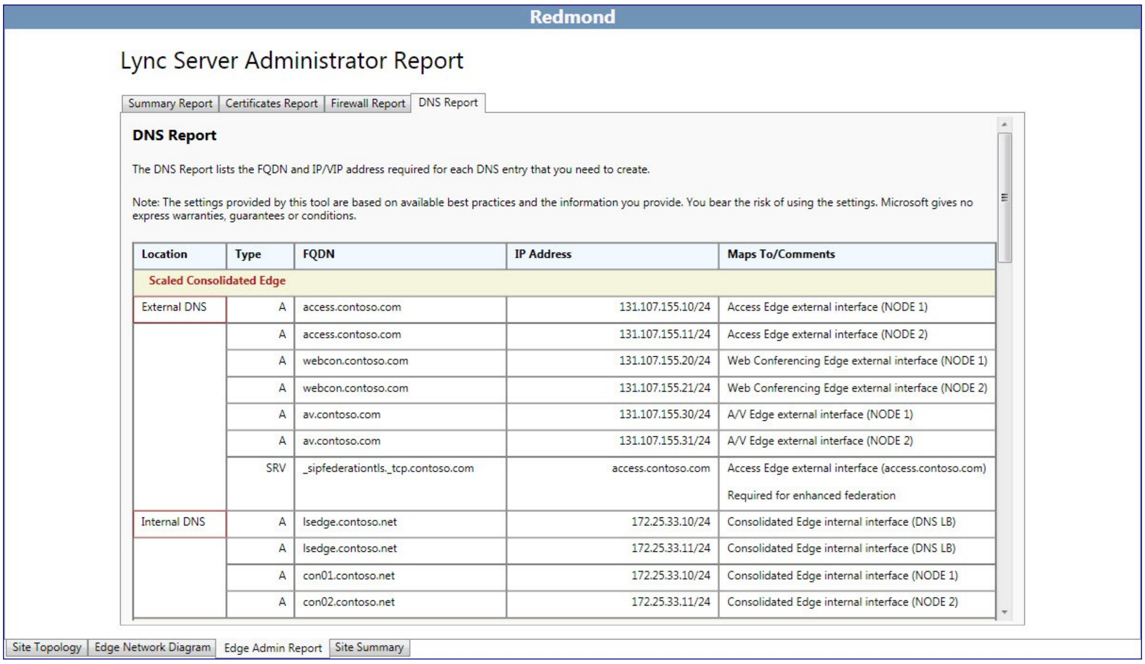
Reviewing the DNS Report

See Also

Deploying Lync Server 2013 > Designing the Topology by Using the Planning Tool > Reviewing the Administrator Reports >

Topic Last Modified: *2013-02-21*

The DNS Report, which is part of the Administrator Report, details all of the recommended and known entries for the Domain Name System (DNS) in the internal, perimeter, and external networks. If the designer has completed the edits to the network diagram, and all IP addresses and fully qualified domain names (FQDNs) are defined to their production values, the DNS Report provides an excellent configuration resource. This report can also serve as an operational troubleshooting document.



Lync Server Administrator Report

DNS Report

The DNS Report lists the FQDN and IP/VIP address required for each DNS entry that you need to create.

Note: The settings provided by this tool are based on available best practices and the information you provide. You bear the risk of using the settings. Microsoft gives no express warranties, guarantees or conditions.

Location	Type	FQDN	IP Address	Maps To/Comments
Scaled Consolidated Edge				
External DNS	A	access.contoso.com	131.107.155.10/24	Access Edge external interface (NODE 1)
	A	access.contoso.com	131.107.155.11/24	Access Edge external interface (NODE 2)
	A	webcon.contoso.com	131.107.155.20/24	Web Conferencing Edge external interface (NODE 1)
	A	webcon.contoso.com	131.107.155.21/24	Web Conferencing Edge external interface (NODE 2)
	A	av.contoso.com	131.107.155.30/24	A/V Edge external interface (NODE 1)
	A	av.contoso.com	131.107.155.31/24	A/V Edge external interface (NODE 2)
	SRV	_sipfederationtls._tcp.contoso.com	access.contoso.com	Access Edge external interface (access.contoso.com) Required for enhanced federation
Internal DNS	A	lsedge.contoso.net	172.25.33.10/24	Consolidated Edge internal interface (DNS LB)
	A	lsedge.contoso.net	172.25.33.11/24	Consolidated Edge internal interface (DNS LB)
	A	con01.contoso.net	172.25.33.10/24	Consolidated Edge internal interface (NODE 1)
	A	con02.contoso.net	172.25.33.11/24	Consolidated Edge internal interface (NODE 2)

You should have your DNS management team review the DNS Report thoroughly to make sure that there are no errors that may cause difficulty during deployment or that may complicate a troubleshooting session.

Other Resources

Reviewing the Administrator Reports

1.4.1.5 Defining and Configuring the Topology

Defining and Configuring the Topology

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2012-09-14*

You define and configure your topology by using Topology Builder. Topology Builder does not require you to be a member of the local Administrators group or a privileged domain group (such as Domain Admins). You can define your topology as a standard user. When you start Topology Builder on first use and subsequent edit sessions, you are prompted for the location where you want Topology Builder to load the current configuration document. The choices are the following:

- Download topology from existing deployment
- Open topology from a local file
- New topology

If you have already defined a topology and have established the Central Management store, you should choose to download a topology from an existing deployment. Topology Builder will read the database and retrieve the current definition. If you have an existing Central Management store, you should always choose this option.

If you have not established a Central Management store and want to edit a previously saved configuration, you should choose to open the topology from a local file. The file that you will open would be the configuration file that was saved in a previous session. You can use this option to edit the previously saved topology.

⚠**Warning:**
If you already have a published topology, you should not load a local configuration file. You should choose to download the topology from an existing deployment.

Choose to create a new topology, if you want to create a new Topology Builder configuration. A previously saved design is not overwritten unless you choose to save it as the same file that you created in an earlier design session.

In each of these options, you will be prompted for a location to store the Topology Builder configuration file. The location for the file could be a local location, a shared location on an established file share, or removable media.

- Define and Configure a Topology in Topology Builder
- Define and Configure a Front End Pool or Standard Edition Server
- Deploying Paired Front End Pools for Disaster Recovery
- Deploying SQL Mirroring for Back End Server High Availability
- Edit or Configure Simple URLs
- Select the Central Management Server

1.4.1.5.1 Define and Configure a Topology in Topology Builder

Define and Configure a Topology in Topology Builder

Deployment > Deploying Lync Server 2013 > Defining and Configuring the Topology >

Topic Last Modified: *2013-02-21*

Running Topology Builder to define a new topology or to modify an existing topology does not require membership in a local administrator or privileged domain group. Topology Builder guides you through the steps necessary to define your topology for an Enterprise Edition Front End pool or a Standard Edition, based on your configuration requirements.

You must use Topology Builder to complete and publish the topology before you can install Lync Server 2013 on servers. The following procedure includes the steps required to define a new topology.

⊟To define a topology

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In Topology Builder, select **New Topology**. You are prompted for a location and file name for saving the topology. Give the topology file a meaningful name and accept the default extension of .tbxml. Click **OK**.
3. Navigate to the location where you want to save the new topology XML file, enter a name for the file, and then click **Save**.
4. On the **Define the primary domain** page, enter the name of the primary SIP domain for your organization, and then click **Next**.
5. On the **Specify additional supported domains** page, enter the names of additional domains, if any, and then click **Next**.
6. On the **Define the first site** page, enter a name and a description for the first site, and then click **Next**.
7. On the **Specify site details** page, enter the location information for the site, and then click **Next**.
8. On the **New topology was successfully defined** page, make sure the **Open the New Front End Wizard when this wizard closes** check box is selected, and then click **Finish**.

After you’ve defined and saved the topology, use the New Front End Wizard to define a

Front End pool or Standard Edition server for your site. For details, see Define and Configure a Front End Pool or Standard Edition Server.

1.4.1.5.2 Define and Configure a Front End Pool or Standard Edition Server

Define and Configure a Front End Pool or Standard Edition Server

Deployment > Deploying Lync Server 2013 > Defining and Configuring the Topology >

Topic Last Modified: *2013-03-08*

This procedure does not require membership in a local administrator or privileged domain group. You should log on to a computer as a standard user.

If you are deploying an Enterprise server, a minimum number of Front End Servers in a pool must be running at all times. The following table summarizes these requirements.

Total number of Front End Servers in the pool	Number of servers that must be running for pool to be functional
1-2	1
3-4	2
5-6	3
7-8	4
9-10	5
11-12	6

Note:

For Lync Server 2013, any time you add or remove a Front End Server from the pool, you must restart services. Removing and adding servers should be done as separate operations. For example, if you are going to add two Front End Servers and remove two Front End Servers, use the following process:

1. Remove the two Front End Servers.
2. Publish and re-activate the topology.
3. Restart the services
4. Add the two Front End Servers.
5. Publish and re-activate the topology.
6. Restart the services.

After you have defined your topology, use the following procedure to define a Front End pool for your site. For details about defining the topology, see Define and Configure a Topology in Topology Builder.

⊟To define a Front End pool

1. In the Define New Front End Pool Wizard, on the **Define the New Front End pool** page, click **Next**.
2. On the **Define the Front End pool FQDN** page, enter a fully qualified domain name (FQDN) for the pool you are creating, click **Enterprise Edition Front End pool**, and then click **Next**.
3. On the **Define the computers in this pool** page, enter a computer FQDN for the first Front End Server in the pool, and then click **Add**. Repeat this step for any additional computers (up to twelve) that you want to add to the pool,

and then click **Next**.

4. On the **Select features** page, select the check boxes for the features that you want on this Front End pool. For example, if you are deploying only instant messaging (IM) and presence features, you would select the **Conferencing** check box to allow multiparty IM but would not select the **Dial-in (PSTN) conferencing**, **Enterprise Voice**, or **Call Admission Control** check boxes, because they represent voice, video, and collaborative conferencing features.
   - **Conferencing** This selection enables a rich set of features including:
     - IM with more than two parties in an IM session.
     - Conferencing, which includes document collaboration, application sharing, and desktop sharing.
     - A/V conferencing, which enables users to have real-time audio/video (A/V) conferences without the need for external services such as the Live Meeting service or a third-party audio bridge.
   - **Dial-in (PSTN) conferencing** Allows users to join the audio portion of a Lync Server 2013 conference by using a public switched telephone network (PSTN) phone without requiring an audio conferencing provider.
   - **Enterprise Voice** Enterprise Voice is the Voice over IP (VoIP) solution in Lync Server 2013 that allows users to make and receive phone calls. You would deploy this feature if you plan to use Lync Server 2013 for voice calls, voice mail, and other functions that use a hardware device or a software client.
   - **Call admission control (CAC)** CAC determines, based on available network bandwidth, whether to allow real-time communications sessions such as voice or video calls to be established. If you have deployed only IM and presence, CAC is not needed because neither of these two features uses CAC.
   - **Archiving** Archiving provides a way for you to archive IM content, conferencing (meeting) content, or both that is sent through Lync Server 2013.
   - **Monitoring** Monitoring Server enables you to collect numerical data that describes the media quality on your network and endpoints, usage information related to VoIP calls, IM messages, A/V conversations, meetings, application sharing, and file transfers, and call error and troubleshooting information for failed calls.

   Note:
   If you would like to enable CAC in your deployment, it is required that you enable CAC in exactly one pool per central site. CAC is recommended if you are deploying voice features or A/V conferencing.

   The following table shows the available features (top) and the functions offered to users (left). The selections in the table are what you should select to enable those features for your organization.

	Conferencing	Dial-In Conferencing	Enterprise Voice	Call Admission Control
Instant messaging and presence	X			
Conferencing	X	X		
A/V conferencing	X	X		X
Enterprise Voice			X	X

5. On the **Select collocated server roles** page, you can to collocate the Mediation Server on the Front End Server or to deploy it as a stand-alone server.

You can collocate the Mediation Server on the Front End pool.

- If you intend to collocate the Mediation Server on the Enterprise Edition Front End pool, ensure the check box is selected. The server role will be deployed on the pool servers.
- If you intend to deploy the Mediation Server as a stand-alone server, clear the appropriate check box. You will deploy Mediation Server in a separate deployment step after you completely deploy the Front End Server.

> **Note:**
>
> We recommend that you collocate the Mediation Server if possible. For details about support for collocated or stand-alone Mediation Servers, see Components and Topologies for Mediation Server in the Planning documentation.

6. The **Associate server roles with this Front End pool** page lets you define and associate server roles with the Front End pool. The following role is available:

   Enable an Edge pool Defines and associates a single Edge Server or a pool of Edge Servers. An Edge Server facilitates communication and collaboration between users inside the organization and people outside the organization, including federated users.

   There are two possible scenarios that you can use to deploy and associate the server roles:

   For scenario one, you are defining a new topology for a new installation. You can approach the installation in one of two ways:

   - Leave the check box clear and proceed with defining the topology. After you have published, configured, and tested the Front End and Back End Server roles, you can run Topology Builder again to add the role servers to the topology. This strategy will enable you to test the Front End pool and the server running SQL Server without additional complications from additional roles. After you have completed your initial testing, you can run Topology Builder again to select the roles you need to deploy.
   - Select roles that you need to install, and then set up the hardware to accommodate the selected roles.

   For scenario two, you have an existing deployment and your infrastructure is ready for new roles or you need to associate existing roles with a new Front End Server:

   - In this case, you will select the roles that you intend to deploy or associate with the new Front End Server. In either case, you will proceed with the definition of the roles, set up any needed hardware, and proceed with the installation.
7. On the **Define the SQL store** page, do one of the following:
   - To use an existing SQL Server store that has already been defined in your topology, select an instance from **SQL store**.
   - To define a new SQL Server instance to store pool information, click **New** and then specify the **SQL Server FQDN**in the **Define New SQL Store** dialog box.
   - To specify the name of a SQL Server instance, select **Named Instance**, and then specify the name of the instance.
   - To use the default instance, click **Default instance**.
   - To use SQL Mirroring, select **Enable SQL mirroring** and select an existing instance or create a new instance.
8. On the **Define the file share** page, do one of the following:
   - To use a file share that has already been defined in your topology, select **Use a previously defined file share**.
   - To define a new file share, select **Define a new file share**, in the **File Server FQDN** box, enter the FQDN of the existing file server where the file share is to reside, and then enter a name for the file share in the **File Share** box.

Important:

The file share for Lync Server 2013 cannot be located on the Front End Server. Note that in this example, the file share has been located on the SQL Server-based Back End Server. This might not be an optimal location for your organization's requirements, and a file server might be a better choice. You can define the file share without the file share having been created. You will need to create the file share in the location you define before you publish the topology.

9. On the **Specify the Web Services URL** page, do one or both of the following:

Important:

The base URL is the Web Services identity for the URL, minus the https://. For example, if the full URL for the Web Services of the pool is https://pool01.contoso.net, the base URL is pool01.contoso.net.

Warning:

If you have more than one Front End pool or Front End Server, the external Web services FQDN must be unique. For example, if you define the external Web services FQDN of a Front End Server as **pool01.contoso.com**, you cannot use **pool01.contoso.com** for another Front End pool or Front End Server.

- If you are configuring DNS load balancing, select the **Override internal Web Services pool FQDN** check box, enter the internal base URL (which must be different from the pool FQDN and could be, for example, internal-<your base URL>) in **Internal Base URL**.

  Warning:

  If you decide to override the Internal web services with a self-defined FQDN, each FQDN must be unique from any other Front End pool, Director or a Director pool. **Use only standard characters** (including A–Z, a–z, 0–9, and hyphens) when defining URLs or fully qualified domain names. Do not use Unicode characters or underscores. Nonstandard characters in a URL or FQDN are often not supported by external DNS and public CAs (that is, when the URL or FQDN must be assigned to the subject name or subject alternative name in the certificate).

- Optionally enter the external base URL in **External Base URL**. You would enter the external base URL to differentiate it from your internal domain naming. For example, your internal domain is contoso.net, but your external domain name is contoso.com. You would define the URL using the contoso.com domain name. This is also important in the case of a reverse proxy. The external base URL domain name would be the same as the domain name of the FQDN of the reverse proxy. Instant messaging and presence does require HTTP access to the Front End pool.

Note:

To use DNS load balancing, you must create the appropriate DNS records. For details, see Configure DNS for Load Balancing.

10. If you selected **Conferencing** on the **Select Features** page, on the **Select an Office Web Apps Server** page select **Associate pool with an Office Web Apps Server** and then click **New** (or select an existing Office Web Apps Server from the drop-down list).
11. In the **Define New Office Web Apps Server** dialog box, type the fully qualified domain name (FQDN) of your Office Web Apps Server computer in the **Office Web Apps Server FQDN** box; when you do this, your Office Web Apps Server discovery URL should automatically be entered into the **Office Web Apps Server discovery URL** box.

    If the Office Web Apps Server is installed on-premises and in the same network zone as Lync Server 2013 then the option **Office Web Apps Server**

is deployed in an external network (that is, perimeter/Internet) should not be selected.

If the Office Web Apps Server is deployed outside your internal firewall, then select the option **Office Web Apps Server is deployed in an external network (that is, perimeter/Internet)**.

> **Note:**
>
> For details, see Configuring Integration with Office Web Apps Server and Lync Server 2013.

12. On the **Define the Archiving SQL store** page, select an existing instance or SQL Server, or define a new instance to store the data associated with archiving data.
13. On the **Define the Monitoring SQL store** page, select an existing instance or SQL Server, or define a new instance to store the data associated with monitoring data.
14. Click **Next**. If you defined other role servers on the **Associate server roles with this Front End pool** page, separate role configuration wizard pages will open to let you configure the server roles. For details, see the following:

    Deploying External User Access
15. If you did not select additional server roles to configure and deploy, or when you have finished the configuration of the additional role servers, click **Finish**.

1.4.1.5.3 Deploying Paired Front End Pools for Disaster Recovery

Deploying Paired Front End Pools for Disaster Recovery

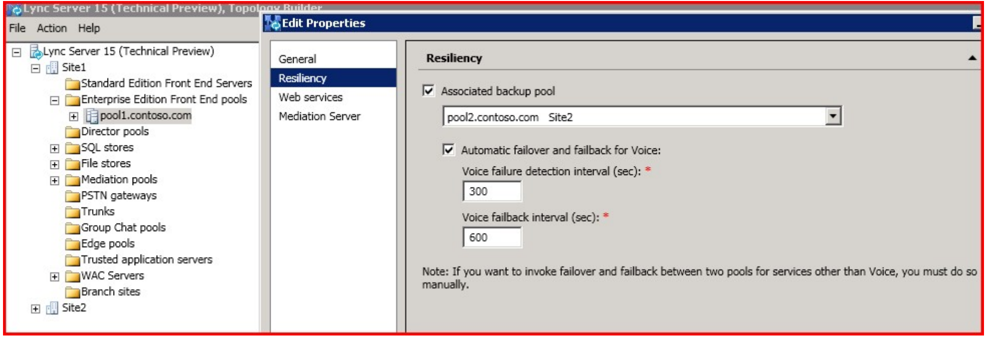
Deployment > Deploying Lync Server 2013 > Defining and Configuring the Topology >

Topic Last Modified: *2013-02-21*

You can easily deploy the disaster recovery topology of paired Front End pools using Topology Builder.

To deploy a pair of Front End pools

1. If the pools are new and not yet defined, use Topology Builder to create the pools.
2. In Topology Builder, right-click one of the two pools, and then click **Edit Properties**.
3. Click **Resiliency** in the left pane, and then select **Associated Backup Pool** in the right pane.
4. In the box below **Associated Backup Pool**, select the pool that you want to pair with this pool. Only existing pools that are not already paired with another pool will be available to select from.



☑ Associated backup pool

pool2.contoso.com Site2

☑ Automatic failover and failback for Voice:

Voice failure detection interval (sec): *

300

Voice failback interval (sec): *

600

Note: If you want to invoke failover and failback between two pools for services other than Voice, you must do so manually.

5. Select **Automatic failover and failback for Voice**, and then click **OK**.

   When you view the details about this pool, the associated pool now appears in the right pane under **Resiliency**.

6. Use Topology Builder to publish the topology.
7. If the two pools were not yet deployed, deploy them now and the configuration will be complete. You can skip the final two steps in this procedure.
   However, if the pools were already deployed before you defined the paired relationship, you must complete the following two final steps.
8. On every Front End Server in both pools, run the following:

   ```
   <system drive>\Program Files\Microsoft Lync Server 2013\Deployment\Boo
   ```

   This configures other services required for backup pairing to work correctly.
9. From a Lync Server Management Shell command prompt, run the following:

   ```
   Start-CsWindowsService -Name LYNCBACKUP
   ```

10. Force the user and conference data of both pools to be synchronized with each other, with the following cmdlets:

   ```
   Invoke-CsBackupServiceSync -PoolFqdn <Pool1 FQDN>
   ```

   ```
   Invoke-CsBackupServiceSync -PoolFqdn <Pool2 FQDN>
   ```

   Synchronizing the data may take some time. You can use the following cmdlets to check the status. Make sure that the status in both directions is in steady state.

   ```
   Get-CsBackupServiceStatus -PoolFqdn <Pool1 FQDN>
   ```

   ```
   Get-CsBackupServiceStatus -PoolFqdn <Pool2 FQDN>
   ```

Note:
The **Automatic failover and failback for Voice** option and the associated time intervals in Topology Builder apply only to the voice resiliency features that were introduced in Lync Server 2010. Selecting this option does not imply that the pool failover discussed in this document is automatic. Pool failover and failback always require an administrator to manually invoke the failover and failback cmdlets, respectively.

1.4.1.5.4 Deploying SQL Mirroring for Back End Server High Availability

Deploying SQL Mirroring for Back End Server High Availability

Deployment > Deploying Lync Server 2013 > Defining and Configuring the Topology >

Topic Last Modified: *2012-10-11*

To be able to deploy SQL mirroring, your servers must run a minimum of SQL Server 2008 R2. This version must run on all the involved servers: the primary, mirror, and the witness. For details, see http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=2083921.

In general, setting up SQL mirroring between the two Back End Servers with a witness requires the following:

- The primary server’s version of SQL Server must support SQL mirroring.
- The primary, mirror, and the witness (if deployed) must have the same version of SQL Server.
- The primary and the mirror must have the same edition of SQL Server. The witness may have a different edition.

For SQL best practices in terms of what SQL versions are supported for a Witness role, see "Database Mirroring Witness" in the MSDN Library at http://go.microsoft.com/fwlink/p/?LinkId=247345.

You use Topology Builder to deploy SQL mirroring. You select an option in Topology Builder to mirror the databases, and Topology Builder sets up the mirroring (including setting up a witness, if you want) when you publish the topology. Note that you set up or remove the witness at the same time you set up or remove the mirror. There is no separate command to deploy or remove only a witness.

To configure server mirroring, you must first set up SQL database permissions correctly. For details, see "Set Up Login Accounts for Database Mirroring or AlwaysOn Availability Groups (SQL Server)" at http://go.microsoft.com/fwlink/p/?LinkId=268454.

With SQL mirroring, database recovery mode is always set to **Full**, which means you must closely monitor transaction log size and back up transaction logs on a regular basis to avoid running out of disk space on the Back End Servers. The frequency of transaction log backups depends on the log growth rate, which in turn depends on database transactions incurred by user activities on the Front End pool. We recommend that you determine how much transaction log growth is expected for your Lync deployment workload so that you can do the planning accordingly. The following articles provide additional information on SQL backup and log management:

- Database recovery models: "Recovery Models (SQL Server)" at http://go.microsoft.com/fwlink/p/?LinkId=268446
- Backup overview: "Backup Overview (SQL Server)" at http://go.microsoft.com/fwlink/p/?LinkId=268449
- Backup transaction log: "Backup a Transaction Log (SQL Server)" at http://go.microsoft.com/fwlink/p/?LinkId=268452

With SQL mirroring, you can either configure the topology for mirroring when you create the pools, or after the pools are already created.

Important:

Using Topology Builder or cmdlets to set up and remove SQL mirroring is supported only when the primary, mirror, and witness (if desired) servers all belong to the same domain. If you want to set up SQL mirroring among servers in different domains, see your SQL Server documentation.

To configure SQL mirroring while creating a pool in Topology Builder

1. On the **Define the SQL Store** page, click **New** next to the **SQL store** box.
2. On the **Define new SQL Store** page, specify the primary store, select **This SQL instance is in mirroring relation**, specify the SQL mirroring port number (the default is 5022), and then click **OK**.
3. Back on the **Define the SQL store** page, select **Enable SQL Store mirroring**.
4. In the **Define new SQL Store** page, specify the SQL store to be used as the mirror. Select **This SQL instance is in mirroring relation**, specify the port number (the default is 5022), and then click **OK**.
5. If you want a witness for this mirror, do the following:
   5.a. Select **Use SQL mirroring witness to enable automatic failover**.
   5.b. In the **Define the SQL Store** page, select **Use SQL mirroring witness to enable automatic failover**, and specify the SQL store to be used as the witness.
   5.c. Specify the port number (the default is 7022) and click **OK**.
6. After you are done defining your Front End pool and all other roles in your topology, use Topology Builder to publish the topology. When the topology is published, if the Front End pool that hosts Central Management store has SQL mirroring enabled, you will see an option to create both primary and mirror SQL store databases.
   Click **Settings**, and type the path to use as the file share for the mirroring backup.

Click **OK** and then **Next** to create the databases and publish the topology. The mirroring and the witness (if specified) will be deployed.

You can use Topology Builder to edit the properties of an already existing pool to enable SQL mirroring.

To add SQL mirroring to an existing Front End pool in Topology Builder

1. In Topology Builder, right-click the pool and then click **Edit Properties**.
2. Select **Enable SQL Store Mirroring**, and then click **New** next to **Mirroring SQL Store**.
3. Specify the SQL store that you want to use as the mirror.
4. Select **This SQL instance is in mirroring relation**, specify the SQL mirroring port number the default port is 5022), and then click **OK**.
5. If you want to configure a witness, select **Use SQL mirroring witness to enable automatic failover**, and click **New**.
6. Specify the SQL store that you want to use as the witness.
7. Select **This SQL instance is in mirroring relation**, specify the SQL mirroring port number (the default port is 7022), and then click **OK**.
8. Click **OK**.
9. Publish the topology. When you do so, you will be prompted to install the database.

You must then install the database before going on to the next procedure.

You should keep the following in mind when setting up SQL mirroring:

- If a mirroring endpoint already exists, it will be reused using the ports defined there, and will ignore the ones you specify in the topology.
- Any port already allocated for other applications on the same server, including those for other SQL instances, should not be used for the installed SQL instances at hand. This implies that if you have more than one SQL instance installed on the same server, they must not use the same port for mirroring. For details, see the following articles:
  - "Specify a Server Network Address (Database Mirroring)" in the MSDN Library at http://go.microsoft.com/fwlink/p/?LinkId=247346
  - "The Database Mirroring Endpoint (SQL Server)" at http://go.microsoft.com/fwlink/p/?LinkId=247347

Using Lync Server Management Shell Cmdlets to Set Up SQL Mirroring

The easiest way to set up mirroring is by using Topology Builder, but you can also do so using cmdlets.

1. Open a Lync Server Management Shell window and run the following cmdlet:

   ```
   Install-CsMirrorDatabase [-ConfiguredDatabases] [-ForInstance] [-ForDe
   ```

   For example:

   ```
   Install-CsMirrorDatabase -ConfiguredDatabases -FileShare \\PRIMARYBE\c
   ```

   You will see the following:

   ```
   Database Name:rtcxds
           Data File:D:\CsData\BackendStore\rtc\DbPath\rtcxds.mdf
            Log File:D:\CsData\BackendStore\rtc\LogPath\rtcxds.ldf
         Primary SQL: e04-ocs.los_a.lsipt.local\rtc
             Account: LOS_A\e04-ocs$
          Mirror SQL: K16-ocs.los_a.lsipt.local\rtc
   ```

```
          Account: LOS_A\K16-ocs$
     Witness SQL : AB14-lct.los_a.lsipt.local\rtc
          Account: LOS_A\AB14-lct$
    Database Name:rtcshared
        Data File:D:\CsData\BackendStore\rtc\DbPath\rtcshared.mdf
         Log File:D:\CsData\BackendStore\rtc\LogPath\rtcshared.ldf
      Primary SQL: e04-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\e04-ocs$
       Mirror SQL: K16-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\K16-ocs$
     Witness SQL : AB14-lct.los_a.lsipt.local\rtc
          Account: LOS_A\AB14-lct$
    Database Name:rtcab
        Data File:D:\CsData\ABSStore\rtc\DbPath\rtcab.mdf
         Log File:D:\CsData\ABSStore\rtc\LogPath\rtcab.ldf
      Primary SQL: e04-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\e04-ocs$
       Mirror SQL: K16-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\K16-ocs$
     Witness SQL : AB14-lct.los_a.lsipt.local\rtc
          Account: LOS_A\AB14-lct$
    Database Name:rgsconfig
        Data File:D:\CsData\ApplicationStore\rtc\DbPath\rgsconfig.mdf
         Log File:D:\CsData\ApplicationStore\rtc\LogPath\rgsconfig.ldf
      Primary SQL: e04-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\e04-ocs$
       Mirror SQL: K16-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\K16-ocs$
     Witness SQL : AB14-lct.los_a.lsipt.local\rtc
          Account: LOS_A\AB14-lct$
    Database Name:rgsdyn
        Data File:D:\CsData\ApplicationStore\rtc\DbPath\rgsdyn.mdf
         Log File:D:\CsData\ApplicationStore\rtc\LogPath\rgsdyn.ldf
      Primary SQL: e04-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\e04-ocs$
       Mirror SQL: K16-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\K16-ocs$
     Witness SQL : AB14-lct.los_a.lsipt.local\rtc
          Account: LOS_A\AB14-lct$
    Database Name:cpsdyn
        Data File:D:\CsData\ApplicationStore\rtc\DbPath\cpsdyn.mdf
         Log File:D:\CsData\ApplicationStore\rtc\LogPath\cpsdyn.ldf
      Primary SQL: e04-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\e04-ocs$
       Mirror SQL: K16-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\K16-ocs$
     Witness SQL : AB14-lct.los_a.lsipt.local\rtc
          Account: LOS_A\AB14-lct$
    Database Name:xds
        Data File:D:\CsData\CentralMgmtStore\rtc\DbPath\xds.mdf
         Log File:D:\CsData\CentralMgmtStore\rtc\LogPath\xds.ldf
      Primary SQL: e04-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\e04-ocs$
       Mirror SQL: K16-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\K16-ocs$
     Witness SQL : AB14-lct.los_a.lsipt.local\rtc
          Account: LOS_A\AB14-lct$
    Database Name:lis
        Data File:D:\CsData\CentralMgmtStore\rtc\DbPath\lis.mdf
         Log File:D:\CsData\CentralMgmtStore\rtc\LogPath\lis.ldf
      Primary SQL: e04-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\e04-ocs$
       Mirror SQL: K16-ocs.los_a.lsipt.local\rtc
          Account: LOS_A\K16-ocs$
     Witness SQL : AB14-lct.los_a.lsipt.local\rtc
          Account: LOS_A\AB14-lct$
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
```

2. Verify the following:
   - Port 5022 is accessible through the firewall if Windows Firewall is enabled

in the primary SQL Server e04-ocs.los_a.lsipt.local\rtc.
- Port 5022 is accessible through the firewall if Windows Firewall is enabled in the mirror SQL Server K16-ocs.los_a.lsipt.local\rtc.
- Port 7022 is accessible through the firewall if Windows Firewall is enabled in the witness SQL Server AB14-lct.los_a.lsipt.local\rtc.
- Accounts running the SQL Servers on all primary and mirror SQL servers have read/write permission to the file share \\E04-OCS\csdatabackup
- Verify that the Windows Management Instrumentation (WMI) provider is running on all these servers. The cmdlet uses this provider to find the account information for SQL Server services running on all primary, mirror and witness servers.
- Verify that the account running this cmdlet has permission to create the folders for the data and log files for all the mirror servers.
- Note that the user account that the SQL instance uses to run must have read/write permission to the file share. If the file share is on a different server, and the SQL instance runs a local system account, you must grant file share permissions to the server that hosts the SQL instance.

3. Type A and press ENTER.
   The mirroring will be configured.

Install-CsMirrorDatabase installs the mirror and configures mirroring for all the databases that are present on the primary SQL store. If you want to configure mirroring for only specific databases, you can use the –DatabaseType option, or if you want to configure mirroring for all databases except for a few, you can use the -ExcludeDatabaseList option, along with a comma-separated list of database names to exclude.

For example, if you add the following option to **Install-CsMirrorDatabase**, all databases except rtcab and rtcxds will be mirrored.

```
-ExcludeDatabaseList rtcab,rtcxds
```

For example, if you add the following option to **Install-CsMirrorDatabase**, only the rtcab, rtcshared, and rtcxds databases will be mirrored.

```
-DatabaseType User
```

Removing or Changing SQL Mirroring

To remove the SQL mirroring of a pool in Topology Builder, you must first use a cmdlet to remove the mirror in SQL Server. You can then use Topology Builder to remove the mirror from the topology. To remove the mirror in SQL Server, use the following cmdlet:

```
Uninstall-CsMirrorDatabase -SqlServerFqdn <SQLServer FQDN> [-SqlInstanceName <SQL
```

For example, to remove mirroring and drop the databases for the User databases, type the following:

```
Uninstall-CsMirrorDatabase -SqlServerFqdn primaryBE.contoso.com -SqlInstanceName
```

The `-DropExistingDatabasesOnMirror` option causes the affected databases to be deleted from the mirror.

Then, to remove the mirror from the topology, do the following:

1. In Topology Builder, right-click the pool and click **Edit Properties**.
2. Uncheck **Enable SQL Store Mirroring** and click **OK**.
3. Publish the topology.

◆Important:

Whenever you make a change to a Back End Database mirroring relationship, you must

restart all the Front End Servers in the pool.
For a change in mirroring, (such as changing the location of a mirror), you must use Topology Builder to perform these three steps:

1. Remove mirroring from the old mirror server.
2. Add mirroring to the new mirror server.
3. Publish the topology.

Removing a Mirroring Witness

Use this procedure if you need to remove the witness from a Back End Server mirroring configuration.

1. In Topology Builder, right-click the pool and click **Edit Properties**.
2. Uncheck **Use SQL Server mirroring witness to enable automatic failover** and click **OK**.
3. Publish the topology.
   After publishing the topology, Topology Builder you will see a message that includes the following
   ```
   Run the Uninstall-CsMirrorDatabase cmdlet to remove databases that are
   ```
   However, do not follow that step, and do not type `Uninstall-CsMirrorDatabase` as that would uninstall the entire mirroring configuration.
4. To remove just the witness from the SQL Server configuration, follow the instructions in "Remove the Witness from a Database Mirroring Session (SQL Server)" at http://go.microsoft.com/fwlink/p/?LinkId=268456.

1.4.1.5.5 Edit or Configure Simple URLs

Edit or Configure Simple URLs

See Also

Deployment > Deploying Lync Server 2013 > Defining and Configuring the Topology >

Topic Last Modified: *2013-02-21*

This procedure does not require membership in a local administrator or privileged domain group. You should log on to a computer as a standard user.

Lync Server 2013 uses simple URLs to direct internal and external calls to services on the Front End Server or on the Director, if one has been deployed. For more information about simple URLs, see Planning for Simple URLs in the Planning documentation. You can select the format for your simple URLs from several options. For details about these options, see DNS Requirements for Simple URLs in the Planning documentation.

By default, simple URLs will be configured in the form of (for example, the dial-in simple URL): https://dialin.<SIP Domain>

⊟To configure simple URLs

1. In Topology Builder, right-click the **Lync Server 2013** node, and then click **Edit Properties**.
2. In the **Simple URLs** pane, select either **Phone access URLs:** (Dial-in) or **Meeting URLs:** (Meet) to edit, and then click **Edit URL**.
3. Update the URL to the value you want, and then click **OK** to save the edited URL. The example shown here has modified the Dial-in URL to https://pool01.contoso.net/dialin.
4. Edit the Meet URL by using the same steps, if necessary.

⊟To define the optional Admin simple URL

1. In Topology Builder, right-click the **Lync Server 2013** node, and then click **Edit Properties**.
2. In the **Administrative access URL** box, enter the simple URL you want for administrative access to Lync Server 2013 Control Panel, and then click **OK**.

> **Tip:**
> We recommend using the simplest possible URL for the Admin URL. The simplest option is **https://admin.**<*domain*>.

> **Important:**
> If you change a simple URL after initial deployment, you must be aware of what changes impact your Domain Name System (DNS) records and certificates for simple URLs. If the change impacts the base of a simple URL, then you must change the DNS records and certificates as well. For example, changing from https://lync.contoso.com/Meet to https://meet.contoso.com changes the base URL from lync.contoso.com to meet.contoso.com, so you would need to change the DNS records and certificates to refer to meet.contoso.com. If you changed the simple URL from https://lync.contoso.com/Meet to https://lync.contoso.com/Meetings, the base URL of lync.contoso.com stays the same, so no DNS or certificate changes are needed. Whenever you change a simple URL name, however, you must run the **Enable-CsComputer** cmdlet on each Director and Front End Server to register the change.

Concepts

Planning for Simple URLs

1.4.1.5.6 Select the Central Management Server

Select the Central Management Server

Deployment > Deploying Lync Server 2013 > Defining and Configuring the Topology >

Topic Last Modified: *2012-01-02*

Before you can define and configure your topology, you must first define the location to install the Central Management Server.

> **Note:**
> This will not take effect until you have published a topology in Topology Builder. To set the Central Management Server before the topology is created and published, run **Set-CSConfigurationStoreLocation**.

⊟To select the Central Management Server

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. Right-click the Lync Server 2013 node, and then click **Edit Properties**.
3. In the Central Management Server pane, select the Front End Server to install the Central Management Server on and then click **OK**.

1.4.1.6 Finalizing and Implementing the Topology Design

Finalizing and Implementing the Topology Design

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2012-06-19*

After you complete the preparation of your environment, you should be ready to finalize and implement your topology design. This includes using Topology Builder to publish your topology, which is required in order to install Lync Server 2013 server roles.

- Install Standard Edition Server Database
- Verify the Topology Design
- Publish the Topology

1.4.1.6.1 Install Standard Edition Server Database

Install Standard Edition Server Database

Deployment > Deploying Lync Server 2013 > Finalizing and Implementing the Topology Design >

Topic Last Modified: *2012-10-01*

Setting up a Standard Edition server as the only server in your infrastructure that homes users differs from other server installations in that there is a selection in the **Deployment Wizard** specifically for setting up the initial server.

⊟To install a Standard Edition server

1. Log on to the server where you are going to install Standard Edition server as a local administrator or a domain equivalent.
2. If you have not prepared Active Directory Domain Services (AD DS), then first perform those procedures. For details, see Preparing Active Directory Domain Services for Lync Server 2013.
3. In the Lync Server Deployment Wizard, click **Prepare first Standard Edition server**.
4. On the **Prepare single Standard Edition Server** page, click **Next**.
5. On the **Executing Commands** page, the SQL Server 2012 Express is installed as the Central Management store. Necessary firewall rules are created. When the installation of the database and prerequisite software is completed, click **Finish**.

   Note:
   The initial installation may take some time with no visible updates to the command output summary screen. This is due to the installation of the SQL Server Express. If you need to monitor the installation of the database, use Task Manager to monitor the setup.

6. On the Lync Server Deployment Wizard page, click **Install Topology Builder** if you have not previously installed the administrative tools. For details, see Install Lync Server Administrative Tools.
7. Confirm that there are green check marks next to "Prepare Active Directory," "Prepare first Standard Edition server," and "Install Topology Builder."

1.4.1.6.2 Verify the Topology Design

Verify the Topology Design

Deployment > Deploying Lync Server 2013 > Finalizing and Implementing the Topology Design >

Topic Last Modified: *2012-01-02*

Topology Builder automatically verifies the topology. Any topology error is identified as a validation error, indicated by the validation error icon next to the server role. It is important to also verify that the topology correctly represents the topology for your deployment.

⊟To verify the topology prior to publication

1. Check that all simple URLs are configured correctly.
2. Confirm that the SQL Server-based server is online and available to the computer where Topology Builder is installed, including any necessary firewall rules.
3. Confirm that the file share is available and has the proper permissions defined.
4. Confirm that the correct server roles that meet the deployment requirements are defined in the topology.
5. Verify that the servers exist in Active Directory Domain Services (AD DS). This will happen automatically if you have joined the servers to the domain.

When you have verified the topology and there are no validation errors, you should be ready to publish the topology. If there are validation errors, you must correct these before you can publish the topology. For details about publishing your topology, see Publish the Topology.

1.4.1.6.3 Publish the Topology

Publish the Topology

See Also

Deployment > Deploying Lync Server 2013 > Finalizing and Implementing the Topology Design >

Topic Last Modified: *2013-02-21*

To successfully publish, enable, or disable a topology when adding or removing a server role, you should be logged in as a user who is a member of the RTCUniversalServerAdmins and Domain Admins groups. It is also possible to delegate the proper administrator rights and permissions. For details, see Delegate Setup Permissions. For other configuration changes, only membership in the RTCUniversalServerAdmins group is required.

After you define your topology in Topology Builder, you must publish the topology to the Central Management store. The Central Management store provides a robust, schematized storage of the data needed to define, set up, maintain, administer, describe, and operate a Lync Server 2013 deployment. It also validates the data to help ensure configuration consistency. All changes to this configuration data happen at the Central Management store, eliminating "out-of-sync" issues. Read-only copies of the data are replicated to all servers in the topology, including Edge Servers.

Note:
For Enterprise Edition only: In order to publish the topology, the SQL Server-based Back End Server must be online and accessible with firewall exceptions in place. For details about specifying firewall exceptions, see Understanding Firewall Requirements for SQL Server. For details about configuring SQL Server, see Configure SQL Server for Lync Server 2013.

⊟To publish a topology

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. Select to open the topology from a local file. If you are on the computer where you defined the topology, this will be in the location where you saved it in earlier steps. Typically, this will be the Documents folder of the user who configured the topology.
3. Right-click the **Lync Server 2013** node, and then click **Publish Topology**.
4. On the **Publish the topology** page, click **Next**.

5. On the **Create databases** page, select the databases you want to publish.

> **Note:**
> If you don’t have the appropriate rights to create the databases, you can clear the check boxes next to those databases, and someone with appropriate rights can later create the databases. For details, see Deployment Permissions for SQL Server.

6. Optionally click **Advanced**. The Advanced SQL Server data file placement options let you select between the following options:
   - **Automatically determine database file location** – This option will determine the best operational performance based on the disk configuration on your SQL Server-based server by distributing the log and data files to the best location.
   - **Use SQL Server instance defaults** – This option puts log and data files onto the SQL Server-based server by using the instance settings. This option does not use the operational functionality of the SQL Server-based server to determine optimal locations for logs and data. The SQL Server administrator would typically move the log and data files to locations that are appropriate for the SQL Server-based server and organization management procedures.

   Click **OK**, and then click **Next**.
7. On the **Select Central Management Server** page, select a Front End pool.
8. Optionally click **Advanced**. The Advanced SQL Server data file placement options enables you to select between the following options:
   - **Automatically determine database file location** – This option will determine the best operational performance based on the disk configuration on your SQL Server-based server by distributing the log and data files to the best location.
   - **Use SQL Server instance defaults** – This option puts log and data files onto the SQL Server-based server by using the instance settings. This option does not use the operational functionality of the SQL Server-based server to determine optimal locations for logs and data. The SQL Server administrator would typically move the log and data files to locations that are appropriate for the SQL Server-based server and organization management procedures.

   Click **OK**.
9. Click **Next** to complete the publishing process.
10. When the publish process has completed, click **Finish**.

    When the topology has been published successfully, you can begin installing a local replica of the Central Management store on each server running Lync Server 2013 in your topology. We recommend that you begin with the first Front End pool.

Other Resources

Setting Up Front End Servers and Front End Pools

1.4.1.7 Setting Up Front End Servers and Front End Pools

Setting Up Front End Servers and Front End Pools

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2012-10-01*

This section guides you through installing Lync Server 2013 and setting up the server roles for the Standard Edition server and the Front End pool, including the Front End Servers and any server roles that are collocated with the Front End Servers. To install and set up server roles, you run the Lync Server Deployment Wizard on each computer on which you are installing a server role. You use the Deployment Wizard to complete all four deployment steps, including installing the Local Configuration store, installing the Front End Servers, configuring certificates, and starting services.

Note:

Before you can set up server roles, you must have successfully published a topology. For details about publishing a topology, see Finalizing and Implementing the Topology Design.

- Install the Local Configuration Store
- Install Lync Servers Server Components
- Configure Certificates for Servers
- Start Services on Servers
- Test the Pool Deployment
- Test the Standard Edition Server

1.4.1.7.1 Install the Local Configuration Store

Install the Local Configuration Store

Deployment > Deploying Lync Server 2013 > Setting Up Front End Servers and Front End Pools >

Topic Last Modified: *2013-02-25*

To successfully complete this procedure, you should be logged on to the server minimally as a local administrator and a domain user who has membership in at least the RTCUniversalReadOnlyAdmin group.

The first step of the Lync Server Deployment Wizard is to install the Local Configuration store. The Local Configuration store is SQL Server Express, which installs a local database that will retain a read-only copy of the Central Management store. The Central Management store is added to the existing SQL Server database installed on the Standard Edition server or SQL Server Express-based database.

Important:

If this is the first time that you have run Lync Server 2013 setup on this server, you will be prompted for a drive and path to install Lync Server 2013. If your organization requires that you locate Internet Information Services (IIS) and all Web Services on a drive other than the system drive, you can change the installation location path for the Lync Server files in the Setup dialog box. If you install the Setup files to this path, including OCSCore.msi, the rest of the Lync Server 2013 files will be deployed to this drive as well.

To install the Local Configuration store

1. From the installation media, browse to \setup\amd64\Setup.exe, and then click **OK**.
2. If you are prompted to install the Microsoft Visual C++ 2012 Redistributable, click **Yes**.
3. On the **Lync Server 2013 Installation Location** page, click **OK**.
4. On the **End User License Agreement** page, review the license terms, select **I accept the terms in the license agreement**, and then click **OK**. This step is required before you can continue.
5. On the Deployment Wizard page, click **Install or Update Lync Server System**.
6. On the **Lync Server 2013** page, next to **Step1: Install Local Configuration Store**, click **Run**.
7. On the **Local Server Configuration** page, make sure that the **Retrieve configuration automatically from the Central Management Store** option is

selected, and then click **Next**.

8. When the local server configuration installation is complete, click **Finish**.

1.4.1.7.2 Install Lync Servers Server Components

Install Lync Servers Server Components

Deployment > Deploying Lync Server 2013 > Setting Up Front End Servers and Front End Pools >

Topic Last Modified: *2012-04-16*

To successfully complete this procedure, you should be logged on to the server as minimally a local administrator and a domain user who has membership in at least the RTCUniversalReadOnlyAdmins group.

The Lync Server Deployment Wizard is used to install the components that are necessary for each server role and to activate the server. This procedure walks you through the steps of deploying the Standard Edition server or the Front End Server in your infrastructure.

⊟To install Lync Server components

1. If the Lync Server Deployment Wizard is not running, start it on the server that you are setting up.
2. Click **Install or Update Lync Server System**.
3. In the Deployment Wizard, verify that **Step 1: Install Local Configuration Store** has a green check mark, which means that the step has been completed. If it is not complete, install the Local Configuration store on the server. For details, see Install the Local Configuration Store.
4. To install the Lync Server 2013 components for the server, click **Run** next to **Step 2: Setup or Remove Lync Server Components**.
5. On the **Setup Lync Server Components** page, click **Next** to set up components as defined in the published topology.
6. The **Executing Commands** page displays a summary of commands and installation information as it proceeds. When finished, you can use the list to select a log to view, and then click **View Log**.
7. When Lync Server 2013 components setup completes, click **Finish**.

> **Note:**
> If you are prompted to restart the computer (which may be required if Windows Desktop Experience was not already installed on the computer), do so. When the computer is back up and running, repeat this procedure, starting from step three (run Step 2 in the Deployment Wizard again).

1.4.1.7.3 Configure Certificates for Servers

Configure Certificates for Servers

See Also

Deployment > Deploying Lync Server 2013 > Setting Up Front End Servers and Front End Pools >

Topic Last Modified: *2013-02-21*

To successfully complete this procedure you should be logged on as a user who is a member of the RTCUniversalServerAdmins group or have the correct permissions delegated. For details about delegating permissions, see Delegate Setup Permissions. Depending on your organization and requirements for requesting certificates, you may require other group memberships. Consult with the group that manages your public key infrastructure (PKI) certification authority (CA).

Note:

Lync Server 2013 includes support for SHA-256 certificates for connections from clients running the Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, or Windows XP operating systems, in addition to Lync Phone Edition. To support external access using SHA-256, the external certificate is issued by a public CA using SHA-256.

Each Standard Edition server or Front End Server requires up to four certificates: the oAuthTokenIssuer certificate, a default certificate, a web internal certificate, and a web external certificate. However, it is possible to request and assign a single default certificate with appropriate subject alternative name entries as well as the oAuthTokenIssuer certificate. For details about the certificate requirements, see Certificate Requirements for Internal Servers. For details about requesting, assigning and installing the oAuthTokenIssuer certificate, see Managing Server-to-Server Authentication (Oauth) and Partner Applications

Use the following procedure to request, assign, and install the Standard Edition server or Front End Server certificates. Repeat the procedure for each Front End Server.

Important:

The following procedure describes how to configure certificates from an internal enterprise PKI deployed by your organization and with offline request processing. For information about obtaining certificates from a public CA, see Certificate Requirements for Internal Servers in the Planning documentation. Also, this procedure describes how to request, assign, and install certificates during set up of the Front End Server. If you requested certificates in advance, as described in the Request Certificates in Advance (Optional) section of this Deployment documentation, or you do not use an internal enterprise PKI deployed in your organization to obtain certificates, you must modify this procedure as appropriate.

⊟To configure certificates for a Front End Server

1. In the Lync Server Deployment Wizard, click **Run** next to **Step 3: Request, Install or Assign Certificates**.
2. On the **Certificate Wizard** page, click **Request**.
3. On the **Certificate Request** page, click **Next**.
4. On the **Delayed or Immediate Requests** page, you can accept the default **Send the request immediately to an online certification authority** option by clicking **Next**. The internal CA with automatic online enrollment must be available if you select this option. If you choose the option to delay the request, you will be prompted for a name and location to save the certificate request file. The certificate request must be presented and processed by a CA either inside your organization, or by a public CA. You will then need to import the certificate response and assign it to the proper certificate role.
5. On the **Choose a Certificate Authority (CA)** page, select the **Select a CA from the list detected in your environment** option, and then select a known (through registration in Active Directory Domain Services (AD DS)) CA from the list. Or, select the **Specify another certification authority** option, enter the name of another CA in the box, and then click **Next**.
6. On the **Certificate Authority Account** page, you are prompted for credentials to request and process the certificate request at the CA. You should have determined if a user name and password is necessary to request a certificate in advance. Your CA administrator will have the required information and may have to assist you in this step. If you need to supply alternate credentials, select the check box, provide a user name and password in the text boxes, and then click **Next**.
7. On the **Specify Alternate Certificate Template** page, to use the default Web Server template, click **Next**.

Note:
If your organization has created a template for use as an alternative for the default Web server CA template, select the check box, and then enter the name of the alternate template. You will need the template name as defined by the CA administrator.

8. On the **Name and Security Settings** page, specify a **Friendly Name** that should allow you to identify the certificate and purpose. If you leave it blank, a name will be generated automatically. Set the **Bit length** of the key, or accept the default of 2048 bits. Select the **Mark the certificate's private key as exportable** if you determine that the certificate and private key needs to be moved or copied to other systems, and then click **Next**.

Note:
Lync Server 2013 has minimal requirements for an exportable private key. One such place is on the Edge Servers in a pool, where the Media Relay Authentication Service uses copies of the certificate, rather than individual certificates for each instance in the pool.

9. On the **Organization Information** page, optionally provide organization information, and then click **Next**.
10. On the **Geographical Information** page, optionally provide geographical information, and then click **Next**.
11. On the **Subject Name / Subject Alternate Names** page, review the subject alternative names that will be added, and then click **Next**.
12. On the **SIP Domain setting** page, select the **SIP Domain**, and then click **Next**.
13. On the **Configure Additional Subject Alternate Names** page, add any additional required subject alternative names, including any that might be required for additional SIP domains in the future, and then click **Next**.
14. On the **Certificate Request Summary** page, review the information in the summary. If the information is correct, click **Next**. If you need to correct or modify a setting, click **Back** to the proper page to make the correction or modification.
15. On the **Executing Commands** page, click **Next**.
16. On the **Online Certificate Request Status** page, review the information returned. You should note that the certificate was issued and installed into the local certificate store. If it is reported as having been issued and installed, but is not valid, make sure that the CA root certificate has been installed in the server's Trusted Root CA store. Refer to your CA documentation on how to retrieve a Trusted Root CA certificate. If you need to view the retrieved certificate, click **View Certificate Details**. By default, the check box for **Assign the certificate to Lync Server certificate usages** is checked. If you want to manually assign the certificate, clear the check box, and then click **Finish**.
17. If you cleared the check box for **Assign the certificate to Lync Server certificate usages** on the previous page, you will be presented with the **Certificate Assignment** page. Click **Next**.
18. On the **Certificate Store** page, select the certificate that you requested. If you want to view the certificate, click **View Certificate Details**, and then click **Next** to continue.

Note:
If the **Online Certificate Request Status** page reported an issue with the certificate, such as the certificate not being valid, viewing the actual certificate can assist in resolving the issue. Two specific issues that can cause a certificate to not be valid is the previously mentioned missing Trusted Root CA certificate, and a missing private key that is associated with the certificate. Refer to your CA documentation to resolve these two issues.

19. On the **Certificate Assignment Summary** page, review the information presented to make sure that this is the certificate that should be assigned, and then click **Next**.

20. On the **Executing Commands** page, review the output of the command. Click **View Log** if you want to review the assignment process or if there was an error or warning issued. When you are finished with your review, click **Finish**.
21. On the **Certificate Wizard** page, verify that the **Status** of the certificate is “Assigned,” and then click **Close**.

Other Resources

Certificate Infrastructure Requirements

1.4.1.7.4 Start Services on Servers

Start Services on Servers

Deployment > Deploying Lync Server 2013 > Setting Up Front End Servers and Front End Pools >

Topic Last Modified: *2012-10-01*

To successfully complete this procedure you should be logged in as a user who is a member of the RTCUniversalServerAdmins group or have the correct permissions delegated. For details about delegating permissions, see **Delegate Setup Permissions**.

⚠**Warning:**
For Lync Server 2013, KB2713435-x64-RP.msu must be installed on Windows Server 2012 computers before some Lync Server services can be restarted.

After you install the Local Configuration store on your servers, install the Lync Server 2013 components, and configure certificates on a Front End Server or Front End Server, you must start the Lync Server 2013 services on the server. Use the following procedure to start services on each Front End Server in your deployment.

⊟To start services on a Standard Edition or Front End Server

1. In the Lync Server Deployment Wizard, on the **Lync Server 2013** page, click **Run** next to **Step 4: Start Services**.
2. On the **Start Services** page, click **Next** to start the Lync Server services on the server.
3. On the **Executing Commands** page, after all services have started successfully, click **Finish**.

◆**Important:**
The command to start the services on the server is a best effort method to report that the services have in fact started. It might not reflect the actual state of the service. We recommend that you use the step **Service Status (Optional)** immediately following **Start Services** to open the Microsoft Management Console (MMC) and confirm that the services have started successfully. If any Lync Server service has not started, you can right-click that service in the MMC, and then click **Start**.

1.4.1.7.5 Configure an Existing Central Management Server

Configure an Existing Central Management Server

Deployment > Deploying Lync Server 2013 > Setting Up Front End Servers and Front End Pools >

Topic Last Modified: *2013-02-21*

If you reuse a Central Management Server from an existing Lync Server 2013 deployment, you must run the procedure described below to make sure that Lync Server Control Panel and Windows PowerShell function correctly.

⊟To configure an existing Central Management Server

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Use the **Update-CsAdminRole** cmdlet to update the role-based access control (RBAC) roles stored in the Central Management Server.

   Note:
   No output is expected unless there is an error.

1.4.1.7.6 Test the Pool Deployment

Test the Pool Deployment

See Also

Deployment > Deploying Lync Server 2013 > Setting Up Front End Servers and Front End Pools >

Topic Last Modified: *2012-10-01*

The following procedure describes how to test the deployment of the Front End pool.

⊟To test the pool deployment

1. Use Active Directory Computers and Users to add the Active Directory user object of the administrator role for the Lync Server 2013 deployment (on which Lync Server 2013 Control Panel is installed) to the **CSAdministrator** group.

   Important:
   If you do not add the appropriate users and groups to the CsAdministors group, you will receive an error when opening Lync Server Control Panel, which states that "Unauthorized: Access is denied due to a role-based access control (RBAC) authorization failure."
2. If the user object is currently logged on, log off and then log on again to register the new group assignment.

   Note:
   The user account cannot be the local administrator of any server running Lync Server 2013.
3. Use the administrative account to log on to the computer where Lync Server Control Panel is installed.
4. Start Lync Server Control Panel, and then provide credentials, if prompted. Lync Server Control Panel displays deployment information.
5. In the left navigation bar, click **Topology**, and then confirm that the service status shows a computer with a green arrow and that a green check mark for replication status is next to each Lync Server server role that has been deployed and brought online.
6. In the left navigation bar, click **Users**, and then click **Enable users**.
7. On the **New Lync Server User** page, click **Add**.
8. To define search parameters for the objects you want to find, on the **Select from Active Directory** page, you can select **Search**, and then optionally click **Add Filter**. You can also select **LDAP search** and enter an LDAP expression to filter or limit the objects that will be returned. After you have decided on your Search options, clink **Find**.
9. In the Search results pane, select all the objects for this search session, and then click **OK**.
10. On the **New Lync Server User** page, the object or objects you selected are

in the **Users** display. In the **Assign users to a pool** list, select the server where the objects should be homed.

Following are a number of options for configuring the objects.

- **Generate user's SIP URI**
- **Telephony**
- **Line URI**
- **Conferencing policy**
- **Client version policy**
- **PIN policy**
- **External access policy**
- **Archiving policy**
- **Location policy**
- **Client policy**

For the purposes of testing the basic functionality, select the option you prefer for the **Generate user's SIP URI** setting (the other options in the configuration will use default settings), and then click **Enable**.

11. A summary page is displayed that shows a check mark in the **Enabled** column to indicate that the objects are now ready for use. The **SIP address** column displays the address you need for the user sign-in configuration.
12. Log one user on to a computer that is joined to the domain, and another user on to another computer in the domain.
13. Install Lync Server 2013 on each of the two client computers, and then verify that both users can sign in to Lync Server 2013 and can send instant messages to each other.

Concepts

Deploying Clients and Devices

1.4.1.7.7 Test the Standard Edition Server

Test the Standard Edition Server

See Also

Deployment > Deploying Lync Server 2013 > Setting Up Front End Servers and Front End Pools >

Topic Last Modified: *2012-10-01*

The following procedure describes how to test the deployment of a Standard Edition server.

⊟To test the deployment of a Standard Edition Server

1. Use Active Directory Computers and Users to add the Active Directory user object of the administrator role for the Lync Server 2013 deployment (on which Lync Server Control Panel is installed) to the **CSAdministrator** group.
2. If the user object is currently logged on, log off and then log on again to register the new group assignment.

> **Note:**
> The user account cannot be the local administrator of the server running Lync Server 2013, Standard Edition. If you do not add the appropriate users and groups to the CsAdministors group, you will receive an error when opening Lync Server 2013 Control Panel, which states that "Unauthorized: Access is denied due to a role-based access control (RBAC) authorization failure."

3. Use the administrative account to log on to the computer where Lync Server Control Panel is installed.
4. Start Lync Server Control Panel and provide credentials, if prompted. Lync Server 2013 Control Panel displays deployment information.

5. In the left navigation bar, click **Topology**, and then confirm that the service status is a computer icon with a green arrow and there is a green check mark next to each Lync Server server role that has been deployed and brought online.
6. In the left navigation bar, click **Users**, and then enable the two users for Lync Server 2013.
7. Log one user on to a computer that is joined to the domain, and the other user on to another computer in the domain.
8. Install Lync Server 2013 on each of the two client computers, and then verify that both users can sign in to Lync Server 2013 and can send instant messages to each other.

Concepts

Deploying Clients and Devices

1.4.1.8 Deploying Lync Server 2013 Standard Edition into an Existing Lync Server 2013 Enterprise

Deploying Lync Server 2013 Standard Edition into an Existing Lync Server 2013 Enterprise

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2012-10-01*

Deploying a Standard Edition server into an existing Enterprise Edition deployment is similar to deploying additional server roles. A Standard Edition server might be deployed to another site, allowing for users in that site to be homed on the Standard Edition server rather than the Front End pool across a wide area network (WAN). The procedures for installing the new site and servers in that site are already defined in other sections of the Deploying Lync Server 2013 documentation.

To define a new site

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In the console tree, right-click **Lync Server 2013**, and then click **New Central Site**.
3. On the **Identify the site** page, give a name to the site and optionally enter a description.
4. Follow the procedures for defining the rest of the site topology. For details, see Defining and Configuring the Topology.
5. Publish the updated topology. For details, see Publish the Topology.
6. Set up and install a Standard Edition server.

Caution:

If you have deployed an environment with only a Standard Edition server, you would have begun the setup process from the Lync Server Deployment Wizard by using the **Prepare first Standard Edition server** link to install the initial database files to the new Standard Edition server. **Do not** follow that process when installing a Standard Edition server into an existing Lync Server 2013 deployment.

1.4.1.9 Adding Server Roles

Adding Server Roles

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2012-06-19*

After you have your initial deployment up and running, you can add additional server roles for Lync Server 2013, such as a Director or a stand-alone Mediation Server.

Note:
Before undertaking the task of installing additional server roles, see the Planning topics related to each role.

- Configuring Dial-in Conferencing

Additionally, for details about the deployment of your client software and devices that can be used with Lync Server 2013, see Deploying Clients and Devices.

1.4.1.10 Setting Up Kerberos Authentication

Setting Up Kerberos Authentication

Microsoft Lync Server 2013 > Deployment > Deploying Lync Server 2013 >

Topic Last Modified: *2013-02-21*

Lync Server 2013 supports NTLM and Kerberos authentication for Web Services. Office Communications Server 2007 and Office Communications Server 2007 R2 used the default RTCComponentService and RTCService as the user accounts to run the Web Services application pools, allowing for a service principal name (SPN) to be assigned to the user accounts and to act as the authentication principal. Lync Server uses NetworkService to run Web Services and NetworkService cannot have SPNs assigned to it.

To solve the issue of not having Active Directory objects to hold the SPNs, Lync Server Control Panel can use computer account objects for this purpose. The computer account objects can hold the SPNs and are not subject to password expiration, which was an issue with using user accounts in previous versions.

You use Windows PowerShell cmdlets to configure the computer objects to provide Kerberos authentication.

- Prerequisites for Enabling Kerberos Authentication
- Create a Kerberos Authentication Account
- Assign a Kerberos Authentication Account to a Site
- Setting Up Kerberos Authentication Account Passwords
- Add Kerberos Authentication to Other Sites
- Remove Kerberos Authentication from a Site
- Testing and Reporting the Status and Assignment of Kerberos Authentication

1.4.1.10.1 Prerequisites for Enabling Kerberos Authentication

Prerequisites for Enabling Kerberos Authentication

Deployment > Deploying Lync Server 2013 > Setting Up Kerberos Authentication >

Topic Last Modified: *2013-02-21*

Before enabling Kerberos authentication, make sure that you complete all prerequisite configuration and infrastructure preparations:

- Active Directory schema is extended for Lync Server 2013.
- Active Directory forest preparation is completed for Lync Server 2013.
- Active Directory domain preparation is completed for Lync Server 2013.
- Central Management store is successfully installed and available.
- The topology has been created and published by using Topology Builder.
- Servers and roles that require Web Services have been defined and deployed, including Front End Servers, Standard Edition servers, and Directors.
- Internet Information Services (IIS) is configured and deployed with the recommended role services to support Web Services in Lync Server 2013.

After the prerequisites have been met, you should be ready to create one or more accounts for Web Services to use for Kerberos authentication for your deployment. At a minimum, you need to create one Kerberos authentication account for each deployment. However, you can create an account for each site to provide local Kerberos authentication at the site. You can only specify one Kerberos authentication account per site.

1.4.1.10.2 Create a Kerberos Authentication Account

Create a Kerberos Authentication Account

Deployment > Deploying Lync Server 2013 > Setting Up Kerberos Authentication >

Topic Last Modified: *2012-01-02*

To successfully complete this procedure, you should be logged on to the server or domain minimally as a member of the Domain Admins group.

You can create Kerberos authentication accounts for each site or you can create a single Kerberos authentication account and use it for all sites. You use Windows PowerShell cmdlets to create and manage the accounts, including identifying the accounts assigned to each site. Topology Builder and the Lync Server 2013 Control Panel do not display Kerberos authentication accounts. Use the following procedure to create one or more user accounts to be used for Kerberos authentication.

⊟To create a Kerberos account

1. As a member of the Domain Admins group, log on to a computer in the domain running Lync Server 2013 or on to a computer where the administrative tools are installed.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. From the command line, run the following command:

   ```
   New-CsKerberosAccount -UserAccount "Domain\UserAccount" -ContainerDN "
   ```

   For example:

   ```
   New-CsKerberosAccount -UserAccount "Contoso\KerbAuth" -ContainerDN "CN
   ```

4. Confirm that the Computer object was created by opening Active Directory User and Computers, expand the **Users** container, and then confirm that the Computer object for the user account is in the container.

1.4.1.10.3 Assign a Kerberos Authentication Account to a Site

Assign a Kerberos Authentication Account to a Site

Deployment > Deploying Lync Server 2013 > Setting Up Kerberos Authentication >

Topic Last Modified: *2012-01-16*

To successfully complete this procedure you should be logged on as a user who is a member of the RTCUniversalServerAdmins group.

After creating the Kerberos account, you must assign it to a site. This is a Lync Server 2013 site, not an Active Directory site. You can create multiple Kerberos authentication accounts per deployment, but you can assign only one account to a site. Use the following procedure to assign a previously created Kerberos authentication account to a site. For details about creating the Kerberos account, see Create a Kerberos Authentication Account.

⊟To assign a Kerberos authentication account to a site

1. As a member of the RTCUniversalServerAdmins group, log on to a computer in the domain running Lync Server 2013 or on to a computer where the administrative tools are installed.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. From the command line, run the following two commands:

```
New-CsKerberosAccountAssignment -UserAccount "Domain\UserAccount" -Ide
```

```
Enable-CsTopology
```

For example:

```
New-CsKerberosAccountAssignment -UserAccount "contoso\kerbauth" -Ident
```

```
Enable-CsTopology
```

Note:
You must specify the UserAccount parameter by using the Domain\User format. The User@Domain.extension format is not supported for referring to the computer objects created for Kerberos authentication purposes.

Important:
After making any changes to Kerberos authentication, such as adding an account or removing an account, you must run **Enable-CsTopology** from the Lync Server Management Shell command prompt.

1.4.1.10.4 Setting Up Kerberos Authentication Account Passwords

Setting Up Kerberos Authentication Account Passwords

Deployment > Deploying Lync Server 2013 > Setting Up Kerberos Authentication >

Topic Last Modified: *2010-11-03*

After you create the computer object for the Kerberos authentication account, you can set up the password for the account. You run the Windows PowerShell cmdlet for setting the Kerberos account password on one server. You can set the password on the object that you created for the Kerberos authentication. The password can be set to a known value, but by default is a random password. The password is available to all Kerberos authentication sources that use the account. You use Windows PowerShell cmdlets to set up and manage Kerberos account passwords.

Note:
The Kerberos account object is a computer object, but uses the UserAccount parameter for operations in the Windows PowerShell cmdlets that are referenced. Note that this is not a mistake, but the intended behavior of the cmdlet when used with the Kerberos account creation and maintenance.

- Set a Kerberos Authentication Account Password on a Server
- Synchronize a Kerberos Authentication Account Password to IIS

1.4.1.10.4.1 Set a Kerberos Authentication Account Password on a Server

Set a Kerberos Authentication Account Password on a Server

Deploying Lync Server 2013 > Setting Up Kerberos Authentication > Setting Up Kerberos Authentication Account Passwords >

Topic Last Modified: *2012-01-16*

To successfully complete this procedure you should be logged on as a user who is a member of the RTCUniversalServerAdmins group.

You must set up a password on the Kerberos account for each site that has Front End Servers, Standard Edition servers, and Directors. You can set up the password by running the **Set-CsKerberosAccountPassword** Windows PowerShell cmdlet on one server in the site (for example, one Front End Server). For each site, you must run the **Set-CsKerberosAccountPassword** cmdlet. The cmdlet configures Internet Information Services (IIS) for the Web Services service, and then sets the password on the computer account in Active Directory Domain Services (AD DS). An alternate method, based on which parameter is used with the cmdlet, configures IIS on one server while using another server that has been configured as the source of the Kerberos account password.

When you use the **Set-CsKerberosAccountPassword** cmdlet to set a password, Kerberos sets the password to a randomly generated string. This cmdlet contacts all IIS instances in all Lync Server 2013 central sites to which this account is assigned.

⊟To set a password for a Kerberos authentication account

1. Log on to any domain computer with Lync Server Management Shell installed as a member of the RTCUniversalServerAdmins group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. From the command line, run the following two commands:

```
Set-CsKerberosAccountPassword -UserAccount "Domain\UserAccount"
```

For example:

```
Set-CsKerberosAccountPassword -UserAccount "contoso\KerbAuth"
```

Note:
You must specify the UserAccount parameter by using the Domain\User format. The User@Domain.extension format is not supported for referencing the computer objects created for Kerberos authentication purposes.

Important:

After making any changes to Kerberos authentication, such as adding an account or removing an account, you must run **Enable-CsTopology** from the Lync Server Management Shell command prompt.

1.4.1.10.4.2 Synchronize a Kerberos Authentication Account Password to IIS

Synchronize a Kerberos Authentication Account Password to IIS

Deploying Lync Server 2013 > Setting Up Kerberos Authentication > Setting Up Kerberos Authentication Account Passwords >

Topic Last Modified: *2010-11-08*

To successfully complete this procedure you should be logged on as a user who is a member of the RTCUniversalServerAdmins group.

In a site, Front End Servers, Standard Edition servers, and Directors can use a Kerberos authentication account for purposes of authenticating requests to the Web Services service. This procedure locates each server running Web Services in a site that has been assigned a Kerberos account and updates the Internet Information Services (IIS) configuration settings to use the Kerberos account. For details, see Set a Kerberos Authentication Account Password on a Server.

⊟To set and configure a Kerberos authentication account password

1. Log on to a source computer (such as fe01.contoso.com) as a member of RTCUniversalServerAdmins group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. From the Lync Server Management Shell command line, run the following two commands:

   ```
   Set-CsKerberosAccountPassword -FromComputer SourceComputer -ToComputer
   ```

   For example:

   ```
   Set-CsKerberosAccountPassword -FromComputer fe01.contoso.com -ToComput
   ```

◆Important:

The name of the source computer and destination computer must be a fully qualified domain (FQDN) name of the server. You cannot use the pool FQDN unless the pool name is the same as the name of the computer that you are using as a source computer or destination computer.

◆Important:

After making any changes to Kerberos authentication, such as adding an account or removing an account, you must run **Enable-CsTopology** from the Lync Server Management Shell command prompt.

1.4.1.10.5 Add Kerberos Authentication to Other Sites

Add Kerberos Authentication to Other Sites

Deployment > Deploying Lync Server 2013 > Setting Up Kerberos Authentication >

Topic Last Modified: *2010-11-03*

If you need to add sites to an existing deployment that you have configured for Kerberos authentication, you can use an existing Kerberos authentication account for the new site or create a new account. For details about creating a new account for a site, see Create a Kerberos Authentication Account. For details about using the same account for a new site by assigning an existing account to the site, see Assign a Kerberos Authentication Account to a Site.

1.4.1.10.6 Remove Kerberos Authentication from a Site

Remove Kerberos Authentication from a Site

Deployment > Deploying Lync Server 2013 > Setting Up Kerberos Authentication >

Topic Last Modified: *2012-01-16*

To successfully complete this procedure you should be logged on as a user who is a member of the RTCUniversalServerAdmins group.

If you need to remove Kerberos authentication from a site or retire a site, you must remove the Kerberos authentication account assignment from the site by using the **Remove-CsKerberosAccountAssignment** cmdlet. Use the following procedure to remove the Kerberos authentication account assignment, which removes the assignment from all computers in the site.

⚠**Warning:**

If you are permanently retiring the Kerberos-enabled account, you should use Active Directory Users and Computers to delete it from Active Directory Domain Services (AD DS) after you have removed the assignment. If you plan to use the object in the future, you might want to keep the Active Directory object.

⊟To remove Kerberos authentication from a site

1. As a member of the RTCUniversalServerAdmins group, log on to a computer in the domain running Lync Server 2013 or on to a computer where the administrative tools are installed.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. From the command line, run the following two commands:

```
Remove-CsKerberosAccountAssignment -Identity "site:SiteName"
```

```
Enable-CsTopology
```

For example:

```
Remove-CsKerberosAccountAssignment -Identity "site:Redmond"
```

```
Enable-CsTopology
```

Important:

After making any changes to Kerberos authentication, such as adding an account or removing an account, you must run **Enable-CsTopology** from the Lync Server Management Shell command prompt.

1.4.1.10.7 Testing and Reporting the Status and Assignment of Kerberos Authentication

Testing and Reporting the Status and Assignment of Kerberos Authentication

Deployment > Deploying Lync Server 2013 > Setting Up Kerberos Authentication >

Topic Last Modified: *2010-11-03*

If you need to test the Kerberos assignments or determine the status of Kerberos authentication, you can use Windows PowerShell cmdlets.

- Test and Report Functional Readiness for Kerberos Authenticaion
- Report Kerberos Account Assignments

1.4.1.10.7.1 Test and Report Functional Readiness for Kerberos Authenticaion

Test and Report Functional Readiness for Kerberos Authenticaion

Deploying Lync Server 2013 > Setting Up Kerberos Authentication > Testing and Reporting the Status and Assignment of Kerberos Authentication >

Topic Last Modified: *2012-01-16*

To successfully complete this procedure you should be logged on as a user who is a member of the RTCUniversalServerAdmins group.

You can use the **Test-CsKerberosAccountAssignment** Windows PowerShell cmdlet to test and report the functional readiness of a site assignment for Kerberos authentication. This command queries the site specified in the required Identity parameter. The optional Report parameter causes the cmdlet to write an HTML report to C:\Logs on the computer on which the command is run. The optional Verbose parameter reports activity information to the screen.

To test and report functional readiness for Kerberos authentication for a site

1. As a member of the RTCUniversalServerAdmins group, log on to a computer in the domain running Lync Server 2013 or on to the computer where the administrative tools are installed.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. From the command line, run the following command:

   ```
   Test-CsKerberosAccountAssignment -Identity "site:SiteName" -Report "c:
   ```

   For example:

   ```
   Test-CsKerberosAccountAssignment -Identity "site:Redmond" -Report "c:\
   ```

1.4.1.10.7.2 Report Kerberos Account Assignments

Report Kerberos Account Assignments

Deploying Lync Server 2013 > Setting Up Kerberos Authentication > Testing and Reporting the Status and Assignment of Kerberos Authentication >

Topic Last Modified: *2012-01-16*

To successfully complete this procedure you should be logged on as a user who is a member of the RTCUniversalServerAdmins group.

You can use the **Get-CsKerberosAccountAssignment** cmdlet to query information about the Kerberos authentication account assignments and report information about the current assignments in your deployment.

⊟To query Kerberos authentication account assignments for a site

1. As a member of the RTCUniversalServerAdmins group, log on to a computer in the domain running Lync Server 2013 or on to a computer where the administrative tools are installed.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. From the command line, run one of the following commands:
   - To query all Kerberos authentication account assignments in your organization and return assignment information about each of them, run the cmdlet without any parameters:

     ```
     Get-CsKerberosAccountAssignment
     ```

   - To query all Kerberos authentication account assignments in your deployment and return site assignment information about each of them, run the cmdlet with the Identity parameter:

     ```
     Get-CsKerberosAccountAssignment -Identity "site:SiteName"
     ```

     For example:

     ```
     Get-CsKerberosAccountAssignment -Identity "site:Redmond"
     ```

   - To query all Kerberos authentication account assignments in a single site and return assignment information about each of them, run the cmdlet with the Filter parameter:

     ```
     Get-CsKerberosAccountAssignment -Filter "SiteName"
     ```

     For example:

     ```
     Get-CsKerberosAccountAssignment -Filter "*Redmond"
     ```

     Note:
     Specifying *SiteName for the Filter parameter returns information about all sites that contain the specified site name anywhere in the site identifier (for example, all sites that contain the string Redmond in the site identifier).

1.4.2 Deploying External User Access

Deploying External User Access

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-09-20*

Deploying edge components for Microsoft Lync Server 2013 makes it possible for external users who are not logged into your organization’s internal network, including authenticated and anonymous remote users, federated partners (including XMPP partners), mobile clients and users of public instant messaging (IM) services, to communicate with other users in your organization using Lync Server. The deployment and configuration processes for Lync Server 2013 are not significantly different from Lync Server 2010. The tools for installation and administration are much the same as in Lync Server 2010.

> **Important:**
> Microsoft Lync Server 2013 Edge Server installation and configuration can be a complex process requiring a potentially significant amount of planning and coordination with your internal teams, including – but not limited to – security, networking, firewall, domain name system (DNS), load balancer, and public key infrastructure (PKI) considerations. It is strongly recommended that you review and use the planning process and documentation provided before deploying your external access components. This will assist in limiting the number and frequency of undesired changes and problems as you proceed through the deployment process. For information on planning you external user access, see Planning for External User Access.

- Deployment Checklist for External User Access
- System Requirements for External User Access Components
- Preparing for Installation of Servers in the Perimeter Network
- Building an Edge and Director Topology
- Setting Up the Director (optional)
- Setting Up Edge Servers
- Setting Up Reverse Proxy Servers
- Configuring Support for External User Access
- Configuring SIP Federation, XMPP Federation and Public Instant Messaging
- Deploying Mobility
- Verifying Your Edge Deployment

1.4.2.1 Deployment Checklist for External User Access

Deployment Checklist for External User Access

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2013-01-11*

Before you deploy your perimeter network and implement support for external users, you must already have deployed your Microsoft Lync Server 2013 internal servers, including a Front End pool or a Standard Edition server. If you plan to deploy the optional Directors in your internal network, you should also deploy them prior to deploying Edge Servers. For details about the Director deployment process, see Scenarios for the Director in the Planning documentation.

Microsoft Lync Server 2013 includes tools to facilitate planning and deployment of both internal servers and Edge Servers. After the topology is completed, publish the resulting topology definition to your production environment. To do this, you must be a member of the **Domain Admins** group and the **RTCUniversalServerAdmins** group.

- **Planning Tool** Office Communications Server 2007 R2 included a Planning Tool and an Edge Planning Tool that you could use to help guide topology design. In Lync Server 2010, these two tools were combined into a single Planning Tool that has additional features and functionality, such as collecting planned user count, voice requirements, external user access types, and federation options. Additionally, you can plan your infrastructure’s network parameters, such as IP addresses, load balancer types and other perimeter network considerations.
- **Topology Builder** Lync Server 2013 Topology Builder helps you define your topology and components. Topology Builder is essential to deploying servers running Lync Server 2013. Topology Builder publishes the results to a Central Management store that is used to configure all of the servers running Lync Server 2013 in your organization. You cannot install Lync Server 2013 on servers without using Topology Builder.

If you designed your edge topology during your planning process, including running

Topology Builder to define your edge topology, you can use those results to start your Edge Server deployment. If you did not finish building your edge topology earlier or you want to change the information you previously specified, you must finish running Topology Builder before proceeding with other deployment steps. For details about how to build your topology, see Scenarios for External User Access.

For details about the Planning Tool and Topology Builder, see Beginning the Planning Process in the Planning documentation.

The following table provides an overview of the Edge Server deployment process. To review the planning decisions that must be made before deploying external user access, see Scenarios for External User Access.

⚠**Warning:**

The information in the following table focuses on a new deployment. If you have deployed Edge Servers in an Lync Server 2013, Office Communications Server 2007 R2 or Office Communications Server 2007 environment, see the Migration for details about migrating to Lync Server 2013. Migration is not supported from any version prior to Office Communications Server 2007 R2, including Office Communications Server 2007, Live Communications Server 2005, and Live Communications Server 2003.

To enhance Edge Server performance and security, and to facilitate deployment, apply the following best practices when you deploy your perimeter network and Edge Servers:

- Deploy Edge Servers only after you have tested and verified operation of Lync Server 2013 inside your organization.
- We recommend that you deploy Edge Servers in a workgroup rather than a domain. Doing so simplifies installation and keeps Active Directory Domain Services (AD DS) out of the perimeter network. Locating AD DS in the perimeter network can present a significant security risk.
- Joining an Edge Server to a domain located entirely in the perimeter network is supported but not recommended. An Edge Server as part of the internal domain violates trusted network boundaries, where the Internet is least trusted, perimeter network is more trusted than the Internet, and the internal network is most trusted. An Edge server as a member of the domain is automatically a part of the most trusted network, but resides in a less trusted network (the perimeter).

Deployment Process for Edge Servers

Phase	**Steps**	**Permissions**	**Documentation**
Create the appropriate edge topology and determine the appropriate components.	• Run Topology Builder to configure Edge Server settings and create and publish the topology, and then use Lync Server Management Shell to export the topology configuration file.	**Domain Admins** group and **RTCUniversalServerAdmins** or **CsAdmins** group 📝**Note:** You can define a topology using an account that is a member of the local users group, but publishing a	Building an Edge and Director Topology in the Deployment documentation

		topology requires an account that is a member of the **Domain Admins** group and the **RTCUniversalServerAdmins** group.	
Prepare for setup.	1. Ensure that system prerequisites are met. 2. Configure IP addresses (IPv4 and IPv6, if used) for both internal and public facing network interfaces on each Edge Server. 3. Configure internal and external DNS records (host A and AAAA for IPv4 and IPv6), including configuring the DNS suffix on the computer to be deployed as an Edge Server. 4. (Optional) Create and install public certificates. The time required to obtain certificates depends on which certification authority (CA) issues the certificate. If you do not perform this step at this point, you must do it during Edge Server installation. The Edge Server services cannot be started until certificates are obtained and installed. 5. Provision support for public IM connectivity, if your deployment is to support communications with Windows Live, AOL, or Yahoo! users. **Important:** - As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License (“PIC USL”) is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to	As appropriate to your organization	Preparing for Installation of Servers in the Perimeter Network in the Deployment documentation

	continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013). • The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down. • More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/ device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM		

	and voice. 1. Provision support for XMPP and federation support for Office Communications Server 2007, Office Communications Server 2007 R2, Lync Server 2010 partners, if your deployment will use these 2. Configure firewalls.		
Set up reverse proxy.	• Set up the reverse proxy (for example, for Microsoft Forefront Threat Management Gateway 2010 or Microsoft Internet Security and Acceleration (ISA) Server with Service Pack 1) in the perimeter network, obtain the necessary public certificates, and configure the web publishing rules on the reverse proxy server. Prepare the reverse proxy for Mobility services if you have planned for Mobility and are deploying the Mobility services on the Front End pool or Standard Edition server.	**Administrators** group or Reverse Proxy administrator	Setting Up Reverse Proxy Servers in the Deployment documentation
Setup a Director (optional).	• (Optional) Install and configure one or more Directors in the internal network.	**Administrators** group	Setting Up the Director in the Deployment documentation
Set up Edge Servers.	1. Install prerequisite software. 2. Transport the exported topology configuration file to each Edge Server. 3. Install the Lync Server 2013 software on each Edge Server. 4. Configure the Edge Servers. 5. Request and install certificates for each Edge Server. 6. Start the Edge Server services.	**Administrators** group	Setting Up Edge Servers in the Deployment documentation
Configure deployment for external user access.	1. Use the Lync Server Control Panel to configure support for each of the following (as applicable): • Media relay • Federation route • Remote user access • Federation with Lync Server, Office Communications Server and Live Communications Server • Public IM connectivity • XMPP federation • Anonymous users	**RTCUniversalServerAdmins** group or user account that is assigned to the **CSAdministrator** role	Configuring Support for External User Access in the Deployment documentation

	2. Configure user accounts for remote user access, federation, public IM connectivity, XMPP and anonymous user support (as applicable)		
Verify your Edge Server configuration.	1. Verify server connectivity and replication of configuration data from internal servers. 2. Verify that external users can connect, including remote users, users in federated domains, public IM users, and anonymous users, as appropriate to your deployment. 3. Verify configuration and communication using the Lync Server Remote Connectivity Analyzer https://www.testocsconnectivity.com 4. Troubleshoot configuration and communication difficulties	For verification of replication, **RTCUniversalServerAdmins** group or user account that is assigned to the **CSAdministrator** role For verification of user connectivity, a user for each type of external user access that you support Remote users	Verifying Your Edge Deployment in the Deployment documentation

1.4.2.2 System Requirements for External User Access Components

System Requirements for External User Access Components

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2013-01-17*

System requirements for edge components include hardware, software, and collocation requirements for Edge Servers, reverse proxy servers and optional Directors that you plan to deploy.

- Components Required for External User Access
- Configuration Requirements for Reverse Proxy
- Hardware Load Balancer Requirements
- Hardware and Software Requirements for Edge Components
- Supported Server Collocation for Edge Components

1.4.2.2.1 Components Required for External User Access

Components Required for External User Access

See Also

Planning > Planning for External User Access > System Requirements for External User Access Components >

Topic Last Modified: *2013-01-17*

Most Edge components are deployed in a perimeter network. The following components make up the edge topology of the perimeter network. Except where noted, the components are part of the Scenarios for External User Access and are in the perimeter network. Edge components include the following:

- Edge Servers
- Reverse proxies
- Firewalls
- Directors (optional, and logically located on the internal network)
- Load balancing for Scaled Edge Topologies (either DNS load balancing or a hardware load balancer)

Important:

Using DNS load balancing on one interface and hardware load balancing on the other is not supported. You must use hardware load balancing for both interfaces or DNS load balancing for both.

Edge Servers

The Edge Servers send and receive network traffic for the services offered by internal deployment by external users. The Edge Server runs the following services:

- **Access Edge service** The Access Edge service provides a single, trusted connection point for both outbound and inbound Session Initiation Protocol (SIP) traffic.
- **Web Conferencing Edge service** The Web Conferencing Edge service enables external users to join meetings that are hosted on your internal Lync Server 2013 deployment.
- **A/V Edge service** The A/V Edge service makes audio, video, application sharing, and file transfer available to external users. Your users can add audio and video to meetings that include external participants, and they can communicate using audio and/or video directly with an external user in point-to-point sessions. The A/V Edge service also provides support for desktop sharing and file transfer.
- **XMPP Proxy service** The XMPP Proxy service accepts and sends extensible messaging and presence protocol (XMPP) messages to and from configured XMPP Federated partners.

Authorized external users can access the Edge Servers in order to connect to your internal Lync Server 2013 deployment, but the Edge Servers do not provide a means for any other access to the internal network.

Reverse Proxy

The reverse proxy is required for the following:

- To allow users to connect to meetings or dial-in conferences using simple URLs
- To enable external users to download meeting content
- To enable external users to expand distribution groups
- To allow the user to obtain a user-based certificate for client certificate based authentication
- To enable remote users to download files from the Address Book Server or to submit queries to the Address Book Web Query service
- To enable remote users to obtain updates to client and device software
- To enable mobile devices to automatically discover Front End Servers offering mobility services
- To enable push notifications to mobile devices from the Office 365 or Apple push notification services

For additional information related to reverse proxies and the requirements that reverse proxies must meet, see the details in Configuration Requirements for Reverse Proxy.

Note:

External users do not need a virtual private network (VPN) connection to your organization in order to participate in communications using Lync Server 2013. If you have implemented VPN technology in your organization and your users use the VPN for Lync, media traffic (such as video conferencing) can be adversely affected. You should consider providing a means for media traffic to connect to the AV Edge service directly and bypass the VPN. For details, see the NextHop Blog article, "Enabling Lync Media to Bypass a VPN Tunnel," at http://go.microsoft.com/fwlink/p/?LinkId=256532.

Firewall

You can deploy your edge topology with only an external firewall or both external and internal firewalls. The scenario architectures include two firewalls. Using two firewalls is the recommended approach because it ensures strict routing from one network edge to the other, and it protects your internal deployment behind two levels of firewall.

Director

A Director is a separate, optional server role in Lync Server 2013 that does not home user accounts, or provide presence or conferencing services. It serves as an internal next hop server to which an Edge Server routes inbound SIP traffic destined for internal servers. The Director preauthenticates inbound requests and redirects them to the user's home pool or server. By preauthenticating at the Director, you can drop requests from user accounts that are unknown to the deployment.

A Director helps insulate Standard Edition servers and Front End Servers in Enterprise Edition Front End pools from malicious traffic such as denial-of-service (DoS) attacks. If the network is flooded with invalid external traffic in such an attack, the traffic ends at the Director. For details about the use of Directors, see Scenarios for the Director.

⊟See Also

Concepts

Hardware Load Balancer Requirements

1.4.2.2.2 Hardware Load Balancer Requirements

Hardware Load Balancer Requirements

Planning > Network Planning for Lync Server > Load Balancing Requirements >

Topic Last Modified: *2012-10-22*

The Lync Server 2013 scaled consolidated Edge topology is optimized for DNS load balancing for new deployments federating primarily with other organizations using Lync Server. If high availability is required for any of the following scenarios, a hardware load balancer must be used on Edge Server pools for the following:

- Federation with organizations using Office Communications Server 2007 R2 or Office Communications Server 2007
- Exchange UM for remote users using Exchange UM prior to Exchange 2010 with SP1
- Connectivity to public IM users

Important:

Using DNS load balancing on one interface and hardware load balancing on the other is not supported. You must use hardware load balancing for both interfaces or DNS load balancing for both.

Note:

If you are using a hardware load balancer, the load balancer deployed for connections with the internal network must be configured to load balance only the traffic to servers running the Access Edge service and the A/V Edge service. It cannot load balance the traffic to the internal Web Conferencing Edge service or the internal XMPP Proxy service.

Note:

The direct server return (DSR) NAT is not supported with Lync Server 2013.

To determine whether your hardware load balancer supports the necessary features required by Lync Server 2013, see "Lync Server 2010 Load Balancer Partners" at http://go.microsoft.com/fwlink/p/?linkId=202452.

Hardware Load Balancer Requirements for Edge Servers Running the A/V Edge Service

Following are the hardware load balancer requirements for Edge Servers running the A/V Edge service:

- Turn off TCP nagling for both internal and external ports 443. Nagling is the process of combining several small packets into a single, larger packet for more efficient transmission.
- Turn off TCP nagling for external port range 50,000 – 59,999.
- Do not use NAT on the internal or external firewall.
- The edge internal interface must be on a different network than the Edge Server external interface and routing between them must be disabled.
- The external interface of the Edge Server running the A/V Edge Service must use publically routable IP addresses and no NAT or port translation on any of the edge external IP addresses.

Hardware Load Balancer Requirements

Cookie-based affinity requirements are greatly reduced in Lync Server 2013 for Web services. If you are deploying Lync Server 2013 and will not retain any Lync Server 2010 Front End Servers or Front End pools, you do not need cookie-based persistence. However, if you will temporarily or permanently retain any Lync Server 2010 Front End Servers or Front End pools, you still use cookie-based persistence as it is deployed and configured for Lync Server 2010.

Note:

If you decide to use cookie-based affinity even though your deployment does not require it, there is no negative impact to doing so.

For deployments that **will not use** cookie-based affinity:

- On the reverse proxy publishing rule for port 4443, set **Forward host header** to True. This will ensure that the original URL is forwarded.

For deployments that **will use** cookie-based affinity:

- On the reverse proxy publishing rule for port 4443, set **Forward host header** to True. This will ensure that the original URL is forwarded.
- Hardware load balancer cookie MUST NOT be marked httpOnly
- Hardware load balancer cookie MUST NOT have an expiration time

- Hardware load balancer cookie MUST be named **MS-WSMAN** (This is the value that the Web services expect, and cannot be changed)
- Hardware load balancer cookie MUST be set in every HTTP response for which the incoming HTTP request did not have a cookie, regardless of whether a previous HTTP response on that same TCP connection had already obtained a cookie. If the load balancer optimizes cookie insert to only occur once per TCP connection, that optimization MUST NOT be used

Note:

Typical hardware load balancer configurations use source-address affinity and a 20 min. TCP session lifetime, which is fine for Lync Server and Lync 2013 clients because session state is maintained through client usage and/or and application interaction.

If you are deploying mobile devices, your hardware load balancer must be able to load balance individual request within a TCP session (in effect, you must be able to load balance an individual request based on the target IP address).

Warning:

F5 hardware load balancers have a feature called OneConnect that ensures each request within a TCP connection is individually load balanced. If you are deploying mobile devices, ensure your hardware load balancer vendor supports the same functionality. The latest Apple iOS mobile apps require Transport Layer Security (TLS) version 1.2. F5 provides specific settings for this.
For details on third party hardware load balancers, see http://go.microsoft.com/fwlink/p/?linkId=230700

Following are the hardware load balancer requirements for Director and Front End pool Web Services:

- For internal Web Services VIPs, set Source_addr persistence (internal port 80, 443) on the hardware load balancer. For Lync Server 2013, Source_addr persistence means that multiple connections coming from a single IP address are always sent to one server to maintain session state.
- Use TCP idle timeout of 1800 seconds.
- On the firewall between the reverse proxy and the next hop pool’s hardware load balancer, create a rule to allow https: traffic on port 4443, from the reverse proxy to the hardware load balancer. The hardware load balancer must be configured to listen on ports 80, 443, and 4443.

Summary of Hardware Load Balancer Affinity Requirements

Client/user location	External web services FQDN affinity requirements	Internal web services FQDN affinity requirements
Lync Web App (internal and external users) Mobile device (internal and external users)	No affinity	Source address affinity
Lync Web App (external users only) Mobile device (internal and external users)	No affinity	Source address affinity
Lync Web App (internal users only)	No affinity	Source address affinity

Mobile device (not deployed)		

Port Monitoring for Hardware Load Balancers

You define port monitoring on the hardware load balancers to determine when specific services are no longer available due to hardware or communications failure. For example, if the Front End Server service (RTCSRV) stops because the Front End Server or Front End pool fails, the HLB monitoring should also stop receiving traffic on the Web Services. You implement port monitoring on the HLB to monitor the following:

Front End Server User Pool – HLB Internal Interface

Virtual IP/Port	Node Port	Node Machine/ Monitor	Persistence Profile	Notes
<pool>web-int_mco_443_vs 443	443	Front End 5061	Source	HTTPS
<pool>web-int_mco_80_vs 80	80	Front End 5061	Source	HTTP

Front End Server User Pool – HLB External Interface

Virtual IP/Port	Node Port	Node Machine/ Monitor	Persistence Profile	Notes
<pool>web_mco_443_vs 443	4443	Front End 5061	None	HTTPS
<pool>web_mco_80_vs 80	8080	Front End 5061	None	HTTP

1.4.2.2.3 Hardware and Software Requirements for Edge Components

Hardware and Software Requirements for Edge Components

Planning > Planning for External User Access > System Requirements for External User Access Components >

Topic Last Modified: *2013-02-21*

The hardware and software requirements for edge components include those for the Microsoft Lync Server 2013 communications software components, including Edge Servers and the optional Directors, as well as those for other components, including reverse proxy servers, firewalls, and load balancers to be deployed the perimeter network to support external user access. For details about the components required to support external user access and supported topologies, see Components Required for External User Access.

Hardware and Software Requirements for Edge Servers

The operating system requirements for Edge Servers are the same as for the other Lync Server 2013 roles: the 64-bit edition of the Windows Server 2008 R2 SP1 or Windows Server 2012.

The following table shows the hardware requirements for Edge Servers.

Hardware System Requirements for Edge Servers

Hardware component	Minimum requirement
CPU	One of the following: • 64-bit dual processor, quad-core, 2.0 GHz or higher • 64-bit 4-way processor, dual-core, 2.0 GHz or higher
Memory	12 GB recommended
Disk	• One of the following: • 10K RPM hard disk drive (HDD) • High-performance solid state drive (SSD) with performance equal to or better than 10K RPM HDD • 2x RAID 10 (striped and mirrored) 15K RPM disk set
Network	Two interfaces required, either one 2-port 1 Gbps NIC or two 1-port 1 Gbps NICs.

Lync Server 2013 is available only in 64-bit, therefore each Edge Server requires one of the following operating systems.

- Windows Server 2008 R2 Enterprise Edition with SP1 operating system, or Windows Server 2008 R2 Standard Edition with SP1 operating system.
- Windows Server 2012 Enterprise or Datacenter operating system.

Directors are internal components and installed as part of the internal network prior to deployment of Edge Servers. For hardware and software requirements for Directors, see Hardware and Software Requirements for the Director.

Lync Server 2013 Edge Servers require the installation of additional programs and updates. The requirements for additional software on Edge Servers are listed here.

- Each server running Lync Server 2013 must have the correct release of Windows PowerShell 3.0 installed. For details, see Installing Windows PowerShell 3.0.
- Lync Server requires Microsoft .NET Framework 4.5. For Lync Server 2013 installed on Windows Server 2008 R2, you must manually install the 64-bit edition of Microsoft .NET Framework 4.5 on the server prior to installing Lync Server 2013. To manually install it, download the Microsoft .NET 4.5 Framework from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?LinkId=268529
- **Windows Identity Foundation** in Lync Server 2013 requires the installation of Windows Identity Foundation in order to support server to server authentication scenarios. Windows Server 2008 R2 and Windows Server 2012

require different procedures to install the Windows Identify Foundation. Select your server operating system from the following list:

- Windows Server 2008 R2   For Windows Server 2008 R2, you check to see if it has already been installed on your computer. To do this, go to **Add/ Remove Programs**, **View Installed Updates**, and look under **Windows** for the entry **Windows Identity Foundation (KB974405)**. For details about installing Windows Identity Foundation, see http://go.microsoft.com/fwlink/?LinkId=285258.
- Windows Server 2012   For Windows Server 2012, you use **Server Manager** to install the Windows Identity Foundation. In the Server Manager **Add Roles and Features Wizard**, select **Features**. Select **Windows Identity Foundation 3.5** from the list. Click **Next**, then click **Install**.

1.4.2.2.4 Supported Server Collocation for Edge Components

Supported Server Collocation for Edge Components

Planning > Planning for External User Access > System Requirements for External User Access Components >

Topic Last Modified: *2012-09-08*

The Access Edge service, Web Conferencing Edge service, A/V Edge service and XMPP Proxy service are collocated on the Edge Servers. The following servers provide functions needed for external user access and must be deployed as dedicated servers:

- Edge Server
- Director (Optional)
- Reverse proxy

Important:

The reverse proxy does not need to be dedicated to serving only Lync Server 2013. For example, you can provide services to publish the Lync Server Web services, and concurrently provide a published Web site for another Web site that has no bearing on Lync Server at all. If you already have a reverse proxy server in the perimeter network to support other services, you can use it for Lync Server 2013.

1.4.2.3 Preparing for Installation of Servers in the Perimeter Network

Preparing for Installation of Servers in the Perimeter Network

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2012-09-08*

Before you set up Edge Server components, you need to ensure that computers that you are setting up meet system requirements and complete other prerequisite steps required for deployment of Edge Server components.

Before you begin, review the details in the following topics in the Planning documentation for the reference architecture that you want to deploy:

- Single Consolidated Edge with Private IP Addresses and NAT
- Single Consolidated Edge with Public IP Addresses
- Scaled Consolidated Edge, DNS Load Balancing with Private IP Addresses Using NAT
- Scaled Consolidated Edge, DNS Load Balancing with Public IP Addresses

- Scaled Consolidated Edge with Hardware Load Balancers
- Configure DNS for Edge Support
- Set Up Hardware Load Balancers for Scaled Edge Topologies
- Configure Firewalls and Ports for External User Access
- Determine External A/V Firewall and Port Requirements
- Request Certificates for Edge Components

1.4.2.3.1 Configure DNS for Edge Support

Configure DNS for Edge Support

See Also

Deployment > Deploying External User Access > Preparing for Installation of Servers in the Perimeter Network >

Topic Last Modified: *2013-02-15*

You must configure Domain Name System (DNS) records for internal and external edge interfaces, including both Edge Server and reverse proxy interfaces. By default, Edge Servers are not joined to a domain and will not have a fully qualified domain name (fully qualified domain name). The Edge Server is only referred to by the short (machine) name, not a fully qualified domain name. However, Topology Builder uses FQDNs, not short names. The name of the Edge Server must match the FQDN used by Topology Builder. To do this, you define a DNS suffix that, when combined with the machine name, results in the expected FQDN. Use the following procedure in "To add the DNS suffix to the computer name on and Edge Server that is not joined to a domain" to add the DNS suffix to the computer name.

Note:

By default, DNS uses a round robin algorithm to rotate the order of resource record data returned in query answers where multiple resource records of the same type exist for a queried DNS domain name. Lync Server 2013 DNS load balancing, depends on DNS round-robin as a part of the DNS Load Balancing mechanism. Verify that round-robin setting has not been disabled. If you are using a DNS server that is not running a Windows operating system, verify that round-robin resource record ordering is enabled.

Use the following procedures in "**To create a DNS SRV record**" to create and verify each DNS SRV record. Use the procedure in "**To create a DNS A record**" to define the DNS A records required for external user access. To confirm that the records are configured and working correctly, see "**To verify a DNS record**" in this topic. For details about each record required to support external user access, see Determine DNS Requirements.

⊟To add the DNS suffix to the computer name on an Edge Server that is not joined to a domain

1. On the computer, click **Start**, right-click **Computer**, and then click **Properties**.
2. Under **Computer name, domain, and workgroup settings**, click **Change settings**.
3. On the **Computer Name** tab, click **Change**.
4. In **Computer Name/Domain Changes**, click **More**.
5. In **DNS Suffix and NetBIOS Computer Name**, in **Primary DNS suffix of this computer**, type the name of your internal domain (for example, corp.contoso.com), and then click **OK** three times.
6. Restart the computer.

⊟To create a DNS SRV record

1. On the appropriate DNS server, click **Start**, click **Control Panel**, click **Administrative Tools**, and then click **DNS**.

Important:
You need to configure DNS so that there are: 1) external DNS entries for external DNS lookups by remote users and federated partners; 2) entries for DNS lookups for use by the Edge Servers within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet), including A records for the internal servers running Lync Server 2013; and 3) internal DNS entries for lookups by the internal clients and servers running Lync Server 2013.

2. In the console tree for your SIP domain, expand **Forward Lookup Zones**, and then right-click the domain where Lync Server 2013 is installed.
3. Click **Other New Records**.
4. In **Select a resource record type**, type **Service Location (SRV)**, and then click **Create Record**.
5. Provide all required information for the DNS SRV record.

⊟To create a DNS A record

1. On the DNS server, click **Start**, click **Control Panel**, click **Administrative Tools**, and then click **DNS**.
2. In the console tree for your SIP domain, expand **Forward Lookup Zones**, and then right-click the domain in which Lync Server 2013 is installed.
3. Click **New Host (A)**.
4. Provide all required information for the DNS SRV record.

⊟To verify a DNS record

1. Log on to a client computer in the domain.
2. Click **Start**, and then click **Run**.
3. At the command prompt, run the following command:

```
nslookup <FQDN edge interface>
```

4. Verify that you receive a reply that resolves to the appropriate IP address for the FQDN.

Tasks

Create a DNS SRV Record for Integration with Hosted Exchange UM

Concepts

Determine DNS Requirements

1.4.2.3.2 Set Up Hardware Load Balancers for Scaled Edge Topologies

Set Up Hardware Load Balancers for Scaled Edge Topologies

Deployment > Deploying External User Access > Preparing for Installation of Servers in the Perimeter Network >

Topic Last Modified: *2012-09-08*

If you are configuring a scaled edge topology using a hardware load balancer, see Scaled Consolidated Edge with Hardware Load Balancers in the Planning documentation.

1.4.2.3.3 Configure Firewalls and Ports for External User Access

Configure Firewalls and Ports for External User Access

See Also

Deployment > Deploying External User Access > Preparing for Installation of Servers in the Perimeter Network >

Topic Last Modified: *2012-05-21*

To configure firewalls and ports, you need to configure them for Edge Servers, reverse proxy servers, and possibly hardware load balancers (for a scaled deployment that does not use DNS load balancing). This section provides information about firewall and port requirements for all Edge Server components and the configuration of firewall ports for Edge Servers. For details about configuring ports for reverse proxy servers, see Setting Up Reverse Proxy Servers. If you are deploying a scaled edge topology and are using hardware load balancing instead of DNS load balancing, see Scaled Consolidated Edge with Hardware Load Balancers in the Planning documentation for details about configuring ports for hardware load balancers.

Concepts

Determine External A/V Firewall and Port Requirements

1.4.2.3.4 Determine External A/V Firewall and Port Requirements

Determine External A/V Firewall and Port Requirements

Microsoft Lync Server 2013 > Planning > Planning for External User Access >

Topic Last Modified: *2012-10-29*

Audio/Video (A/V) communication can be a complex. Because of the nature of protocols used in A/V and how clients and servers use the protocols, a special section is warranted to explain the differences between client and server versions.

Use the following A/V Firewall and Port table to determine firewall requirements and which ports to open. Then, review the network address translation (NAT) terminology because NAT can be implemented in many different ways. For a detailed example of firewall port settings, see the reference architectures in Scenarios for External User Access.

General Protocol Usage for UDP and TCP in Audio/Video and Media Traffic

Audio/Video Transport	Usage
UDP	Preferred transport layer protocol for audio and video
TCP	Fallback transport layer protocol for audio and video Required transport layer protocol for application sharing to Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013 Required transport layer protocol for file transfer to Lync Server 2010 and Lync Server 2013

External A/V Firewall Port Requirements for External User Access

The firewall port requirements for external (and internal) SIP and conferencing interfaces are consistent, regardless of the version of your client or the version of the federation partner.

The same is not true for the Audio/Video Edge external interface. For federation with Office Communications Server 2007, the A/V Edge service requires that external firewall rules allow RTP/TCP and RTP/UDP traffic in the 50,000 through 59,999 port range to flow in both directions. The previous table assumes that Lync Server 2013 is the primary federation partner and it is being configured to communicate with one of the other federation partner types listed.

Configuring the Audio/Video port range of 50,000-59,999 must take into account that the port range will contain the source ports for communications to federation partners. In detail, consider that a communication is initiated from a federation partner. The communication from the A/V Edge service ports in the 50,000-59,999 range will connect to the expected port TCP 443 of the partner’s A/V Edge service. Conversely, inbound traffic to your A/V Edge service port TCP 443 will have a source port in the range of 50,000-59,999.

Different firewalls and policies for firewall administration may require only destination rules to be configured, or they may require both source and destination to be configured. If your requirements are for destination ports only, the Audio/Video requirements are:

Source IP	Destination IP	Destination Port
A/V Edge service interface	Any	TCP 443
A/V Edge service interface	Any	UDP 3478
Any	A/V Edge service interface	TCP 443
Any	A/V Edge service interface	UDP 3478

If your policies require both inbound and outbound firewall rule definitions, the Audio/Video requirements are:

Source IP	Destination IP	Source Port	Destination Port
A/V Edge service interface	Any	TCP 50,000-59,999	TCP 443
A/V Edge service interface	Any	UDP 3478	UDP 3478
Any	A/V Edge service interface	Any	TCP 443
Any	A/V Edge service interface	Any	UDP 3478

◆**Important:**

Microsoft Office Communications Server 2007 requires a slightly different configuration. The TCP and UDP port range of 50,000-59,999 must be open inbound and outbound. This requirement is only for Office Communicator 2007. Office Communications Server 2007 R2, Lync Server 2010 and Lync Server 2013 only require TCP range 50,000-59,999 open outbound.

NAT Requirements for External User Access

NAT has typically been a routing function, but newer devices such as firewalls and even hardware load balancers can be configured for NAT. Rather than focusing on which device is performing NAT, this topic describes the required NAT behavior instead.

Lync Server 2013 communications software does not support NAT for traffic to or from the Edge internal interface, but for the Edge external interface, the following NAT behavior is required.

> **◆Important:**
>
> You must configure symmetric NAT for incoming and outgoing traffic. Symmetric NAT is the NAT technology described in this topic.

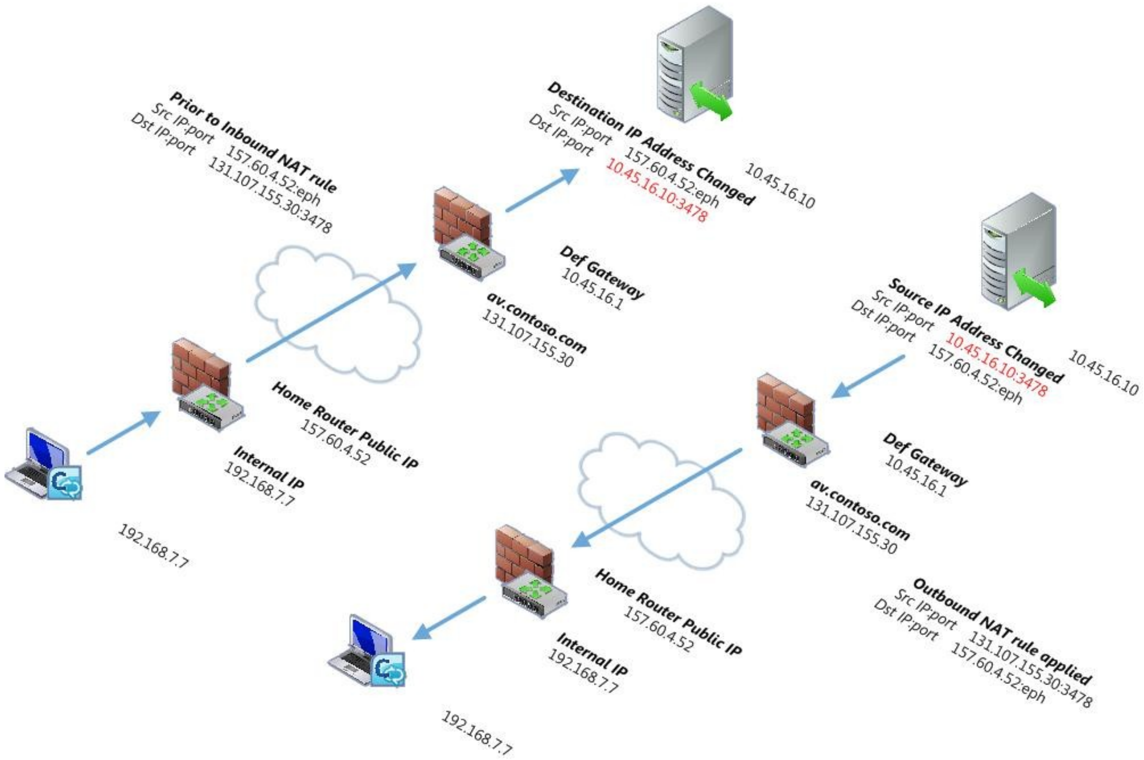
This documentation uses the acronyms ChangeDST and ChangeSRC in tables and drawings to define the following required behavior:

- **ChangeDST** The process of changing the destination IP address on packets destined for the network that is using NAT. This is also known as transparency, port forwarding, destination NAT mode, or half-NAT mode.
- **ChangeSRC** the process of changing the source IP address on packets leaving the network that is using NAT. This is also known as proxy, secure NAT, stateful NAT, source NAT or full-NAT mode.

Regardless of the naming convention used, the NAT behavior required for the external interface of the Edge Server is as follows:

- For traffic from the Internet to the Edge external interface:
  - Change the destination IP address of the incoming packet from the Edge external interface public IP address to the translated IP address of the Edge external interface.
  - Leave the source IP address intact so that there is a return route for the traffic.
- For traffic from the Edge external interface to the Internet:
  - Change the source IP address of the packet leaving the Edge external interface, from the translated IP address to the public IP address of the Edge external interface so that the internal Edge IP address is not exposed and because it is a non-routable IP address.
  - Leave the destination IP address intact on the outgoing packets.

The following figure shows the distinction between changing the destination IP address (ChangeDST) for inbound traffic and changing the source IP Address (ChangeSRC) for outbound traffic using the A/V edge as an example.


Prior to Inbound NAT rule
Src IP:port 157.60.4.52:eph
Dst IP:port 131.107.155.30:3478
Destination IP Address Changed
Src IP:port 157.60.4.52:eph
Dst IP:port 10.45.16.10:3478
10.45.16.10
Def Gateway
10.45.16.1
av.contoso.com
131.107.155.30
Home Router Public IP
157.60.4.52
Internal IP
192.168.7.7
192.168.7.7
Source IP Address Changed
Src IP:port 10.45.16.10:3478
Dst IP:port 157.60.4.52:eph
10.45.16.10
Def Gateway
10.45.16.1
av.contoso.com
131.107.155.30
Outbound NAT rule applied
Src IP:port 131.107.155.30:3478
Dst IP:port 157.60.4.52:eph
Home Router Public IP
157.60.4.52
Internal IP
192.168.7.7
192.168.7.7

The key points are:

- Traffic that is inbound to the server running the A/V Edge service, the source IP address does not change but the destination IP address changes from 131.107.155.30 to the translated IP address of 10.45.16.10.
- Traffic that is outbound from the server running the A/V Edge service back to the workstation, the source IP address changes from the server's public IP address to the public IP address of the server running the A/V Edge service. The destination IP remains the workstation's public IP address. After the packet leaves the first NAT device outbound, the rule on the NAT device changes the source IP address of the server running the A/V Edge service external interface IP address (10.45.16.10) to its public IP address (131.107.155.30).

1.4.2.3.5 Request Certificates for Edge Components

Request Certificates for Edge Components

Deployment > Deploying External User Access > Preparing for Installation of Servers in the Perimeter Network >

Topic Last Modified: *2012-09-08*

The certificates required to support external user access include certificates issued by a public certification authority (CA), and certificates issued by an internal Enterprise CA:

- Certificates required for the external interface of Edge Server and the reverse proxy must be issued by a public CA.
- Certificates required for the internal interface can be issued by either a public CA or an internal enterprise CA. We recommend using an internal Windows Server 2008 CA, Windows Server 2008 R2 CA, or Windows Server 2012 CA for

creating these certificates to save on the expense of using public certificates.

Important:
It can take time to process certificate requests, especially requests to public CAs, so you should request certificates for your Edge Servers early enough to ensure that they are available when you start deployment of your Edge Server components. For a summary of certificate requirements for Edge Servers, see Certificate Requirements for External User Access.

Although you can choose to use a public CA for the internal edge certificate, we recommend that you use an internal enterprise CA for those other certificates instead to minimize the cost of certificates. For a summary of certificate requirements for Edge Servers, see Certificate Requirements for External User Access.

Note:
When you install an Edge Server, setup includes a certificate wizard that facilitates the tasks of requesting, assigning, and installing certificates, as described in the Set Up Edge Certificates section. If you want to request certificates prior to installing an Edge Server (such as to save time during actual deployment of Edge Server components), you can do so using internal servers as long as you ensure that the certificates are exportable and contain all of the required subject alternative names. This documentation does not provide procedures for using internal servers to request certificates.

Request certificates from a public CA

Your Edge Server deployment requires a single public certificate for the external interfaces of Edge Servers, which is used for the Access Edge service, the Web Conferencing Edge service, and for A/V authentication service. This certificate must have an exportable private key to ensure that the A/V authentication service uses the same keys on all Edge Servers in a pool. The reverse proxy, which is used with Microsoft Internet Security and Acceleration (ISA) Server 2006 or Microsoft Forefront Threat Management Gateway 2010, also requires a public certificate.

Request certificates from an internal Enterprise CA

The certificates required for the internal edge interface can be issued by either a public certification authority (CA) or an internal CA. You can use an internal enterprise CA to help minimize the cost of certificates. If your organization has an internal CA deployed, the certificates for the internal edge should be issued by the internal CA. Using an internal enterprise CA for internal certificates can reduce the cost of certificates.

For a summary of certificate requirements for edge components, see Certificate Requirements for External User Access. For details about using a public CA to obtain certificates, see Request Certificates for Edge Components. For details about requesting, installing, and assigning certificates, see Set Up Edge Certificates.

1.4.2.4 Building an Edge and Director Topology

Building an Edge and Director Topology

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2012-09-08*

Building the topology involves the following planning and deployment tasks:

- **Planning** You need to define an appropriate topology for your organization and identify the components required to deploy it. These are standard steps in the planning process. The Microsoft Lync Server 2013, Planning Tool provided with Lync Server 2013 makes it easy to start the planning process, as well as including the ability to easily make changes as your requirements and plans are finalized.
- **Deployment** The topology that you define using Topology Builder is essential to the deployment of any Lync Server 2013 server. If you do not finish defining and publishing your topology by using Topology Builder as part of your planning efforts, you must complete it and publish the topology before you deploy your Edge Servers.

You cannot deploy Edge Server components until you have deployed at least one internal pool, and you must install Topology Builder to deploy an internal pool. This section does not cover installation of Topology Builder because that is part of the installation process for the internal pool.

For details about these tools, see Deployment Checklist for External User Access.

Note:

If you previously used Topology Builder to define a complete topology, including the edge topology, you do can skip the Define Your Edge Topology and Publish Your Topology tasks in this section, but you do need to complete the Export Your Topology and Copy It to External Media for Edge Installation task.

- Define Your Edge Topology
- Define Optional Director Topologies in Your Topology
- Publish Your Topology
- Export Your Topology and Copy It to External Media for Edge Installation

1.4.2.4.1 Define Your Edge Topology

Define Your Edge Topology

Deployment > Deploying External User Access > Building an Edge and Director Topology >

Topic Last Modified: *2012-09-28*

You must use Topology Builder to build your topology and you must set up at least one internal Front End pool or Standard Edition server before you can deploy your Edge Server. Use the following procedure to define the edge topology for a single Edge Server, and then use the procedures in Publish Your Topology and Export Your Topology and Copy It to External Media for Edge Installation to publish the topology and make it available to your Edge Server.

Note:

The internal Edge interface and external Edge interface must use the same type of load balancing. You cannot use DNS load balancing on one Edge interface and hardware load balancing on the other Edge interface.

To successfully publish, enable, or disable a topology when adding or removing a server role, you must be logged in as a user who is a member of the RTCUniversalServerAdmins and Domain Admins groups. You can also grant the administrator rights and permissions required for adding server roles to a user account. For details, see Delegate Setup Permissions in the Standard Edition server or Enterprise Edition server Deployment documentation. For other configuration changes, only membership in the RTCUniversalServerAdmins group is required.

If you defined your edge topology when you defined and published your internal topology, and no changes are required to the edge topology that you previously defined, you do not need to do define it and publish it again. Use the following procedure only if you need to make changes to your edge topology. You must make the previously defined and published topology available to your Edge Servers, which you do by using the procedure in Export Your Topology and Copy It to External Media for Edge Installation.

Important:

You cannot run Topology Builder from an Edge Server. You must run it from your Front End Server or Standard Edition servers.

The process to define your Edge Server topology is done in Topology Builder. The three primary types of Edge Server topologies that you plan and configure are listed below:

- To define the Topology for a Single Edge Server
- To define the Topology for a Load Balanced Edge Server Pool
- To define the Topology for a Hardware Load Balanced Edge Pool

⊟To define the topology for a single Edge Server

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In the console tree, expand the site in which you want to deploy an Edge Server.
3. Right-click **Edge pools**, and then click **New Edge Pool**.
4. In **Define the New Edge Pool**, click **Next**.
5. In **Define the Edge pool FQDN**, do the following:
   - In **Pool FQDN**, type the fully qualified domain name (FQDN) of the internal interface for the Edge Server.

     Important:

     The name you specify must be identical to the computer name configured on the server. By default the computer name of a computer that is not joined to a domain is a short name, not an FQDN. Topology Builder uses FQDNs, not short names. So, you must configure a DNS suffix on the name of the computer to be deployed as an Edge Server that is not joined to a domain. Use only standard characters (including A–Z, a–z, 0–9, and hyphens) when assigning FQDNs of your Lync Servers, Edge Servers, and pools. Do not use Unicode characters or underscores. Nonstandard characters in an FQDN are often not supported by external DNS and public CAs (when the FQDN must be assigned to the SN in the certificate). For details about adding a DNS suffix to a computer name, see Configure DNS for Edge Support.

   - Click **Single computer pool**, and then click **Next**.
6. In **Select features**, do the following:
   - If you plan to use a single FQDN and IP address for the SIP Access service, Lync Server 2013 Web Conferencing service, and A/V Edge services, select the **Use a single FQDN and IP Address** check box.
   - If you plan to enable federation select the **Enable federation for this Edge pool (Port 5061)** check box.

     Note:

     You can select this option, but only one Edge pool or Edge Server in your organization can be published externally for federation. All access by federated users, including public instant messaging (IM) users, go through the same Edge pool or single Edge Server. For example, if your deployment includes an Edge pool or single Edge Server deployed in New York and one deployed in London and you enable federation support on the New York Edge pool or single Edge Server, signal traffic for federated users will go through the New York Edge pool or single Edge Server. This is true even for communications with London users, although a London internal user calling a London federated user uses the

> London pool or Edge Server for A/V traffic.

- If you plan to support the extensible messaging and presence protocol (XMPP) for your deployment, select the **Enable XMPP federation (port 5269)** check box

7. In **Select IP Options**, do the following:
   - **Enable IPv4 on internal interface**: Select the check box if you want to apply an IPv4 address to the Edge Server or Edge pool internal interface
   - **Enable IPv6 on internal interface**: Select the check box if you want to apply an IPv6 address to the Edge Server or Edge pool internal interface
   - **Enable IPv4 on external interface**: Select the check box if you want to apply an IPv4 address to the Edge Server or Edge pool external interface
   - **Enable IPv6 on external interface**: Select the check box if you want to apply an IPv6 address to the Edge Server or Edge pool external interface

   You can also configure the Edge Server or Edge pool to use a network address translation address for the external IP addresses. You do this by selecting the check box **The external IP address of this Edge pool is translated by NAT**.
8. In **External FQDNs**, do the following:
   - If in **Select features** you chose to use a single FQDN and IP address for the SIP access, Web Conferencing service, and A/V Edge service, type the external FQDN in **SIP Access**.

     > **Note:**
     >
     > If you choose this option, you must specify a different port number for each of the edge services (recommended port settings: 5061 for Access Edge service, 444 for Web Conferencing Edge service, and 443 for A/V Edge service). Selecting this option can help prevent potential connectivity issues, and simplify the configuration because you can then use the same port number (for example, 443) for all three services.

   - If in **Select features** you did not chose to use a single FQDN and IP Address, type the External FQDNs for **SIP Access**, **Web Conferencing** and **Audio Video**, keeping the default ports.
9. Click **Next**.
10. In **Define the Internal IP address**, type the IP address of your Edge Server in **Internal IPv4 address** and **Internal IPv6 address** as is appropriate for your requirements. Click **Next**.
11. In **Define the External IP address**, do the following:
    - If you chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Edge service, type the external IPv4 address of the Edge Server in **SIP Access**, and then, click **Next**.
    - If you chose to use IPv6 addresses, type the external IPv6 address of the Edge Server in **SIP Access**, and then, click **Next**.
    - If you did not chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Edge service, type the external IPv4 addresses of the Edge Server in **SIP Access**, **Web Conferencing**, and **A/V Conferencing**, and then click **Next**.
    - If you chose to use IPv6 addresses and did not chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Edge service, type the external IPv6 addresses of the Edge Server in **SIP Access**, **Web Conferencing**, and **A/V Conferencing**, and then click **Next**.

      > **Note:**
      >
      > If you did not choose to enable and assign IPv6 addressing, you will not see this dialog box.
12. If you chose to use NAT, a dialog box appears. In **Public IPv4 address for the A/V Edge service**, type the public IPv4 address to be translated by NAT, and then click **Next**.

> **Note:**
> This should be the external IP address of the A/V Edge service.

13. If you chose to use NAT and IPv6 addresses, a dialog box appears. In **Public IPv6 address for the A/V Edge service**, type the public IPv6 address to be translated by NAT, and then click **Next**.

> **Note:**
> This should be the external IP address of the A/V Edge service.

14. In **Define the next hop**, in **Next hop pool**, select the name of the internal pool, which can be either a Front End pool or a Standard Edition pool. Or, if your deployment includes a Director, select the Director. Then, click **Next**.
15. In **Associate Front End pools**, specify one or more internal pools, which can include Front End pools and Standard Edition servers, to be associated with this Edge Server, by selecting the names of the internal pools that are to use this Edge Server for communication with supported external users.

> **Note:**
> Only one load-balanced Edge pool or single Edge Server can be associated with each internal pool for A/V traffic. If you already have an internal pool associated with an Edge pool or Edge Server, a warning appears indicating that the internal pool is already associated an Edge pool or Edge Server. If you select a pool that is already associated with another Edge Server, it will change the association.

16. Click **Finish**.
17. Publish your topology.

To define the topology for a DNS load balanced Edge Server pool

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In the console tree, expand the site in which you want to deploy Edge Servers.
3. Right-click **Edge Pools**, and then click **New Edge Pool**.
4. In **Define the New Edge Pool**, click **Next**.
5. In **Define the Edge pool FQDN**, do the following:
   - In **Pool FQDN**, type the fully qualified domain name (FQDN) for the internal connection of the Edge pool.

     > **Important:**
     > The name you specify for the pool must be the internal edge pool name. This must be defined as a FQDN. Topology Builder uses FQDNs, not short names. Use only standard characters (including A–Z, a–z, 0–9, and hyphens) when assigning FQDNs of your Lync Servers, Edge Servers, and pools. Do not use Unicode characters or underscores. Nonstandard characters in an FQDN are often not supported by external DNS and public CAs (when the FQDN must be assigned to the SN in the certificate).

   - Click **Multiple computer pool**, and then click **Next**.
6. In **Select features**, do the following:
   - If you plan to use a single FQDN and IP address for the SIP access, Lync Server 2013 Web Conferencing service and A/V Edge services, select the **Use a single FQDN and IP Address** check box.
   - If you plan to enable federation, select the **Enable federation for this Edge pool (Port 5061)** check box. Click **Next**

     > **Note:**
     > You can select this option, but only one Edge pool or Edge Server in your organization can be published externally for federation. All access by federated users, including public instant messaging (IM) users, go through the same Edge pool or single Edge Server.

> For instance, if your deployment includes an Edge pool or single Edge Server deployed in New York and one deployed in London and you enable federation support on the New York Edge pool or single Edge Server, signal traffic for federated users will go through the New York Edge pool or single Edge Server. This is true even for communications with London users, although a London internal user calling a London federated user uses the London pool or Edge Server for A/V traffic.

- If you plan to support the extensible messaging and presence protocol (XMPP) for your deployment, select the **Enable XMPP federation (port 5269)** check box

7. Click **Next**.
8. In **Select IP Options**, do the following:
   - **Enable IPv4 on internal interface**: Select the check box if you want to apply an IPv4 address to the Edge Server or Edge pool internal interface
   - **Enable IPv6 on internal interface**: Select the check box if you want to apply an IPv6 address to the Edge Server or Edge pool internal interface
   - **Enable IPv4 on external interface**: Select the check box if you want to apply an IPv4 address to the Edge Server or Edge pool external interface
   - **Enable IPv6 on external interface**: Select the check box if you want to apply an IPv6 address to the Edge Server or Edge pool external interface

   You can also configure the Edge Server or Edge pool to use a network address translation address for the external IP addresses. You do this by selecting the check box **The external IP address of this Edge pool is translated by NAT**.
9. In **External FQDNs**, do the following:
   - If in **Select features** you chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Edge service, type the external FQDN in **SIP Access**.

     > **Note:**
     >
     > If you choose this option, you must specify a different port number for each of the Edge services (recommended port settings: 5061 for Access Edge service, 444 for Web Conferencing Edge service, and 443 for A/V Edge service). By selecting this option, you can help prevent potential connectivity issues and simplify the configuration because you can then use the same port number (for example, 443) for all three services.

   - If in **Select features** you did not chose to use a single FQDN and IP Address, type the FQDN that you have chosen for your public facing side of the edge pool for in **SIP Access**. In **Web Conferencing**, type the FQDN you have chosen for your public facing side of the Edge pool. In **Audio/Video**, type the FQDN you have chosen for your public facing side of the Edge pool. Use the default ports.
10. Click **Next**.
11. In **Define the computers in this pool**, click **Add**.
12. In **Internal FQDN and IP address**, do the following:
    - In **Internal IPv4 address**, type the IPv4 address and **Internal IPv6 address** as is appropriate for your requirements for the first Edge Server that you want to create in this pool.
    - In **Internal FQDN**, type the FQDN of the first Edge Server that you want to create in this pool.

      > **Note:**
      >
      > The name you specify must be identical to the computer name configured on the server. By default, the computer name of a computer that is not joined to a domain is a short name, not an FQDN. Topology Builder uses FQDNs, not short names. So, you must configure a DNS suffix on the name of the computer to be

deployed as an Edge Server that is not joined to a domain. Use only standard characters (including A–Z, a–z, 0–9, and hyphens) when assigning FQDNs of your Lync Servers, Edge Servers, pools, and arrays. Do not use Unicode characters or underscores. Nonstandard characters in an FQDN are often not supported by external DNS and public CAs (when the FQDN must be assigned to the SN in the certificate). For details about adding a DNS suffix to a computer name, see Configure DNS for Edge Support.

13. Click **Next**.
14. In **Define the external IP addresses**, do the following:
    - If you chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Edge service, type the external IP address of the Edge Server in **SIP Access**.
    - If you did not chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Conferencing service, type the IP address that you have chosen for your public facing side of this Edge pool server for **SIP Access**. In **Web Conferencing**, type the IP address that you have chosen for your public facing side of this Edge pool server. In **A/V Conferencing**, type the IP address you have chosen for your public facing side of this Edge pool server.
15. Click **Next**.
16. If you chose to enable IPv6 addresses, In **Define the external IP addresses**, do the following:
    - If you chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Edge service, type the external IPv6 address of the Edge Server in **SIP Access**.
    - If you did not chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Conferencing service, type the IPv6 address that you have chosen for your public facing side of this Edge pool server for **SIP Access**. In **Web Conferencing**, type the IPv6 address that you have chosen for your public facing side of this Edge pool server. In **A/V Conferencing**, type the IPv6 address you have chosen for your public facing side of this Edge pool server.

Note:

If you did not choose to enable and assign IPv6 addressing, you will not see this dialog box.

17. Click **Finish**.

Note:

You will now see the first Edge Server you created in your pool in the **Define the computers in this pool** dialog box.

18. In **Define the computers in this pool**, click **Add**, and then repeat steps 11 through 14 for the second Edge Server that you want to add to you Edge pool.
19. After you repeat steps 11 through 14, click **Next** in **Define the computers in this pool**.

Note:

At this point, you can see both of the Edge Servers in your pool.

20. If you chose to use NAT, a dialog box appears. In **Public IP address**, type the public IPv4 and IPv6 (as appropriate) addresses to be translated by NAT, and then click **Next**.

Note:

This should be the external IP Address of the A/V Edge.

21. In **Define the next hop**, in the **Next hop pool** list, select the name of the internal pool, which can be either a Front End pool or a Standard Edition pool. Or, if your deployment includes a Director, select the name of the Director.

Then, click **Next**.

22. In **Associate Front End pools**, specify one or more internal pools, which can include Front End pools and Standard Edition servers, to be associated with this Edge Server, by selecting the names of the internal pool(s) that is to use this Edge Server for communication with supported external users.

> **Note:**
> Only one load-balanced Edge pool or single Edge Server can be associated with each internal pool for A/V traffic. If you already have an internal pool associated with an Edge pool or Edge Server, a warning appears indicating that the internal pool is already associated an Edge pool or Edge Server. If you select a pool that is already associated with another Edge Server, it will change the association.

23. Click **Finish**.
24. Publish your topology.

⊟To define the topology for a hardware load balanced Edge Server pool

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In the console tree, expand the site in which you want to deploy Edge Servers.
3. Right-click **Edge Pools**, and then select **New Edge Pool**.
4. In **Define the New Edge Pool**, click **Next**.
5. In **Define the Edge pool FQDN**, do the following:
   - In **FQDN**, type the fully qualified domain name (FQDN) you have chosen for the internal side of the Edge pool.

     > **Important:**
     > The name you specify for the pool must be the internal edge pool name. This must be defined as a FQDN. Topology Builder uses FQDNs, not short names. Use only standard characters (including A–Z, a–z, 0–9, and hyphens) when assigning FQDNs of your Lync Servers, Edge Servers, and pools. Do not use Unicode characters or underscores. Nonstandard characters in an FQDN are often not supported by external DNS and public CAs (when the FQDN must be assigned to the SN in the certificate).

   - Click **Multiple computer pool**, and then **Next**.
6. In **Select features** do the following:
   - If you plan to use a single FQDN and IP address for the SIP access service, Lync Server Web Conferencing service, and A/V Edge service, select the **Use a single FQDN & IP Address** check box.
   - If you plan to enable federation, select the **Enable federation for this Edge pool (Port 5061)** check box.

     > **Note:**
     > You can select this option, but only one Edge pool or Edge Server in your organization may be published externally for federation. All access by federated users, including public instant messaging (IM) users, go through the same Edge pool or single Edge Server. For instance, if your deployment includes an Edge pool or single Edge Server deployed in New York and one deployed in London and you enable federation support on the New York Edge pool or single Edge Server, signal traffic for federated users will go through the New York Edge pool or single Edge Server. This is true even for communications with London users, although a London internal user calling a London federated user uses the London pool or Edge Server for A/V traffic.

   - If you plan to support the extensible messaging and presence protocol (XMPP) for your deployment, select the **Enable XMPP federation (port 5269)** check box

7. Click **Next**.
8. In **Select IP Options**, do the following:
   - **Enable IPv4 on internal interface**: Select the check box if you want to apply an IPv4 address to the Edge Server or Edge pool internal interface
   - **Enable IPv6 on internal interface**: Select the check box if you want to apply an IPv6 address to the Edge Server or Edge pool internal interface
   - **Enable IPv4 on external interface**: Select the check box if you want to apply an IPv4 address to the Edge Server or Edge pool external interface
   - **Enable IPv6 on external interface**: Select the check box if you want to apply an IPv6 address to the Edge Server or Edge pool external interface

Important:

Do Not select the **The external IP address of the Edge pool is translated by NAT** check box. Network address translation (NAT) is not supported when you are using hardware load balancing.

9. In **External FQDNs**, do the following:
   - If in **Select features** you chose to use a single FQDN and IP address for the SIP access, Web Conferencing service, and A/V Edge service, type the external FQDN in **SIP Access**.

Note:

If you choose to select this option, you must specify a different port number for each of the Edge services (recommended port settings: 5061 for Access Edge service, 444 for Web Conferencing Edge service, and 443 for A/V Edge service). By selecting this option, you can help prevent potential connectivity issues and simplify the configuration because you can then use the same port number (for example, 443) for all three services.

   - If in **Select features** you did not chose to use a single FQDN and IP address, type the FQDN that you have chosen for your public facing side of the edge pool for in **SIP Access**. In **Web Conferencing**, type the FQDN you have chosen for your public facing side of the Edge pool. In **Audio/Video**, type the FQDN you have chosen for your public facing side of the Edge pool. Use the default ports.

Note:

These will be the publicly facing virtual IP (VIP) FQDNs for the pool.

10. Click **Next**.
11. In **Define the computers in this pool**, click **Add**.
12. In **Define the external IP addresses**, do the following:
    - If you chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Edge service, type the external IPv4 address of the Edge Server in **SIP Access**.external IP address of the Edge Server in **SIP Access**.
    - If you did not chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Conferencing service, type the IP address that you have chosen for your public facing side of this Edge pool server for **SIP Access**. In **Web Conferencing**, type the IP address that you have chosen for your public facing side of this Edge pool server. In **A/V Conferencing**, type the IP address you have chosen for your public facing side of this Edge pool server.
13. Click **Next**.
14. If you chose to enable IPv6 addresses, In **Define the external IP addresses**, do the following:
    - If you chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Edge service, type the external IPv6 address of the Edge Server in **SIP Access**.
    - If you did not chose to use a single FQDN and IP Address for the SIP access, Web Conferencing service, and A/V Conferencing service, type the

IPv6 address that you have chosen for your public facing side of this Edge pool server for **SIP Access**. In **Web Conferencing**, type the IPv6 address that you have chosen for your public facing side of this Edge pool server. In **A/V Conferencing**, type the IPv6 address you have chosen for your public facing side of this Edge pool server.

> **Note:**
> If you did not choose to enable and assign IPv6 addressing, you will not see this dialog box.

15. Click **Finish**.

> **Note:**
> You will now see the first Edge Server you created in your pool in the **Define the computers in this pool** dialog box.

16. In **Define the computers in this pool**, click **Add**, and then repeat steps 11 through 14 for the second Edge Server that you want to add to your Edge pool.
17. After you repeat steps 11 through 14, click **Next** in **Define the computers in this pool**.

> **Note:**
> At this point, you can see both of the Edge Servers in your pool.

18. In **Define the next hop**, in the **Next hop pool** list, select the name of the internal pool, which can be either a Front End pool or a Standard Edition pool. Or, if your deployment includes a Director, select the name of the Director. Then, click **Next**.
19. In **Associate Front End pools**, specify one or more internal pools, which can include Front End pools and Standard Edition servers, to be associated with this Edge Server, by selecting the names of the internal pool(s) that is to use this Edge Server for communication with supported external users.

> **Note:**
> Only one load-balanced Edge pool or single Edge Server can be associated with each internal pool for A/V traffic. If you already have an internal pool associated with an Edge pool or Edge Server, a warning appears indicating that the internal pool is already associated an Edge pool or Edge Server. If you select a pool that is already associated with another Edge Server, it will change the association.

20. Click **Finish**.

21. Publish your topology.

1.4.2.4.2 Define Optional Director Topologies in Your Topology

Define Optional Director Topologies in Your Topology

Deployment > Deploying External User Access > Building an Edge and Director Topology >

Topic Last Modified: *2012-09-08*

Lync Server 2013 Directors can be single-instance servers or they can be installed as a load-balanced pool of multiple Directors for higher availability and capacity. Both hardware load balancing and Domain Name System (DNS) load balancing are supported. This topic explains how to configure DNS load balancing for Director pools.

To successfully publish, enable, or disable a topology when you add or remove a server role, you should be logged on as a user who is a member of the **RTCUniversalServerAdmins** and **Domain Admins** groups. You can also delegate the proper administrator rights and permissions for adding server roles. For details, see Delegate Setup Permissions in the Standard Edition server or Enterprise Edition server Deployment documentation. For other configuration changes, only membership in the **RTCUniversalServerAdmins** group is required.

This topic describes the steps to define and publish the topology for the two Director topologies:

- To define the Director (single instance)
- To define the Director (multiple Director pool)

⊟To define the Director (single instance)

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. On the welcome page, click **Download Topology from Existing Deployment**.
3. In the **Save Topology As** dialog box, type the name and location of the local copy of the existing topology, and then click **Save**.
4. Expand the site in which you plan to add the Director, right-click **Director pools**, and then click **New Director Pool**.
5. In the **Define the Director pool FQDN** dialog box, do the following:
   - In **Pool FQDN**, type the FQDN for the Director pool.
   - Click **Single computer pool**, and then click **Next**.
6. In the **Define the file share** dialog box, do one of the following:
   - To use an existing file share, click **Use a previously defined file share**, select a file share from the list, and then click **Next**.
   - To create a new file share, click **Define a new file share**, type the FQDN for the location of the file share in **File Server FQDN**, type the name of the share in **File Share**, and then click **Next**.

   Important:

   The file share that you specify or create in this step must exist or be created prior to publishing the topology.

   The file share assigned to a Director is not actually used, so you can assign the file share of any pool in the organization.
7. In the **Specify the Web Services URL** dialog box, in **External Base URL**, specify the FQDN for the Directors, and then click **Finish**.

   Important:

   The name must be resolvable from Internet DNS servers and point to the public IP address of the reverse proxy, which listens for HTTP/HTTPS requests to that URL and proxies them to the external Web Services virtual directory on that Director.

   ⚠Warning:

   If you have more than one Front End pool or Front End Server the external Web services FQDN must be unique. For example, if you define the external Web services FQDN of a Front End Server as **pool01.contoso.com**, you cannot use **pool01.contoso.com** for another Front End pool or Front End Server. If you are also deploying Directors, the external Web services FQDN defined for any Director or Director pool must be unique from any other Director or Director pool as well as any Front End pool or Front End Server. If decide to override the Internal web services with a self-defined FQDN, each FQDN must be unique from any other Front End pool, Director or a Director pool.
8. Publish the topology.

⊟To define the Director (multiple Director pool)

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.

2. On the welcome page, click **Download Topology from Existing Deployment**.
3. In the **Save Topology As** dialog box, type the name and location of the local copy of the existing topology, and then click **Save**.
4. Expand the site in which you plan to add the Director, right-click **Director pools**, and then click **New Director Pool**.
5. In the **Define the Director pool FQDN** dialog box, do the following:
   - In **Pool FQDN**, type the FQDN for the Director pool.
   - Click **Multiple computer pool**, and then click **Next**.
6. In the **Define the computers in this pool** dialog box, do the following:
   - Specify the computer FQDN of the first pool member, and then click **Add**.
   - Repeat the previous step for each computer that you want to add. When you are finished, click **Next**.
7. In the **Define the file share** dialog box, do one of the following:
   - To use an existing file share, click **Use a previously defined file share**, select a file share from the list, and then click **Next**.
   - To create a new file share, click **Define a new file share**, type the FQDN for the location of the file share in **File Server FQDN**, type the name of the share in **File Share**, and then click **Next**.

> **Important:**
>
> The file share that you specify or create in this step must exist or be created prior to publishing the topology.
>
> The file share assigned to a Director is not actually used, so you can assign the file share of any pool in the organization.

8. In the **Specify the Web Services URL** dialog box, in **External Base URL**, specify the FQDN for the Directors, and then click **Finish**.

> **Important:**
>
> The name must be resolvable from Internet DNS servers and point to the public IP address of the reverse proxy, which listens for HTTP/HTTPS requests sent to that URL and proxies them to the external Web Services virtual directory on that Director pool.

> **Warning:**
>
> If you have more than one Front End pool or Front End Server the external Web services FQDN must be unique. For example, if you define the external Web services FQDN of a Front End Server as **pool01.contoso.com**, you cannot use **pool01.contoso.com** for another Front End pool or Front End Server. If you are also deploying Directors, the external Web services FQDN defined for any Director or Director pool must be unique from any other Director or Director pool as well as any Front End pool or Front End Server. If decide to override the Internal web services with a self-defined FQDN, each FQDN must be unique from any other Front End pool, Director or a Director pool.

9. Publish the topology.

1.4.2.4.3 Publish Your Topology

Publish Your Topology

Deployment > Deploying External User Access > Building an Edge and Director Topology >

Topic Last Modified: *2012-09-08*

Each time you use Topology Builder to build your topology, you must publish the topology to a database in the Central Management store so that the data can be used to deploy Lync Server 2013. Use the following procedure to publish your topology.

⊟To publish the topology

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In Topology Builder, in the console tree, right-click **Lync 2013**, and then click **Publish Topology**.
3. On the **Welcome** page of the wizard, click **Next**.
4. On the **Topology Builder found a CMS store** page, click **Next**.
5. On the **Create other databases** page, click **Next**.
6. When the status indicates that database creation succeeded, do the following:
   - To view the log, click **View log**.
   - To close the wizard, click **Finish**.

Important:

If this is a new installation of an Edge Server or Edge pool, you must export the Edge Server configuration from an existing Front End Server, Front End pool, or Standard Edition server. To export the configuration, see Export Your Topology and Copy It to External Media for Edge Installation. You will import the configuration file from the external media or network share during the setup and deployment phase of the Edge Servers through the Lync Server Deployment Wizard.

Once the Edge Servers are operational and the local configuration management store database is replicating with the internal deployment, subsequent updates to the Lync Server 2013 configuration will be published and replicated to the Edge Servers.

1.4.2.4.4 Export Your Topology and Copy It to External Media for Edge Installation

Export Your Topology and Copy It to External Media for Edge Installation

Deployment > Deploying External User Access > Building an Edge and Director Topology >

Topic Last Modified: *2012-09-08*

After you publish your topology, the Lync Server Deployment Wizard needs access to the Central Management store data in order to start the deployment process on the server. In the internal network, the data is available directly from the servers, but Edge Servers that are not in the internal domain cannot access the data. To make the topology configuration data available for an Edge Server deployment, you must export the topology data to a file and copy it to external media (for example, a USB drive or a network share that is available from the Edge Server) before you run the Lync Server Deployment Wizard on the Edge Server. Use the following procedure to make your topology configuration data available on the Edge Server that you are deploying.

Note:

After you install Lync Server 2013 on an Edge Server, you manage the Edge Server using the administrative tools in the internal network, which automatically replicate configuration to any Edge Servers in your deployment. The only exception is assigning and installing certificates and stopping and starting services, both of which must be done on the Edge Server.

⊟To make your topology data available on an Edge Server by using Lync Server Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. In the Lync Server Management Shell, run the following cmdlet:

```
Export-CsConfiguration -FileName <ConfigurationFilePath.zip>
```

3. Copy the exported file to external media (for example, a USB drive or a network share that is available from the Edge Server during deployment).

1.4.2.5 Setting Up the Director

Setting Up the Director

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2012-09-08*

If you enable access for external users by deploying Edge Servers, you optionally can deploy a Director. A Director is a server running Microsoft Lync Server 2013 that authenticates user requests, but does not home any user accounts. The primary steps required to setting up a Director or Director pool are similar to that of setting up an Enterprise Edition Front End pool or Standard Edition server. After you have defined your Director(s) in Topology Builder, you need to perform the steps in this section.

- Install the Local Configuration Store
- Install Lync Server 2013 on the Director
- Configure Certificates for the Director
- Start Services on the Director
- Test the Director
- Configure Automatic Client Sign-In To Use the Director

1.4.2.5.1 Install the Local Configuration Store

Install the Local Configuration Store

Deployment > Deploying Lync Server 2013 > Setting Up Front End Servers and Front End Pools >

Topic Last Modified: *2013-02-25*

To successfully complete this procedure, you should be logged on to the server minimally as a local administrator and a domain user who has membership in at least the RTCUniversalReadOnlyAdmin group.

The first step of the Lync Server Deployment Wizard is to install the Local Configuration store. The Local Configuration store is SQL Server Express, which installs a local database that will retain a read-only copy of the Central Management store. The Central Management store is added to the existing SQL Server database installed on the Standard Edition server or SQL Server Express-based database.

◆**Important:**
If this is the first time that you have run Lync Server 2013 setup on this server, you will be prompted for a drive and path to install Lync Server 2013. If your organization requires that you locate Internet Information Services (IIS) and all Web Services on a drive other than the system drive, you can change the installation location path for the Lync Server files in the Setup dialog box. If you install the Setup files to this path, including OCSCore.msi, the rest of the Lync Server 2013 files will be deployed to this drive as well.

⊟To install the Local Configuration store

1. From the installation media, browse to \setup\amd64\Setup.exe, and then click **OK**.
2. If you are prompted to install the Microsoft Visual C++ 2012 Redistributable, click **Yes**.
3. On the **Lync Server 2013 Installation Location** page, click **OK**.
4. On the **End User License Agreement** page, review the license terms, select **I accept the terms in the license agreement**, and then click **OK**. This step is required before you can continue.
5. On the Deployment Wizard page, click **Install or Update Lync Server System**.
6. On the **Lync Server 2013** page, next to **Step1: Install Local Configuration Store**, click **Run**.
7. On the **Local Server Configuration** page, make sure that the **Retrieve configuration automatically from the Central Management Store** option is selected, and then click **Next**.
8. When the local server configuration installation is complete, click **Finish**.

1.4.2.5.2 Install Lync Server 2013 on the Director

Install Lync Server 2013 on the Director

Deployment > Deploying External User Access > Setting Up the Director >

Topic Last Modified: *2012-09-08*

Use the following steps to install the Lync Server 2013 components on a Director.

⊟To install Lync Server components on a Director

1. In the Lync Server Deployment Wizard, on the Lync Server 2013 page, next to **Step 2: Setup or Remove Lync Server Components**, click **Run**.
2. On the **Setup Lync Server components** page, click **Next** to set up components as defined in the published topology.
3. When Lync Server components setup has completed, click **Finish**.

1.4.2.5.3 Configure Certificates for the Director

Configure Certificates for the Director

Deployment > Deploying External User Access > Setting Up the Director >

Topic Last Modified: *2012-09-08*

Important:
When you run the Certificate Wizard, ensure that you are logged in using an account that is a member of a group that has been assigned the appropriate permissions for the type of certificate template you will use. By default, a Lync Server 2013 certificate request will use the Web Server certificate template. If you use an account that is a member of the RTCUniversalServerAdmins group to request a certificate using this template, verify that the group has been assigned the Enroll permissions required to use that template.

Each Director requires a default certificate, a web internal certificate, and a web external certificate. For details about the certificate requirements for Directors, see Certificate Requirements for Internal Servers in the Planning documentation.

Use the following procedure to configure Director certificates. Repeat the procedure for each Director. The steps of this procedure describe how to configure a certificate from an Internal Enterprise Root certification authority (CA) deployed by your organization and with offline request processing. For details about obtaining certificates from an external CA, contact your support team.

⊟To configure certificates for the Director or Director pool

1. In the Lync Server Deployment Wizard, next to **Step 3: Request, Install or Assign Certificates**, click **Run**.
2. On the **Certificate Wizard** page, click **Request**.
3. On the **Certificate Request** page, click **Next**.
4. On the **Delayed or Immediate Requests** page, accept the default **Send the request immediately to an online certification authority** option, and then click **Next**.
5. On the **Choose a Certification Authority (CA)** page, click the internal Windows certification authority that you want to use, and then click **Next**.
6. On the **Certification Authority Account** page, specify alternate credentials to be used if the account you are logged on with does not have sufficient authority to request the certificate, and then click **Next**.
7. On the **Specify Alternate Certificate Template** page, click **Next**.
8. On the **Name and Security Settings** page, you can specify a **Friendly Name**, accept the 2048-bit key length, and then click **Next**.
9. On the **Organization Information** page, optionally specify organization information, and then click **Next**.
10. On the **Geographical Information** page, optionally specify geographical information, and then click **Next**.
11. On the **Subject Name / Subject Alternative Names** page, click **Next**.

> **Note:**
> The subject alternative name list should contain the name of the computer on which you are installing the Director (if a single Director) or the Director pool name, and the simple URL names configured for the organization.

12. On the **SIP Domain Setting on Subject Alternate Names (SANs)** page, select the **Configured SIP Domains** for all domains that you want the Director to handle, and then click **Next**.
13. On the **Configure Additional Subject Alternative Names** page, add any additional required subject alternative names, and then click **Next**.
14. On the **Certificate Request Summary** page, click **Next**.
15. On the **Executing Commands** page, click **Next** after the commands have finished running.
16. On the **Online Certificate Request Status** page, click **Finish**.
17. On the **Certificate Assignment** page, click **Next**.

> **Note:**
> if you want to view the certificate, double-click the certificate in the list.

18. On the **Certificate Assignment Summary** page, click **Next**.
19. On the **Executing Commands** page, click **Finish** after the commands have finished running.
20. On the **Certificate Wizard** page, click **Close**.

1.4.2.5.4 Start Services on the Director

Start Services on the Director

Deployment > Deploying External User Access > Setting Up the Director >

Topic Last Modified: *2012-09-08*

After you install the Local Configuration Store, install the Lync Server Components, and configure certificates on a Director, you must start the Lync Server services on the server. You can use the following procedure to start services on each Director in your deployment.

To start services on a Director

1. In the Lync Server Deployment Wizard, on the **Lync Server 2013** page, click the **Run** button next to **Step 4: Start Services**.
2. On the **Start Services** page, click **Next** to start the Lync Server services on the server.
3. On the **Executing Commands** page, after all services have started successfully, click **Finish**.
4. Below **Step 4: Start Services**, click **Services Status (Optional)**.
5. In the **Services** Microsoft Management Console (MMC) on the server, verify that all of the Lync Server 2013 services are running.

1.4.2.5.5 Test the Director

Test the Director

Deployment > Deploying External User Access > Setting Up the Director >

Topic Last Modified: *2012-09-08*

At this stage, you have a Director or Director pool configured, but your Domain Name System (DNS) SRV entries still point clients to log on by using a pool or Standard Edition server. Before changing the DNS record to make Lync 2013 clients log on automatically by using the Director, test a client by manually pointing it to the Director.

To test the deployment

1. Log on to the computer on which you have the Lync Server Control Panel installed with a domain account that is part of the **CSAdministrator** group.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the navigation pane, click **Topology**, and in the **Status** column confirm that there is a green server with an arrow (that is,) for your Director or Director pool.
4. Connect two client computers that have the Lync Server 2013 client installed and log on with a different user account enabled for Lync Server 2013 to each computer.
5. On one of the client computers, click the **Options** menu, select the **Personal** settings group, click **Advanced**, click **Manual Configuration**, and then set the **Internal Server name or IP address** to the fully qualified domain name (FQDN) of the new Director or Director pool.
6. Log on to both clients and verify that the client logging on by using the Director is able to log on successfully, see the presence status of the other user, and that they can exchange instant messages.

1.4.2.5.6 Configure Automatic Client Sign-In To Use the Director

Configure Automatic Client Sign-In To Use the Director

Deployment > Deploying External User Access > Setting Up the Director >

Topic Last Modified: *2012-09-08*

When you deploy a Lync Server 2013, Director or a pool of Directors, we recommend that you use Automatic Client Sign-In as a best practice. For details about how to configure DNS servers for automatic client sign-in, see DNS Requirements for Automatic Client Sign-

In in the Planning documentation.

If you have already deployed Automatic Client Sign-In, see the following sections to configure it on your Director(s).

Single Director Instance

If you already have Automatic Client Sign-In deployed and it is pointing to a Front End Server or a Front End pool, you need to change the DNS SRV record to point to the Director.

Director Pool

If you already have Automatic Client Sign-In deployed and it is pointing to a Front End Server or a Front End pool, you need to change the DNS SRV record to point to the Director pool.

1.4.2.6 Setting Up Edge Servers

Setting Up Edge Servers

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

***Topic Last Modified:** 2012-09-08*

The primary tasks required to set up Edge Servers are the same for installing a single Edge Server or a load-balanced pool of Edge Servers, except that a pool of hardware load balanced Edge Servers requires deployment of the load balancers and additional steps for replicating the set up on multiple Edge Servers.

- Set Up Network Interfaces for Edge Servers
- Install Prerequisite Software on Edge Servers
- Export Your Topology and Copy It to External Media for Edge Installation
- Install Edge Servers
- Set Up Edge Certificates
- Start Edge Servers
- Setting Up Reverse Proxy Servers

1.4.2.6.1 Set Up Network Interfaces for Edge Servers

Set Up Network Interfaces for Edge Servers

Deployment > Deploying External User Access > Setting Up Edge Servers >

***Topic Last Modified:** 2012-09-08*

Each Edge Server is a multihomed computer with external and internal facing interfaces. The adapter Domain Name System (DNS) settings depend on whether there are DNS servers in the perimeter network. If DNS servers exist in the perimeter, they must have a zone containing one or more DNS A records for the next hop server or pool (that is, either a Director or a designated Front End pool), and for external queries they refer name lookups to other public DNS servers. If no DNS servers exist in the perimeter, the Edge Server(s) use external DNS servers to resolve Internet name lookups, and each Edge Server uses a HOST to resolve the next hop server names to IP addresses.

Security Note:

For security reasons, we recommend that you do not have your Edge Servers access a DNS server located in the internal network.

⊟To configure interfaces with DNS servers in the perimeter network

1. Install two network adapters for each Edge Server, one for the internal-facing interface and one for the external-facing interface.

   Important:

   The internal and external subnets must not be routable to each other.

2. On the external interface, configure three static IP addresses on the external perimeter network (also known as DMZ, demilitarized zone, and screened subnet) subnet, and point the default gateway to the internal interface of the external firewall. Configure adapter DNS settings to point to a pair of perimeter DNS servers.

   Note:

   It is possible to use as few as one IP address for this interface, but to do this you need to change the port assignments to non-standard values. You determine this when you create the topology in Topology Builder.

3. On the internal interface, configure one static IP address on the internal perimeter network subnet and do not set a default gateway. Configure adapter DNS settings to point to at least one DNS server, preferably a pair of perimeter DNS servers.
4. Create persistent static routes on the internal interface to all internal networks where clients, Lync Server 2013, and Exchange Unified Messaging (UM) servers reside.

⊟To configure interfaces without DNS servers in the perimeter network

1. Install two network adapters for each Edge Server, one for the internal-facing interface and one for the external-facing interface.

   Important:

   The internal and external subnets must not be routable to each other.

2. On the external interface, configure three static IP addresses on the external perimeter network subnet. You also configure the default gateway on the external interface. For example, define the Internet-facing router or the external firewall as the default gateway. Configure DNS settings to point to a DNS server, preferably to a pair of external DNS servers.

   Note:

   It is possible, but not recommended, to use as few as one IP address for the external interface. To allow this to work, you need to change the port assignments to non-standard values, and away from the default port 443 that is typically "firewall friendly" for client communication. You determine the IP address setting and the port settings when you create the topology in Topology Builder.

3. On the internal interface, configure one static IP address on the internal perimeter network subnet and do not set a default gateway. Leave adapter DNS settings empty.
4. Create persistent static routes on the internal interface to all internal networks where Lync clients or servers running Lync Server 2013 reside.
5. Edit the HOST file on each Edge Server to contain a record for the next hop server or virtual IP (VIP) (the record will be the Director, Standard Edition server, or a Front End pool that was configured as the Edge Server next hop address in Topology Builder). If you are using DNS load balancing, include a line for each member of the next hop pool.

1.4.2.6.2 Install Prerequisite Software on Edge Servers

Install Prerequisite Software on Edge Servers

Deployment > Deploying External User Access > Setting Up Edge Servers >

Topic Last Modified: *2012-09-08*

You need to deploy prerequisite software on each Edge Server that you deploy prior to installing Lync Server 2013. This includes installing the operating system on a server that meets system requirements. For details about system requirements, including the supported operating systems, see System Requirements for External User Access Components.

1.4.2.6.3 Install Edge Servers

Install Edge Servers

Deployment > Deploying External User Access > Setting Up Edge Servers >

Topic Last Modified: *2012-09-08*

You install Lync Server 2013 on Edge Servers by using Lync Server Deployment Wizard. By running the Deployment Wizard on each Edge Server, you can complete most of the tasks required to set up the Edge Server. In order to deploy Lync Server 2013 on an Edge Server, you must have already run Topology Builder to define and publish your Edge Server topology, and exported it to media that is available from the Edge Server. For details, see Scenarios for External User Access and Export Your Topology and Copy It to External Media for Edge Installation.

After using the Deployment Wizard to install each Edge Server, install and assign the required certificates, and start the required services, you can complete the setup by using the information in Configuring Support for External User Access to enable and configure external user access and the information in Verifying Your Edge Deployment to validate the setup, including server and client connectivity.

⊟To install an Edge Server

1. Log on to the computer on which you want to install your Edge Server as a member of the local Administrators group or an account with equivalent user rights and permissions.
2. Ensure that the topology configuration file you created using Topology Builder, and then exported and copied to external media, is available on the Edge Server (for example, access to the USB drive onto which you copied the topology configuration file, or verify access to the network share where you copied the file).
3. Start the Deployment Wizard.

Note:
If you get a message saying that you need to install Microsoft Visual C++ Redistributable, click **Yes**. In the next dialog box, you can accept the default **Installation Location** or click the **Browse** to select an alternate location, and then click **Install**. In the next dialog box, select the **I accept the terms in the license agreement** check box, and then click **OK**.

4. In the Deployment Wizard, click **Install or Update Lync Server System**.
5. After the wizard determines the deployment state, for **Step 1. Install Local Configuration Store**, click **Run** and then do the following:
   - In the **Configure Local Replica of Central Management Store** dialog box, click **Import from a file (Recommended for Edge Servers)**, go to the

location of the exported topology configuration file, select the .zip file, click **Open**, and then click **Next**.
- The Deployment Wizard reads the configuration information from the configuration file and writes the XML configuration file to the local computer.
- After the **Executing Commands** process is finished, click **Finish**.

6. In the Deployment Wizard, click **Step 2: SetUp or Remove Lync Server Components** to install the Lync Server 2013 edge components specified in the XML configuration file that is stored on the local computer.
7. After completing the installation, use the information in Set Up Edge Certificates to install and assign the required certificates before you start services.

1.4.2.6.4 Set Up Edge Certificates

Set Up Edge Certificates

Deployment > Deploying External User Access > Setting Up Edge Servers >

Topic Last Modified: *2012-09-08*

When you install an Edge Server, you need to request, install, and assign the required certificates for the internal and external interfaces.

- Certificate Requirements for External User Access
- Set Up Certificates for the Internal Edge Interface
- Set Up Certificates for the External Edge Interface
- Set Up Certificates for the Reverse Proxy

1.4.2.6.4.1 Certificate Requirements for External User Access

Certificate Requirements for External User Access

See Also

Planning > Determining Your Infrastructure Requirements > Certificate Infrastructure Requirements >

Topic Last Modified: *2012-09-08*

Microsoft Lync Server 2013 communications software supports the use of a single public certificate for access and web conferencing Edge external interfaces, plus the A/V Authentication service. The Edge internal interface typically uses a private certificate issued by an internal certification authority (CA), but can also use a public certificate, provided that it is from a trusted public CA. The reverse proxy in your deployment uses a public certificate and encrypts the communication from the reverse proxy to clients and the reverse proxy to internal servers by using HTTP (that is, Transport Layer Security over HTTP).

Following are the requirements for the public certificate used for access and web conferencing Edge external interfaces, and the A/V authentication service:

- The certificate must be issued by an approved public CA that supports subject alternative name. For details, see Microsoft Knowledge Base article 929395, "Unified Communications Certificate Partners for Exchange Server and for Communications Server," at http://go.microsoft.com/fwlink/p/?linkId=202834.
- If the certificate will be used on an Edge pool, it must be created as exportable, with the same certificate used on each Edge Server in the Edge pool. The exportable private key requirement is for the purposes of the A/V Authentication service, which must use the same private key across all Edge Servers in the pool.
- If you want to maximize the uptime for your Audio/Video services, review the

certificate requirements for implementing a decoupled A/V Edge service certificate (that is, a separate A/V Edge service certificate from the other External Edge certificate purposes). For details, see Changes in Lync Server 2013 That Affect Edge Server Planning, Plan for Edge Server Certificates and Staging AV and OAuth Certificates Using -Roll in Set-CsCertificate.

- The subject name of the certificate is the Access Edge service external interface fully qualified domain name (FQDN) or hardware load balancer VIP (for example, access.contoso.com).

  > **Note:**
  > For Lync Server 2013, this is no longer a requirement, but it is still recommended for compatibility with Office Communications Server.

- The subject alternative name list contains the FQDNs of the following:
  - The Access Edge service external interface or hardware load balancer VIP (for example, sip.contoso.com).

    > **Note:**
    > Even though the certificate subject name is equal to the access Edge FQDN, the subject alternative name must also contain the access Edge FQDN because Transport Layer Security (TLS) ignores the subject name and uses the subject alternative name entries for validation.

  - The web conferencing Edge external interface or hardware load balancer VIP (for example, webcon.contoso.com).
  - If you are using client auto-configuration or federation, also include any SIP domain FQDNs used within your company (for example, sip.contoso.com, sip.fabrikam.com).
  - The A/V Edge service does not use the subject name or the subject alternative names entries.

  > **Note:**
  > The order of the FQDNs in the subject alternative names list does not matter.

If you are deploying multiple, load-balanced Edge Servers at a site, the A/V authentication service certificate that is installed on each Edge Server must be from the same CA and must use the same private key. Note that the certificate's private key must be exportable, regardless of whether it is used on one Edge Server or many Edge Servers. It must also be exportable if you request the certificate from any computer other than the Edge Server. Because the A/V authentication service does not use the subject name or subject alternative name, you can reuse the access Edge certificate as long as the subject name and subject alternative name requirements are met for the access Edge and the web conferencing Edge and the certificate’s private key is exportable.

Requirements for the private (or public) certificate used for the Edge internal interface are as follows:

- The certificate can be issued by an internal CA or an approved public certificate CA.
- The subject name of the certificate is typically the Edge internal interface FQDN or hardware load balancer VIP (for example, lsedge.contoso.com). However, you can use a wildcard certificate on the Edge internal.
- No subject alternative name list is required.

The reverse proxy in your deployment services requests for:

- External user access to meeting content for meetings
- External user access to expand and display members of distribution groups
- External user access to downloadable files from the Address Book Service
- External user access to the Lync Web App client
- External user access to the Dial-in Conferencing Settings web page
- External user access to the Location Information Service

- External device access to the Device Update Service and obtain updates

The reverse proxy publishes the internal server Web Components URLs. The Web Components URLs are defined on the Director, Front End Server or Front End pool as the **External web services** in Topology Builder.

Wildcard entries are supported in the subject alternative name field of the certificate assigned to the reverse proxy. For details about how to configure the certificate request for the reverse proxy, see Request and Configure a Certificate for Your Reverse HTTP Proxy.

Concepts

Wildcard Certificate Support

1.4.2.6.4.2 Set Up Certificates for the Internal Edge Interface

Set Up Certificates for the Internal Edge Interface

Deploying External User Access > Setting Up Edge Servers > Set Up Edge Certificates >

Topic Last Modified: *2012-09-08*

Important:

When you run the Certificate Wizard, ensure that you are logged in using an account that is a member of a group that has been assigned the appropriate permissions for the type of certificate template you will use. By default, a Lync Server 2013 certificate request will use the Web Server certificate template. If you use an account that is a member of the RTCUniversalServerAdmins group to request a certificate using this template, verify that the group has been assigned the Enroll permissions required to use that template.

A single certificate is required on the internal interface of each Edge Server. Certificates for the internal interface can be issued by an internal enterprise certification authority (CA) or a public CA. If your organization has an internal CA deployed you can save on the expense of using public certificates by using the internal CA to issue the certificate for the internal interface. You can use an internal Windows Server 2008 CA or Windows Server 2008 R2 CA to create these certificates.

For details about this and other certificate requirements, see Certificate Requirements for External User Access.

To set up certificates on the internal edge interface at a site, use the procedures in this section to do the following:

1. Download the CA certification chain for the internal interface to each Edge Server.
2. Import the CA certification chain for the internal interface, on each Edge Server.
3. Create the certificate request for the internal interface, on one Edge Server, called the first Edge Server.
4. Import the certificate for the internal interface on the first Edge Server.
5. Import the certificate on the other Edge Servers at this site (or deployed behind this load balancer).
6. Assign the certificate for the internal interface of every Edge Server.

If you have more than one site with Edge Servers (that is, a multiple-site edge topology), or separate sets of Edge Servers deployed behind different load balancers, you need to follow these steps for each site that has Edge Servers, and for each set of Edge Servers deployed behind a different load balancer.

Note:

The steps for procedures in this section are based on using a Windows Server 2008 CA Windows Server 2008 R2 CA or Windows Server 2012 CA to create a certificate for each Edge Server. For step-by-step guidance for any other CA, consult the documentation for that CA. By default, all authenticated users have the appropriate user rights to request certificates.

The procedures in this section are based on creating certificate requests on the Edge Server as part of the Edge Server deployment process. It is possible to create certificate requests using the Front End Server. You can do this to complete the certificate request early in the planning and deployment process, before you start deployment of the Edge Servers. To do this, you must ensure that the certificate you request is defined with an exportable private key.

The procedures in this section describe using a .cer and a .p7b file for the certificate. If you use a different type of file, modify these procedures as appropriate.

⊟To download the CA certification chain for the internal interface using certsrv Web site

1. Log on to an Lync Server 2013 server in the internal network (that is, not the Edge Server) as a member of the **Administrators** group.
2. Run the following command at a command prompt by clicking **Start**, clicking **Run**, and then typing the following:

   ```
   https://<name of your Issuing CA Server>/certsrv
   ```

   For example:

   ```
   https://ca01.contoso.net/certsrv
   ```

   Note:

   If you are using a Windows Server 2008 or Windows Server 2008 R2 enterprise CA, you must use https, not http.
3. On the issuing CA's certsrv web page, under **Select a task**, click **Download a CA certificate, certificate chain, or CRL**.
4. Under **Download a CA Certificate, Certificate Chain, or CRL**, click **Download CA certificate chain**.
5. In the **File Download** dialog box, click **Save**.
6. Save the .p7b file to the hard disk drive on the server, and then copy it to a folder on each Edge Server.

   Note:

   The .p7b file contains all of the certificates that are in the certification path. To view the certification path, open the server certificate and click the certification path.

⊟To export the CA certification chain for the internal interface using MMC

1. You can export the CA root certificate from any domain joined machine using the Microsoft Management Console (MMC). Click **Start**, click **Run**, and then type **MMC**.
2. In the MMC console, click **File**, click **Add/Remove**.
3. From the **Add or Remove Snap-ins** dialog list, select **Certificates**, then click **Add**. When prompted, select **Computer Account**. On the **Select Computer** dialog, select **Local Computer**. Click **Finish**. Click **OK**.
4. Expand **Certificates (Local Computer)**. Expand **Trusted Root Certification Authorities**, select **Certificates**.
5. Click the root certificate issued by your CA. Right click the certificate, select **All Tasks**, select **Export**. The **Certificate Export Wizard** will open.
6. In the **Certificate Export Wizard**, click **Next**.
7. On the **Export File Format** dialog, select a format to export to. We recommend the **Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**. If you select the **Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**, select the **Include all certificates**

in the certification path if possible checkbox to export the certificate chain, including the root CA certificate and any Intermediate CA certificates. Click **Next**.

8. On the **File to Export** dialog in the file name entry, type a path and file name (default extension is .p7b) for the exported certificate. Optionally, click **Browse**, locate a directory to place the exported certificate in and provide a name for the exported certificate. Click **Save**. Click **Next**.
9. Review the summary of actions, and click **Finish** to complete the export of the certificate. Click **OK** to confirm the successful export.

⊟To import the CA certification chain for the internal interface

1. On each Edge Server, open the Microsoft Management Console (MMC) by clicking **Start**, clicking **Run**, typing **mmc** in the **Open** box, and then clicking **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In the **Add Standalone Snap-ins** box, click **Certificates**, and then click **Add**.
4. In the **Certificate snap-in** dialog box, click **Computer account**, and then click **Next**.
5. In the **Select Computer** dialog box, ensure that the **Local computer: (the computer this console is running on)** check box is selected, and then click **Finish**.
6. Click **Close**, and then click **OK**.
7. In the console tree, expand **Certificates (Local Computer)**, right-click **Trusted Root Certification Authorities**, point to **All Tasks**, and then click **Import**.
8. In the wizard, in **File to Import**, specify the file name of the certificate (that is, the name of that you specified when you downloaded the CA certification chain for the internal interface in the previous procedure).
9. Repeat this procedure on each Edge Server.

⊟To create the certificate request for the internal interface

1. On one of the Edge Servers, start the Deployment Wizard, and next to **Step 3: Request, Install, or Assign Certificates**, click **Run**.

Note:
If you have multiple Edge Servers in one location in a pool, you can run the Certificate Wizard on any one of the Edge Servers. After you run Step 3 the first time, the button changes to **Run again**, and a green check mark that indicates successful completion of the task is not displayed until all require certificates have been requested, installed, and assigned.

2. On the **Available Certificate Tasks** page, click **Create a new certificate request**.
3. On the **Certificate Request** page, click **Next**.
4. On the **Delayed or Immediate Requests** page, click **Prepare the request now, but send it later**.
5. On the **Certificate Request File** page, type the full path and file name to which the request is to be saved (for example, **c:\cert_internal_edge.cer**).
6. On the **Specify Alternate Certificate Template** page, to use a template other than the default WebServer template, select the **Use alternative certificate template for the selected Certificate Authority** check box.
7. On the **Name and Security Settings** page, do the following:
   - In **Friendly name**, type a display name for the certificate (for example, Internal Edge).
   - In **Bit length**, specify the bit length (typically, the default of **2048**).

Note:
Higher bit lengths offer more security, but they have a negative impact on speed.

   - If the certificate needs to be exportable, select the **Mark certificate**

private key as exportable check box.

8. On the **Organization Information** page, type the name for the organization and the organizational unit (OU) (for example, a division or department).
9. On the **Geographical Information** page, specify the location information.
10. On the **Subject Name/Subject Alternate Names** page, the information to be automatically populated by the wizard is displayed.
11. On the **Configure Additional Subject Alternate Names** page, specify any additional subject alternative names that are required.
12. On the **Request Summary** page, review the certificate information that is going to be used to generate the request.
13. After the commands complete, do the following:
    - To view the log for the certificate request, click **View Log**.
    - To complete the certificate request, click **Next**.
14. On the **Certificate Request File** page, do the following:
    - To view the generated certificate signing request (CSR) file, click **View**.
    - To close the wizard, click **Finish**.
15. Submit this file to your CA (by email or other method supported by your organization for your enterprise CA) and, when you receive the response file, copy the new certificate to this computer so that it is available for import.

⊟To import the certificate for the internal interface

1. Log on to the Edge Server on which you created the certificate request as a member of the local Administrators group.
2. In the Deployment Wizard, next to **Step 3: Request, Install, or Assign Certificates**, click **Run again**.

   After you run Step 3 the first time, the button changes to **Run again**, but a green check mark (indicating successful completion of the task) is not displayed until all require certificates have been requested, installed, and assigned.
3. On the **Available Certificate Tasks** page, click **Import a certificate from a .P7b, .pfx or .cer file**.
4. On the **Import Certificate** page, type the full path and file name of the certificate that you requested and received for the internal interface of this Edge Server (or, click **Browse** to locate and select the file).
5. If you are importing certificates for other members of the pool a certificate containing a private key, select the **Certificate file contains certifcate's private key** check box and specify the password.

⊟To export the certificate with the private key for Edge Servers in a pool

1. Log on as a member of the Administrators group to the same Edge Server on which you imported the certificate.
2. Click **Start**, click **Run**, and type **MMC**.
3. From the MMC console, click **File**, click **Add/Remove Snap-in**.
4. From Add or Remove Snap-ins page, click **Certificates**, click **Add**.
5. In the Certificates snap-in dialog, select **Computer account**. Click **Next**. In Select Computer, select **Local computer: (the computer this console is running on)**. Click **Finish**. Click **OK** to complete configuration of the MMC console.
6. Double-click **Certificates (Local Computer)** to expand the certificate stores. Double-click **Personal**, then double-click **Certificates**.

   Important:

   If there are no certificates in the Certificates Personal store for the local computer, there is no private key associated with the certificate that was imported. Review the request and import steps. If the problem persists, contact your certification authority administrator or provider.
7. In the Certificates Personal store for the local computer, right-click the certificate that you are exporting. Click **All Tasks**, click **Export**.
8. In the Certificate Export Wizard, click **Next**. Select **Yes, export the private**

key. Click **Next**.

> **Note:**
>
> If the selection **Yes, export the private key** is not available, the private key associated with this certificate was not marked for export. You will need to request the certificate again, ensuring that the certificate is marked to allow for the export of the private key before you can continue with the export. Contact your certification authority administrator or provider.

9. On the Export File Formats dialog, select **Personal Information Exchange – PKCS#12 (.PFX)** and then select the following:
   - Include all certificates in the certification path if possible
   - Export all extended properties

   > **Warning:**
   >
   > When exporting the certificate from an Edge server, do not select **Delete the private key if the export is successful**. Selecting this option will require that you import the certificate and the private key to this Edge server.

   Click **Next** to continue.
10. If you want to assign password to protect the private key, type a password for the private key. Re-enter the password to confirm. Click **Next**.
11. Type a path and file name for the exported certificate, using a file extension of .pfx. The path must either be accessible to all other Edge servers in the pool or available to transport by means of removable media - for example, a USB flash drive. Click **Next**.
12. Review the summary on the Completing the Certificate Export Wizard dialog. Click **Finish**.
13. Click **OK** in the successful export dialog.
14. Import the exported certificate file to the other Edge servers following the steps outlined in the Set Up Certificates for the External Edge Interface procedures.

⊟To assign the internal certificate on the Edge Servers

1. On each Edge Server, in the Deployment Wizard, next to **Step 3: Request, Install, or Assign Certificates**, click **Run again**.
2. On the **Available Certificate Tasks** page, click **Assign an existing certificate**.
3. On the **Certificate Assignment** page, select **Edge Internal** in the list.
4. On the **Certificate Store** page, select the certificate that you imported for the internal edge (from the previous procedure).
5. On the **Certificate Assignment Summary** page, review your settings, and then click **Next** to assign the certificates.
6. On the wizard completion page, click **Finish**.
7. After using this procedure to assign the internal edge certificate, open the Certificate snap-in on each server, expand **Certificates (Local computer)**, expand **Personal**, click **Certificates**, and then verify in the details pane that the internal edge certificate is listed.
8. If your deployment includes multiple Edge Servers, repeat this procedure for each Edge Server.

1.4.2.6.4.3 Set Up Certificates for the External Edge Interface

Set Up Certificates for the External Edge Interface

Deploying External User Access > Setting Up Edge Servers > Set Up Edge Certificates >

Topic Last Modified: *2012-09-08*

> **Important:**

When you run the Certificate Wizard, ensure that you are logged in using an account that is a member of a group that has been assigned the appropriate permissions for the type of certificate template you will use. By default, a Lync Server certificate request will use the Web Server certificate template. If you use an account that is a member of the RTCUniversalServerAdmins group to request a certificate using this template, verify that the group has been assigned the Enroll permissions required to use that template.

Each Edge Server requires a public certificate on the interface between the perimeter network and the Internet, and the certificate's subject alternative name must contain the external names of the Access Edge service and Web Conferencing Edge service fully qualified domain names (FQDNs).

For details about this and other certificate requirements, see Certificate Requirements for External User Access.

For a list of public certification authorities (CAs) that provide certificates that comply with specific requirements for unified communications certificates and have partnered with Microsoft to ensure they work with the Lync Server 2013 Certificate Wizard, see Microsoft Knowledge Base article 929395, "Unified Communications Certificate Partners for Exchange Server and for Communications Server," at http://go.microsoft.com/fwlink/p/?linkId=202834.

Configuring Certificates on the External Interfaces

To set up a certificate on the external edge interface at a site, use the procedures in this section to do the following:

- Create the certificate request for the external interface of the Edge Server.
- Submit the request to your public CA.
- Import the certificate for the external interface of each Edge Server.
- Assign the certificate for the external interface of each Edge Server.
- If your deployment includes multiple Edge Servers, export the certificate along with its private key, and then copy it to the other Edge Servers. Then, for each Edge Server, import it and assign it as previously described. Repeat this procedure for each Edge Server.

You can request public certificates directly from a public certification authority (CA) (such as from the website of a public CA). The procedures in this section use the Certificate Wizard for most certificate tasks. If you chose to request a certificate directly from a public CA, then you will need to modify each procedure as appropriate to request, transport, and import the certificate and also to import the certificate chain.

When you request a certificate from an External CA, the credentials provided must have rights to request a certificate from that CA. Each CA has a security policy that defines which credentials (that is, specific user and group names) are allowed to request, issue, manage, or read certificates.

If you decide to use the Certificates Microsoft Management Console (MMC) to import the certificate chain and certificate, you must import them to the certificate store for the computer. If you import them to the user or service certificate store, the certificate will not be available for assignment in the Lync Server 2013 Certificate Wizard.

⊟To create the certificate request for the external interface of the Edge Server

1. On the Edge Server, in the Deployment Wizard, next to **Step 3: Request, Install, or Assign Certificates**, click **Run again**.

   Note:

> If your organization wants to support public instant messaging (IM) connectivity with AOL, you cannot use the Lync Server Deployment Wizard to request the certificate. Instead, perform the steps in the “To create a certificate request for the external interface of the Edge Server to support public IM connectivity with AOL” procedure later in this topic.
> If you have multiple Edge Servers in one location in a pool, you can run the Lync Server 2013 Certificate Wizard on any one of the Edge Servers.

2. On the **Available Certificate Tasks** page, click **Create a new certificate request**.
3. On the **Certificate Request** page, click **External Edge Certificate**.
4. On the **Delayed or Immediate Request** page, select the **Prepare the request now, but send it later** check box.
5. On the **Certificate Request File** page, type the full path and file name of the file to which the request is to be saved (for example, c:\cert_exernal_edge.cer).
6. On the **Specify Alternate Certificate Template** page, to use a template other than the default WebServer template, select the **Use alternative certificate template for the selected certification authority** check box.
7. On the **Name and Security Settings** page, do the following:
   - In **Friendly name**, type a display name for the certificate.
   - In **Bit length**, specify the bit length (typically, the default of **2048**).
   - Verify that the **Mark certificate private key as exportable** check box is selected.
8. On the **Organization Information** page, type the name for the organization and the organizational unit (for example, a division or department).
9. On the **Geographical Information** page, specify the location information.
10. On the **Subject Name/Subject Alternate Names** page, the information to be automatically populated by the wizard is displayed. If additional subject alternative names are needed, you specify them in the next two steps.
11. On the **SIP Domain Setting on Subject Alternate Names (SANs)** page, select the domain check box to add a sip.<*sipdomain*> entry to the subject alternative names list.
12. On the **Configure Additional Subject Alternate Names** page, specify any additional subject alternative names that are required.
13. On the **Request Summary** page, review the certificate information to be used to generate the request.
14. After the commands finish running, do the following:
    - To view the log for the certificate request, click **View Log**.
    - To complete the certificate request, click **Next**.
15. On the **Certificate Request File** page, do the following:
    - To view the generated certificate signing request (CSR) file, click **View**.
    - To close the wizard, click **Finish**.
16. Copy the output file to a location where you can submit it to the public CA.

⊟To create a certificate request for the external interface of the Edge Server to support public IM connectivity with AOL

1. When the required template is available to the CA, use the following Windows PowerShell cmdlet from at the Edge Server to request the certificate:

```
Request-CsCertificate -New -Type AccessEdgeExternal  -Output C:\ <cert
```

   The default certificate name of the template provided in Lync Server 2013 is Web Server. Only specify the <*template name*> if you need to use a template that is different from the default template.

Note:

> If your organization wants to support public IM connectivity with AOL, you must use Windows PowerShell instead of the Certificate Wizard to request the certificate to be assigned to the external edge for the Access Edge

> service. This is because the Lync Server 2013 Web Server template that the Certificate Wizard uses to request a certificate does not support client EKU configuration. Before using Windows PowerShell to create the certificate, the CA administrator must create and deploy a new template that supports client EKU.

To submit a request to a public certification authority

1. Open the output file.
2. Copy and paste the contents of the Certificate Signing Request (CSR).
3. If prompted, specify the following:
   - **Microsoft** as the server platform.
   - **IIS** as the version.
   - **Web Server** as the usage type.
   - **PKCS7** as the response format.
4. When the public CA has verified your information, you will receive an email message containing text required for your certificate.
5. Copy the text from the email message and save the contents in a text file (.txt) on your local computer.

To import the certificate for the external interface of the Edge Server

1. Log on as a member of the Administrators group to the same Edge Server on which you created the certificate request.
2. In the Deployment Wizard, on the **Deploy Edge Server** page, next to **Step 3: Request, Install, or Assign Certificates**, click **Run again**.
3. On the **Available Certificate Tasks** page, click **Import a certificate from a .p7b, pfx or .cer file**.
4. On the **Import Certificate** page, click **Browse** to locate and select the certificate that you requested for the external interface of the Edge Server (or, you can type the full path and file name). If the certificate contains a private key, select **Certificate file contains certificate's private key** and type the password for the private key. Click **Next**.
5. On **Import Certificate Summary** page, review the summary and then click **Next**.
6. On **Executing Commands**, review the results of the import, click **View Log** for more information as needed, and then click **Finish** to complete the certificate import.
7. If you are configuring an Edge Server pool, export the certificate with its private key as outlined in the "To export the certificate with the private key for Edge Servers in a pool" procedure later in this topic. Copy the exported certificate file to the other Edge Servers, and import it into the computer store on each Edge Server.

To export the certificate with the private key for Edge Servers in a pool

1. Log on as a member of the Administrators group to the same Edge Server on which you imported the certificate.
2. Click **Start**, click **Run**, and type **MMC**.
3. In the Microsoft Management Console (MMC) console, click **File**, and then click **Add/Remove Snap-in**.
4. In **Add or Remove Snap-ins**, click **Certificates**, and then click **Add**.
5. In the **Certificates** dialog box, select **Computer account**, click **Next**, select **Local computer: (the computer this console is running on)** in **Select Computer**, click **Finish** and then click **OK** to complete configuration of the MMC console.
6. Double-click **Certificates (Local Computer)** to expand the certificate stores, double-click **Personal**, and then double-click **Certificates**.

> **Important:**
>
> If there are no certificates in the Certificates Personal store for the local

> computer, there is no private key associated with the certificate that was imported. Review the request and import steps. If the problem persists, contact your certification authority administrator or provider.

7. In the **Certificates Personal store for the local computer**, right-click the certificate that you are exporting, click **All Tasks**, and then click **Export**.
8. In the Certificate Export Wizard, click **Next**, select **Yes, export the private key**, and then click **Next**.

> **Note:**
>
> If the selection **Yes, export the private key** is not available, the private key associated with this certificate was not marked for export. You will need to request the certificate again, ensuring that the certificate is marked to allow for the export of the private key before you can continue with the export. Contact your certification authority administrator or provider.

9. On the Export File Formats dialog, select **Personal Information Exchange – PKCS#12 (.PFX)** and then select the following:
   - Include all certificates in the certification path if possible
   - Export all extended properties

> ⚠**Warning:**
>
> When exporting the certificate from an Edge server, do not select **Delete the private key if the export is successful**. Selecting this option will require that you import the certificate and the private key to this Edge server.

10. Click **Next**.
11. Type a password for the private key, type the password again to confirm, and then click **Next**.
12. Type a path and file name for the exported certificate, using a file extension of .pfx. The path must either be accessible to all other Edge servers in the pool or available to transport by means of removable media - for example, a USB flash drive. Click **Next**.
13. Review the summary in **Completing the Certificate Export Wizard**, and then click **Finish**.
14. In the successful export dialog box, click **OK**.
15. Import the exported certificate file to the other Edge servers following the steps outlined in the "To import the certificate for the external interface of the Edge Server" procedure earlier in this topic.

⊟To assign the certificate for the external interface of the Edge Server

1. On each Edge Server, in the Deployment Wizard, next to **Step 3: Request, Install, or Assign Certificates**, click **Run again**.
2. On the **Available Certificate Tasks** page, click **Assign an existing certificate**.
3. On the **Certificate Assignment** page, click **External Edge Certificate** and select the **Advanced Certificate Usages** check box.
4. On the **Advanced Certificate Usages** page, select all check boxes to assign the certificate for all usages.
5. On the **Certificate Store** page, select the public certificate that you requested and imported for the external interface of the Edge Server.

> **Note:**
>
> If the certificate you requested and imported is not in the list, one of the trouble shooting methods is to verify that subject name and subject alternative names of the certificate meet all requirements for the certificate and, if you manually imported the certificate and certificate chain instead of using the preceding procedures, that the certificate is in the correct certificate store (the computer certificate store, not the user or service certificate store).

6. On the **Certificate Assignment Summary** page, review your settings, and then click **Next** to assign the certificates.

7. On the wizard completion page, click **Finish**.
8. After using this procedure to assign the edge certificate, open the Certificate snap-in on each server, expand **Certificates (Local computer)**, expand **Personal**, click **Certificates**, and then verify in the details pane that the certificate is listed.
9. If your deployment includes multiple Edge Servers, repeat this procedure for each Edge Server.

1.4.2.6.4.4 Set Up Certificates for the Reverse Proxy

Set Up Certificates for the Reverse Proxy

Deploying External User Access > Setting Up Edge Servers > Set Up Edge Certificates >

Topic Last Modified: *2012-09-08*

Each reverse proxy server requires a web server certificate for use by the listening service. The web server certificate must be issued by a public certification authority (CA).

For details about this and other certificate requirements, see Certificate Requirements for External User Access.

⊟To set up a Web Services certificate for the reverse proxy

- You should have already set up your reverse proxy, including setting up the Web Services certificate. If you did not do so before starting your deployment of your Edge Servers, use the procedures in Setting Up Reverse Proxy Servers to create request and install the Web Services certificate, and then create each web publishing rule and configure it to use the certificate.

1.4.2.6.5 Start Edge Servers

Start Edge Servers

Deployment > Deploying External User Access > Setting Up Edge Servers >

Topic Last Modified: *2012-01-16*

After completing the set up of the Edge Servers and load balancers, you need to start the services on each Edge Server.

⊟To start the services

1. On each Edge Server, in the Deployment Wizard, next to **Step 4: Start Services**, click **Run**.
2. On the **Start Lync Server 15 Services** page, review the list of services, and then click **Next** to start the services.
3. After the services are started, click **Finish** to close the wizard.
4. Under **Step 4: Start Services**, click **Services Status (Optional)**.
5. In the **Services** Microsoft Management Console (MMC) on the server, verify that all of the Lync Server 2013 services are running.

1.4.2.7 Setting Up Reverse Proxy Servers

Setting Up Reverse Proxy Servers

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2012-05-26*

For Microsoft Lync Server 2013 Edge Server deployments, an HTTPS reverse proxy in the perimeter network is required for external clients to access the Lync Server 2013 Web Services (called *Web Components* in Office Communications Server) on the Director and the user's home pool. Some of the features that require external access through a reverse proxy include the following:

- Enabling external users to download meeting content for your meetings.
- Enabling external users to expand distribution groups.
- Enabling remote users to download files from the Address Book service.
- Accessing the Lync Web App client.
- Accessing the Dial-in Conferencing Settings webpage.
- Accessing the Location Information service.
- Enabling external devices to connect to Device Update web service and obtain updates.
- Enabling mobile applications to automatically discover mobility URLs from the Internet.

We recommend that you configure your HTTP reverse proxy to publish all Web Services in all pools. Publishing https:// *ExternalFQDN*/* publishes all IIS virtual directories for a pool. You need one publishing rule for each Standard Edition server, Front End pool, or Director or Director pool in your organization.

In addition, you need to publish the simple URLs. If the organization has a Director or Director pool, the HTTP reverse proxy listens for HTTP/HTTPS requests to the simple URLs and proxies them to the external Web Services virtual directory on the Director or Director pool. If you have not deployed a Director, you need to designate one pool to handle requests to the simple URLs. (If this is not the user's home pool, it will redirect them onward to the Web Services on the user's home pool). The simple URLs can be handled by a dedicated web publishing rule, or you can add it to the public names of the web publishing rule for the Director.

If you are deploying mobile applications and plan to use automatic discovery, you also need to publish the external Autodiscover Service URL.

You can use Microsoft Forefront Threat Management Gateway 2010 or Microsoft Internet Security and Acceleration (ISA) Server 2006 SP1 as a reverse proxy. The detailed steps in this section describe how to configure Forefront Threat Management Gateway 2010, and the steps for configuring ISA Server 2006 are almost identical. If you are using a different reverse proxy, consult the documentation for that product and map the requirements defined here to the associated features in other reverse proxies.

The following topics and procedures use Forefront Threat Management Gateway 2010 as the basis for the deployment and configuration procedures.

- Configure Web Farm FQDNs
- Configure Network Adapters
- Request and Configure a Certificate for Your Reverse HTTP Proxy
- Configure Web Publishing Rules for a Single Internal Pool
- Verify or Configure Authentication and Certification on IIS Virtual Directories
- Create DNS Records for Reverse Proxy Servers
- Verify Access through Your Reverse Proxy

Before You Begin

To successfully deploy Forefront Threat Management Gateway 2010 as your reverse proxy, you need to setup and configure a server, using the prerequisites and hardware requirements defined in the Forefront Threat Management Gateway 2010 documentation.

See the following topics to properly configure the hardware and to install Forefront Threat Management Gateway 2010 on the server before proceeding.

1.4.2.7.1 Configure Web Farm FQDNs

Configure Web Farm FQDNs

Deployment > Deploying External User Access > Setting Up Reverse Proxy Servers >

Topic Last Modified: *2012-06-20*

When you defined the configuration of the Standard Edition server, Front End pool, and Director or Director pool in Topology Builder, you configure an external web services fully qualified domain name (FQDN). During the log on process of a client homed in the Standard Edition server or Front End pool, the configured web services FQDNs are sent by way of in-band provisioning. If you need to add or change the external web services URL, you use Topology Builder to configure or reconfigure the web services configuration using the procedure in this topic.

To configure an external pool FQDN for web services

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In Topology Builder, in the console tree under **Standard Edition Front Ends**, **Enterprise Edition Front Ends**, and **Directors**, right-click the pool name that you need to edit, and then click **Edit Properties**.
3. In the **Web services** section, add or edit the **External web services FQDN**.
4. Review and adjust the **Listening ports** for both HTTP and HTTPS. The defaults will be:
   - **Listening ports:** HTTP 8080, HTTPS 4443
   - **Published ports:** HTTP 80, HTTPS 443

   Where the **Listening ports** is the port that the external web services will be configured to receive requests from the reverse proxy, and the **Published ports** is the ports that are published externally by the reverse proxy and is communicated to clients during in-band provisioning.
5. When you have completed your additions and updates, click **OK** to continue.
6. Right-click **Lync Server 2013**, and then click **Publish**.

   > **Important:**
   >
   > After publishing successfully completes, a link may be presented that informs you that there are additional steps that need to be taken. The link, if clicked, opens a list of servers affected by the changes made in Topology Builder that will require you to re-run the Lync Server Deployment Wizard on each listed server to update the configuration for added, removed, or changed components.
7. Repeat these steps for all Standard Edition servers, Front End pools, Directors, and Director pools in the organization.

1.4.2.7.2 Configure Network Adapters

Configure Network Adapters

Deployment > Deploying External User Access > Setting Up Reverse Proxy Servers >

Topic Last Modified: *2012-10-21*

You must assign one or more IP addresses to the external network adapter and at least one IP address to the internal network adapter.

If this is a new installation, install Microsoft Forefront Threat Management Gateway 2010 according to the setup instructions included with the product.

In the following procedures, the server running Forefront Threat Management Gateway (TMG) 2010 has two network adapters:

- A public, or external, network adapter, for clients that attempt to connect to your website (that is, usually over the Internet).
- A private, or internal, network interface, for internal servers running Lync Server that are hosting Web Services.

Important:

Similar to the Edge Servers, you set the default gateway on the, external network adapter only. The default gateway will be the IP address of the router or external facing firewall that directs traffic to the Internet. For traffic that is destined from the reverse proxy to the internal facing network adaptor, you must use persistent static routes (such as the route command in Windows Server) for all subnets containing servers referenced by the web publishing rules.

However, creating persistent routes for all subnets may not be necessary if your network’s routers are configured to summarize routes. Create a persistent route to the network where the router is defined and use the router as the default gateway. If you are not sure how your network is configured and need guidance on what persistent routes need to be created, consult with your company’s Network Engineers.

The reverse proxy must be able to resolve the DNS host (A) records for the internal Director and next hop pool FQDNs used in the web publishing rules. As with the Edge Servers, for security reasons, we recommend that you do not have reverse proxy servers access a DNS server located in the internal network. This means you either need DNS servers in the perimeter, or you need HOSTS file entries on the reverse proxy that resolves each of these FQDNs to the internal IP address of the servers.

To configure the network adapter cards on the reverse proxy computer

1. On the Windows Server 2008 or Windows Server 2008 R2 server running TMG 2010, open Change Adapter Settings by clicking **Start**, pointing to **Control Panel**, clicking **Network and Sharing Center**, and then clicking **Change Adapter Settings**.
2. Right-click the external network connection that you want to use for the external interface, and then click **Properties**.
3. On the **Properties** page, click the **Networking** tab, click **Internet Protocol Version 4 (TCP/IPv4)** in the **This connection uses the following items** list, and then click **Properties**.
4. On the **Internet Protocol (TCP/IP) Properties** page, configure the IP addresses as appropriate for the network subnet to which the network adapter is attached.

   Note:

   If the reverse proxy is already being used by other applications that use HTTPS/443, such as for publishing Outlook Web Access, you either need to add another IP address so that you can publish the Lync Server 2013 Web Services on HTTPS/443 without interfering with the existing rules and web listeners, or you need to replace the existing certificate with one that adds the new external FQDN names to the subject alternative name.

5. Click **OK**, and then click **OK**.
6. In **Network Connections**, right-click the internal network connection that you want to use for the internal interface, and then click **Properties**.
7. Repeat steps 3 through 5 to configure the internal network connection.

1.4.2.7.3 Request and Configure a Certificate for Your Reverse HTTP Proxy

Request and Configure a Certificate for Your Reverse HTTP Proxy

Deployment > Deploying External User Access > Setting Up Reverse Proxy Servers >

Topic Last Modified: *2013-02-15*

You need to install the root certification authority (CA) certificate on the server running Microsoft Forefront Threat Management Gateway 2010 for the CA infrastructure that issued the server certificates to the internal servers running Microsoft Lync Server 2013.

You also must install a public web server certificate on your reverse proxy server. This certificate's subject alternative names should contain the published external fully qualified domain names (FQDNs) of each pool that is home to users enabled for remote access, and the external FQDNs of all Directors or Director pools that will be used within that Edge infrastructure. The subject alternative name must also contain the meeting simple URL, the dial-in simple URL, and, if you are deploying mobile applications and plan to use automatic discovery, the external Autodiscover Service URL as shown in the following table.

	Value	**Example**
Subject name	Pool FQDN	webext.contoso.com
Subject alternative name	Pool FQDN	webext.contoso.com **Important:** The subject name must also be present in the subject alternative name.
Subject alternative name	Meeting simple URL **Note:** All meeting simple URLs must be in the subject alternative name. Each SIP domain must have at least one active meeting simple URL.	meet.contoso.com
Subject alternative name	Dial-in simple URL	dialin.contoso.com
Subject alternative name	External Autodiscover Service URL	lyncdiscover.contoso.com

Note:
If your internal deployment consists of more than one Standard Edition server or Front End pool, you must configure web publishing rules for each external web farm FQDN and you will either need a certificate and web listener for each, or you must obtain a certificate whose subject alternative name contains the names used by all of the pools, assign it to a web listener, and share it among multiple web publishing rules.

Create a Certificate Request

You create a certificate request on the reverse proxy. You create a request on another computer, but you must export the signed certificate with the private key and import it onto the reverse proxy once you have received it from the public certification authority.

Note:

> A certificate request or a certificate signing request (CSR) is a request to a trusted public certification authority (CA) to validate and sign the requesting computer's public key. When a certificate is generated, a public key and a private key are created. Only the public key is shared and signed. As the name implies, the public key is made available to any public request. The public key is for use by clients, servers and other requesters that need to exchange information securely and validate a computer's identity. The private key is kept secured and is used only by the computer that created the key pair to decrypt messages encrypted with its public key. The private key can be used for other purposes. For reverse proxy purposes, data encipherment is the primary use. Secondarily, the certificate authentication at the certificate key level is another use, and is limited only to validation that a requester has the computer's public key, or that the computer that you have a public key for is actually the computer that it claims to be.

To generate a certificate signing request on the computer where the certificate and private key will be assigned, you do the following:

Creating a certificate signing request

1. Open the Microsoft Management Console (MMC) and add the Certificates snap-in and select **Computers**, then expand **Personal**. For details on how to create a certificates console in the Microsoft Management Console (MMC), see http://go.microsoft.com/fwlink/?LinkId=282616.
2. Right-click **Certificates**, click **All Tasks**, click **Advanced Operations**, click **Create Custom Request**.
3. On the **Certificate Enrollment** page, click **Next**.
4. On the **Select Certificate Enrollment Policy** page under **Custom Request**, select **Proceed without enrollment policy**. Click **Next**.
5. On the **Custom Request** page, for **Template** select **(No template) Legacy key**. Unless otherwise directed by your certificate provider, leave **Suppress default extensions** unchecked and the **Request format** selection on **PKCS #10**. Click **Next**.
6. On the **Certificate Information** page, click **Details**, then click **Properties**.
7. On the **Certificate Properties** page on the **General** tab in the **Friendly Name** field, type a name for this certificate. Optionally, type a description in the **Description** field. The Friendly Name and description are typically used by the Administrator to identify what the certificate purpose is, such as **Reverse Proxy Listener for Lync Server**.
8. Select the **Subject** tab. Under **Subject name** for the **Type**, select **Common name** for the Subject name type. For the **Value**, type the subject name that you will use for the reverse proxy. In the example provided in the table in this topic, the subject name is webext.contoso.com and would be typed into the Value field for the Subject name.
9. On the **Subject** tab under **Alternative name**, select **DNS** from the drop down for **Type**. For each defined subject alternative name that you require on the certificate, type the fully qualified domain name, then click **Add**. For example, in the table there are three subject alternative names, meet.contoso.com, dialin.contoso.com, and lyncdiscover.contoso.com. In the **Value** field, type meet.contoso.com, then click **Add**. Repeat for each subject alternative names that you need to define.
10. On the **Certificate Properties** page, click the **Extensions** tab. On this page, you will define the cryptographic key purposes in **Key usage** and the extended key usage in **Extended Key Usage (application policies)**.
11. Click the **Key usage** arrow to show the **Available options**. Under Available options, click **Digital signature**, then click **Add**. Click **Key encipherment**, then click **Add**. If the checkbox for **Make these key usages critical** is unchecked, select the checkbox.
12. Click the **Extended Key Usage (application policies)** arrow to show the **Available options**. Under Available options, click **Server Authentication**, then click **Add**. Click **Client Authentication**, then click **Add**. If the check box for **Make the Extended Key Usages critical** is checked, unselect the checkbox. Contrary to the Key usage checkbox (which must be checked) you must be

sure that the Extended Key Usage checkbox is not checked.

13. On the **Certificate Properties** page, click the **Private Key** tab. Click the **Key options** arrow. For **Key size**, select **2048** from the drop down. If you are generating this key pair and CSR on a computer other than the reverse proxy that this certificate is intended for, select **Make private key exportable**.

Security Note:

Selecting **Make a private key exportable** is generally advised when you have more than one reverse proxy in a farm because you will copy the certificate and the private key to each machine in the farm. If you do allow for an exportable private key, you must take extra care with the certificate and the computer that it is generated on. The private key, if compromised, will render the certificate useless as well as potentially expose the computer or computers to external access and other security vulnerabilities.

14. On the **Private Key** tab, click the **Key options** arrow. Select the **Exchange** option.
15. Click **OK** to save the **Certificate Properties** that you have set.
16. On the **Certificate Enrollment** page, click **Next**.
17. On the **Where do you want to save the offline request?** page, you are prompted for a **File Name** and a **File Format** for saving the certificate signing request.
18. In the **File Name** entry field, type a path and filename for the request, or click **Browse** to select a location for the file and type the filename for the request.
19. For **File format**, click either **Base 64** or **Binary**. Select **Base 64** unless you are instructed otherwise by the vendor for your certificates.
20. Locate the request file that you saved in the previous step. Submit to your public certification authority.

Important:

Microsoft has identified Public CAs that meet the requirements for Unified Communications purposes. A list is maintained in the following knowledge base article. http://go.microsoft.com/fwlink/?LinkId=282625

1.4.2.7.4 Configure Web Publishing Rules for a Single Internal Pool

Configure Web Publishing Rules for a Single Internal Pool

Deployment > Deploying External User Access > Setting Up Reverse Proxy Servers >

Topic Last Modified: *2012-05-26*

Microsoft Forefront Threat Management Gateway 2010 uses web publishing rules to publish internal resources, such as a meeting URL, to users on the Internet.

In addition to the Web Services URLs for the virtual directories, you must also create publishing rules for simple URLs. For each simple URL, you must create an individual rule on the reverse proxy that points to that simple URL.

If you are deploying mobility and using automatic discovery, you need to create a publishing rule for the external Autodiscover Service URL. Automatic discovery also requires publishing rules for the external Lync Server Web Services URL for your Director pool and Front End pool. For details about creating the web publishing rules for automatic discovery, see Configuring the Reverse Proxy for Mobility.

Use the following procedures to create web publishing rules.

Note:

These procedures assume that you have installed the Standard Edition of Forefront

Threat Management Gateway (TMG) 2010.

⊟To create a web server publishing rule on the computer running TMG 2010

1. Click **Start**, select **Programs**, select **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, select **New**, and then click **Web Site Publishing Rule**.
3. On the **Welcome to the New Web Publishing Rule** page, type a display name for the publishing rule (for example, LyncServerWebDownloadsRule).
4. On the **Select Rule Action** page, select **Allow**.
5. On the **Publishing Type** page, select **Publish a single Web site or load balancer**.
6. On the **Server Connection Security** page, select **Use SSL to connect to the published Web server or server farm**.
7. On the **Internal Publishing Details** page, type the fully qualified domain name (FQDN) of the internal web farm that hosts your meeting content and Address Book content in the **Internal Site name** box.

   Note:

   If your internal server is a Standard Edition server, this FQDN is the Standard Edition server FQDN. If your internal server is a Front End pool, this FQDN is a hardware load balancer virtual IP (VIP) that load balances the internal web farm servers. The TMG server must be able to resolve the FQDN to the IP address of the internal web server. If the TMG server is not able to resolve the FQDN to the proper IP address, you can select **Use a computer name or IP address to connect to the published server**, and then in the **Computer name or IP address** box, type the IP address of the internal web server. If you do this, you must ensure that port 53 is open on the TMG server and that it can reach a DNS server that resides in the perimeter network. You can also use entries in the local hosts file to provide name resolution.

8. On the **Internal Publishing Details** page, in the **Path (optional)** box, type **/*** as the path of the folder to be published.

   Note:

   In the website publishing wizard you can only specify one path. Additional paths can be added by modifying the properties of the rule.

9. On the **Public Name Details** page, confirm that **This domain name** is selected under **Accept Requests for**, type the external Web Services FQDN, in the **Public Name** box.
10. On **Select Web Listener** page, click **New** to open the New Web Listener Definition Wizard.
11. On the **Welcome to the New Web Listener Wizard** page, type a name for the web listener in the **Web listener name** box (for example, LyncServerWebServers).
12. On the **Client Connection Security** page, select **Require SSL secured connections with clients**.
13. On the **Web Listener IP Address** page, select **External**, and then click **Select IP Addresses**.
14. On the **External Listener IP selection** page, select **Specified IP address on the Forefront TMG computer in the selected network**, select the appropriate IP address, click **Add**.
15. On the **Listener SSL Certificates** page, select **Assign a certificate for each IP address**, select the IP address that is associated with the external web FQDN, and then click **Select Certificate**.
16. On the **Select Certificate** page, select the certificate that matches the public names specified in step 9, click **Select**.
17. On the **Authentication Setting** page, select **No Authentication**.
18. On the **Single Sign On Setting** page, click **Next**.
19. On the **Completing the Web Listener Wizard** page, verify that the **Web**

listener settings are correct, and then click **Finish**.

20. On the **Authentication Delegation** page, select **No delegation, but client may authenticate directly**.
21. On the **User Set** page, click **Next**.
22. On the **Completing the New Web Publishing Rule Wizard** page, verify that the web publishing rule settings are correct, and then click **Finish**.
23. Click **Apply** in the details pane to save the changes and update the configuration.

⊟To modify the properties of the web publishing rule

1. Click **Start**, point to **Programs**, select **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In the left pane, expand **ServerName**, and then click **Firewall Policy**.
3. In the details pane, right-click the web server publishing rule that you created in the previous procedure (for example, LyncServerExternalRule), and then click **Properties**.
4. On the **Properties** page, on the **From** tab, do the following:
    - In the **This rule applies to traffic from these sources** list, click **Anywhere**, and then click **Remove**.
    - Click **Add**.
    - In **Add Network Entities**, expand **Networks**, click **External**, click **Add**, and then click **Close**.
5. On the **To** tab, ensure that the **Forward the original host header instead of the actual one** check box is selected.
6. On the **Bridging** tab, select the **Redirect request to SSL port** check box, and then specify port **4443**.
7. On the **Public Name** tab, add the simple URLs (for example, meet.contoso.com and dialin.contoso.com).
8. Click **Apply** to save changes, and then click **OK**.
9. Click **Apply** in the details pane to save the changes and update the configuration.

1.4.2.7.5 Verify or Configure Authentication and Certification on IIS Virtual Directories

Verify or Configure Authentication and Certification on IIS Virtual Directories

See Also

Deployment > Deploying External User Access > Setting Up Reverse Proxy Servers >

Topic Last Modified: *2012-05-25*

Use the following procedure to configure the certificate on your Internet Information Services (IIS) virtual directories or verify that the certificate is configured correctly. Perform the following procedure on each server running IIS in your internal Lync Server pool and the optional Director.or Director pool servers.

Note:

The following procedure defines a procedure to request a combined certificate that is used for all purposes Lync Server, Internal Web Site and External Web Site in IIS. Lync Server 2010 introduced a set of Lync Server Management Shell Windows PowerShell cmdlets for the express purpose of managing certificate request, import, and assignment. The procedure assumes that there is an internally deployed certification authority (CA) that can process the request. If you use public certificates for your Lync Server purposes, or your CA requires an offline request, see the detailed syntax in this topic for information on the –Output parameter. Request-CsCertificate

⊟To configure authentication and certificates on IIS virtual directories

1. To successfully complete the following, you must be logged on to the computer (Front End Server or Director) where the web services are installed and be a local administrator. You must have the **read** and **enroll** permissions on the certification authority that you will be requesting certificates from, if the certification authority is your organization's certification authority. You do not need permissions to the certification authority if you will configure and send an offline certificate request.
2. Click **Start**, select **All Programs**, select **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
3. In **Internet Information Services (IIS) Manager**, select **ServerName**. In **Features View**, select **Server Certificates**, right-click and select **Open Feature**.

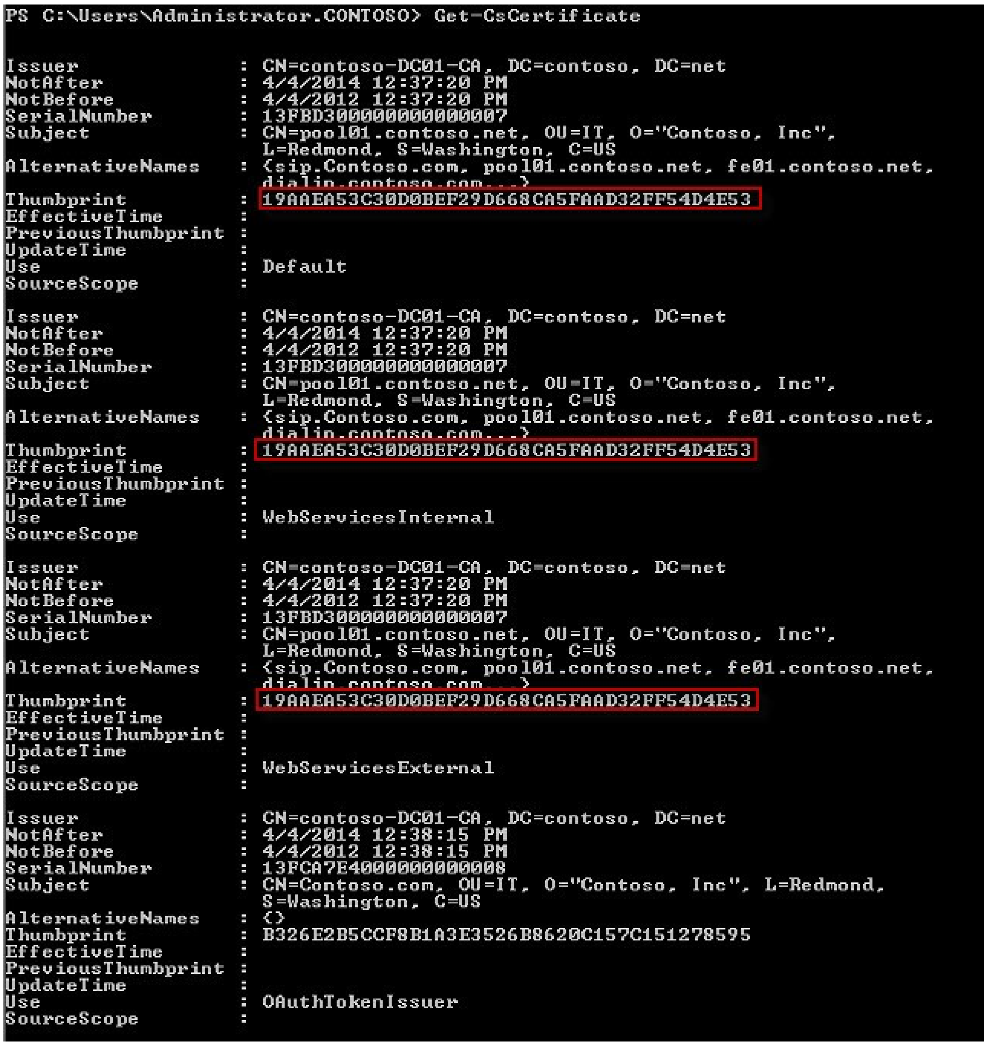
   Tip:

   In the Server Certificates Feature View, if there are certificates assigned to the server, they will appear here. If there is a certificate that matches the requirements for the External Web Site in IIS, you can re-use that certificate. To view a certificate, right-click the certificate and select **View...**

4. On the Front End Server or Director that you are requesting the certificate for, click **Start**, select **All Programs**, select **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
5. In the Lync Server Management Shell, type the following:

   ```
   Get-CsCertificate
   ```

   The output is a list of the certificates that are currently on the server in the Computer Personal certificate store. Note that in the combined certificate (that is, where the default, web services internal and web services external are using the same certificate) you will see that the Use property will be populated with Default, WebServicesInternal and WebServicesExternal. Also, the Thumbprint property will be the same for each of the Use types. An example output of Get-CsCertificate is shown in this example:



```
PS C:\Users\Administrator.CONTOSO> Get-CsCertificate


Issuer              : CN=contoso-DC01-CA, DC=contoso, DC=net
NotAfter            : 4/4/2014 12:37:20 PM
NotBefore           : 4/4/2012 12:37:20 PM
SerialNumber        : 13FBD300000000000007
Subject             : CN=pool01.contoso.net, OU=IT, O="Contoso, Inc",
                      L=Redmond, S=Washington, C=US
AlternativeNames    : {sip.Contoso.com, pool01.contoso.net, fe01.contoso.net,
                      dialin.contoso.com...}
Thumbprint          : 19AAEA53C30D0BEF29D668CA5FAAD32FF54D4E53
EffectiveTime       :
PreviousThumbprint  :
UpdateTime          :
Use                 : Default
SourceScope         :

Issuer              : CN=contoso-DC01-CA, DC=contoso, DC=net
NotAfter            : 4/4/2014 12:37:20 PM
NotBefore           : 4/4/2012 12:37:20 PM
SerialNumber        : 13FBD300000000000007
Subject             : CN=pool01.contoso.net, OU=IT, O="Contoso, Inc",
                      L=Redmond, S=Washington, C=US
AlternativeNames    : {sip.Contoso.com, pool01.contoso.net, fe01.contoso.net,
                      dialin.contoso.com...}
Thumbprint          : 19AAEA53C30D0BEF29D668CA5FAAD32FF54D4E53
EffectiveTime       :
PreviousThumbprint  :
UpdateTime          :
Use                 : WebServicesInternal
SourceScope         :

Issuer              : CN=contoso-DC01-CA, DC=contoso, DC=net
NotAfter            : 4/4/2014 12:37:20 PM
NotBefore           : 4/4/2012 12:37:20 PM
SerialNumber        : 13FBD300000000000007
Subject             : CN=pool01.contoso.net, OU=IT, O="Contoso, Inc",
                      L=Redmond, S=Washington, C=US
AlternativeNames    : {sip.Contoso.com, pool01.contoso.net, fe01.contoso.net,
                      dialin.contoso.com...}
Thumbprint          : 19AAEA53C30D0BEF29D668CA5FAAD32FF54D4E53
EffectiveTime       :
PreviousThumbprint  :
UpdateTime          :
Use                 : WebServicesExternal
SourceScope         :

Issuer              : CN=contoso-DC01-CA, DC=contoso, DC=net
NotAfter            : 4/4/2014 12:38:15 PM
NotBefore           : 4/4/2012 12:38:15 PM
SerialNumber        : 13FCA7E4000000000008
Subject             : CN=Contoso.com, OU=IT, O="Contoso, Inc", L=Redmond,
                      S=Washington, C=US
AlternativeNames    : {}
Thumbprint          : B326E2B5CCF8B1A3E3526B8620C157C151278595
EffectiveTime       :
PreviousThumbprint  :
UpdateTime          :
Use                 : OAuthTokenIssuer
SourceScope         :
```

6. In the Lync Server Management Shell, type the following:

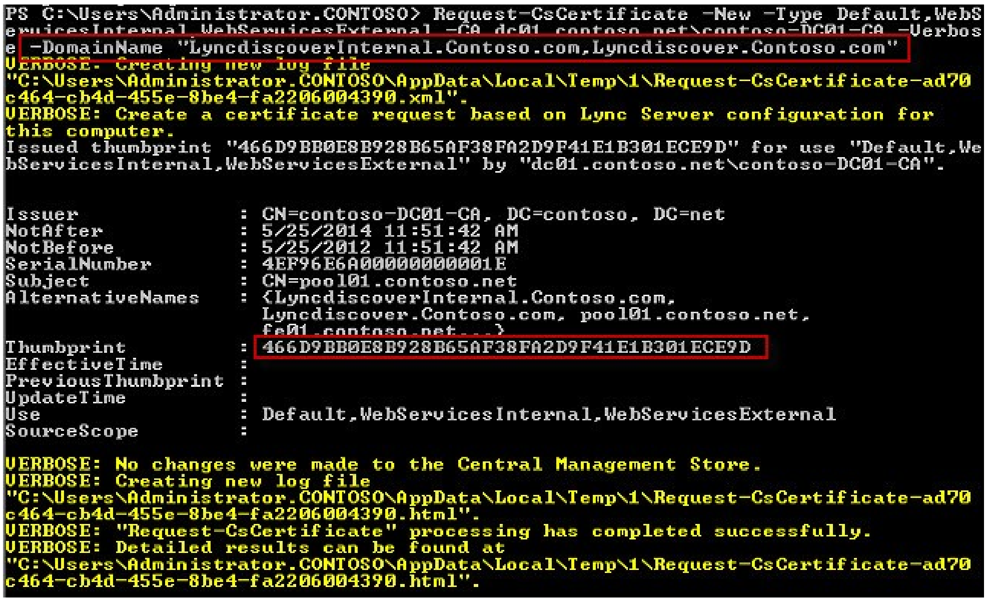
```
Request-CsCertificate -New -Type Default,WebServicesInternal,WebServic
```

Where the full command would appear like following example:

```
Request-CsCertificate -New -Type Default,WebServicesInternal,WebServic
```

Tip:

By default, Request-CsCertificate will populate the subject name with the server or pool name and populate entries in the subject alternative name with the server FQDN, pool FQDN, Simple URL FQDNs, and internal and external web services FQDNs. It does this by referencing to the topology document in your deployment. If there is a missing value and you have specified the –Verbose parameter, you will be notified that the computed and actual values for alternative names are different, but it does not inform you which values are missing. It does supply you with the entire computed value that the cmdlet references. Use the computed alternative names string in the output to re-request a new certificate that will include all values.



```
PS C:\Users\Administrator.CONTOSO> Request-CsCertificate -New -Type Default,WebS
ervicesInternal,WebServicesExternal -CA dc01.contoso.net\contoso-DC01-CA -Verbos
e -DomainName "LyncdiscoverInternal.Contoso.com,Lyncdiscover.Contoso.com"
VERBOSE: Creating new log file
"C:\Users\Administrator.CONTOSO\AppData\Local\Temp\1\Request-CsCertificate-ad70
c464-cb4d-455e-8be4-fa2206004390.xml".
VERBOSE: Create a certificate request based on Lync Server configuration for
this computer.
Issued thumbprint "466D9BB0E8B928B65AF38FA2D9F41E1B301ECE9D" for use "Default,We
bServicesInternal,WebServicesExternal" by "dc01.contoso.net\contoso-DC01-CA".


Issuer              : CN=contoso-DC01-CA, DC=contoso, DC=net
NotAfter            : 5/25/2014 11:51:42 AM
NotBefore           : 5/25/2012 11:51:42 AM
SerialNumber        : 4EF96E6A00000000001E
Subject             : CN=pool01.contoso.net
AlternativeNames    : {LyncdiscoverInternal.Contoso.com,
                      Lyncdiscover.Contoso.com, pool01.contoso.net,
                      fe01.contoso.net...}
Thumbprint          : 466D9BB0E8B928B65AF38FA2D9F41E1B301ECE9D
EffectiveTime       :
PreviousThumbprint  :
UpdateTime          :
Use                 : Default,WebServicesInternal,WebServicesExternal
SourceScope         :

VERBOSE: No changes were made to the Central Management Store.
VERBOSE: Creating new log file
"C:\Users\Administrator.CONTOSO\AppData\Local\Temp\1\Request-CsCertificate-ad70
c464-cb4d-455e-8be4-fa2206004390.html".
VERBOSE: "Request-CsCertificate" processing has completed successfully.
VERBOSE: Detailed results can be found at
"C:\Users\Administrator.CONTOSO\AppData\Local\Temp\1\Request-CsCertificate-ad70
c464-cb4d-455e-8be4-fa2206004390.html".
```

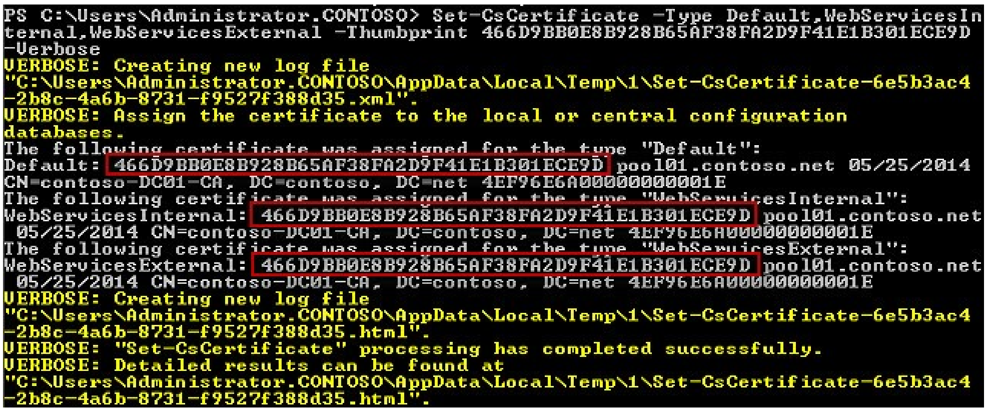
7. In the Lync Server Management Shell, type the following:

   ```
   Set-CsCertificate -Type Default,WebServicesInternal,WebServicesExterna
   ```

   Where the full command would appear like following example:

   ```
   Set-CsCertificate -Type Default,WebServicesInternal,WebServicesExterna
   ```

   The output from the Set-CsCertificate cmdlet will show that the same certificate (identified by the thumbprint of the certificate) is assigned for the Default, WebServicesExternal and WebServicesInternal usage.



```
PS C:\Users\Administrator.CONTOSO> Set-CsCertificate -Type Default,WebServicesIn
ternal,WebServicesExternal -Thumbprint 466D9BB0E8B928B65AF38FA2D9F41E1B301ECE9D
-Verbose
VERBOSE: Creating new log file
"C:\Users\Administrator.CONTOSO\AppData\Local\Temp\1\Set-CsCertificate-6e5b3ac4
-2b8c-4a6b-8731-f9527f388d35.xml".
VERBOSE: Assign the certificate to the local or central configuration
databases.
The following certificate was assigned for the type "Default":
Default: 466D9BB0E8B928B65AF38FA2D9F41E1B301ECE9D pool01.contoso.net 05/25/2014
CN=contoso-DC01-CA, DC=contoso, DC=net 4EF96E6A00000000001E
The following certificate was assigned for the type "WebServicesInternal":
WebServicesInternal: 466D9BB0E8B928B65AF38FA2D9F41E1B301ECE9D pool01.contoso.net
 05/25/2014 CN=contoso-DC01-CA, DC=contoso, DC=net 4EF96E6A00000000001E
The following certificate was assigned for the type "WebServicesExternal":
WebServicesExternal: 466D9BB0E8B928B65AF38FA2D9F41E1B301ECE9D pool01.contoso.net
 05/25/2014 CN=contoso-DC01-CA, DC=contoso, DC=net 4EF96E6A00000000001E
VERBOSE: Creating new log file
"C:\Users\Administrator.CONTOSO\AppData\Local\Temp\1\Set-CsCertificate-6e5b3ac4
-2b8c-4a6b-8731-f9527f388d35.html".
VERBOSE: "Set-CsCertificate" processing has completed successfully.
VERBOSE: Detailed results can be found at
"C:\Users\Administrator.CONTOSO\AppData\Local\Temp\1\Set-CsCertificate-6e5b3ac4
-2b8c-4a6b-8731-f9527f388d35.html".
```

⊟To verify or configure authentication and certificates on IIS virtual directories

1. Click **Start**, select **All Programs**, select **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In **Internet Information Services (IIS) Manager**, expand **ServerName**, and then expand **Sites**.
3. Right-click **Lync Server External Web Site**, and then click **Edit Bindings**
4. Verify that https is associated with port 4443, and then click **https**.
5. Select the HTTPS entry, click **Edit**, and then verify that Lync Server WebServicesExternalCertificate is bound to this protocol. Compare the thumbprint from the Set-CsCertificate cmdlet to ensure that the expected certificate is correctly associated with the HTTPS binding.

Other Resources

Get-CsCertificate
Set-CsCertificate

1.4.2.7.6 Create DNS Records for Reverse Proxy Servers

Create DNS Records for Reverse Proxy Servers

Deployment > Deploying External User Access > Setting Up Reverse Proxy Servers >

Topic Last Modified: *2012-09-27*

Create external DNS A records that point to the public external interface of your Microsoft Internet Security and Acceleration (ISA) Server 2006 SP1 or Forefront Threat Management Gateway 2010 Server, as described in Configure DNS for Edge Support. You need DNS records for the external Web Service FQDNs for each pool, the Director (or Director pool), and each simple URL.

The minimum DNS records for client resolution to the reverse proxy, the following records must be created:

- Host (A) record that defines the reverse proxy (for example, **lsrp.contoso.com**)
- Host (A) record(s) that define the published external web services for Directors and Director pools (for example, **webdirexternal.contoso.com**)
- Host (A) record(s) that define the published external web services for external web services hosted on the any Front End pools and Standard Edition server roles (for example, **webexternal.contoso.com**)
- Host (A) records for the Simple URLs (for example, **dialin.contoso.com** and **meet.contoso.com**)
- Host (A) record for the Lync Discover External record, and also provides pointer to AutoDiscover for all Web apps, including the Lync Web App, scheduler and Mobility (for example, **lyncdiscover.contoso.com**)

For details, see DNS Summary - Reverse Proxy.

1.4.2.7.7 Verify Access through Your Reverse Proxy

Verify Access through Your Reverse Proxy

Deployment > Deploying External User Access > Setting Up Reverse Proxy Servers >

Topic Last Modified: *2012-05-26*

Use the following procedure to verify that your users can access information on the reverse proxy. You might need to complete the firewall configuration and Domain Name System (DNS) configuration before access will work correctly.

⊟To verify that you can access the website through the Internet

- Open a web browser, type the URLs in the **Address** bar that clients use to access the Address Book files and the website for conferencing as follows:
  - For Address Book Server, type a URL similar to the following: **https://*externalwebfarmFQDN*/abs** where *externalwebfarmFQDN* is the external FQDN of the external web services that hosts Address Book services. The user should receive an HTTP challenge, because directory security on the Address Book Server folder is configured to Windows authentication by default.
  - For conferencing, type a URL similar to the following: **https://*externalwebfarmFQDN*/meet** where *externalwebfarmFQDN* is the external FQDN of the web farm that hosts meeting content. This URL should display the troubleshooting page for conferencing. Alternatively, confirm that your Simple URL for conferencing functions correctly. An example Simple URL for

the conference join might be https://meet.contoso.com

- For distribution group expansion, type a URL similar to the following: **https://*externalwebfarmFQDN*/GroupExpansion/service.svc**. The user should receive an HTTP challenge, because directory security on the distribution group expansion service is configured to Windows authentication by default.
- For dial-in, type the simple URL similar to the following **https://*externalwebfarmFQDN*/dialin** where *externalwebfarmFQDN* is the external FQDN of the web farm that hosts the dial-in page for dial-in conferencing. The user should be directed to the dial-in page. Alternatively, confirm that your Simple URL dial-in functions correctly. An example Simple URL for dial-in might be https://dialin.contoso.com

1.4.2.8 Configuring Support for External User Access

Configuring Support for External User Access

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2013-02-21*

Deploying an Edge Server or Edge pool is the first step to supporting external users. For details about deploying Edge Servers, see Deploying External User Access in the Deployment documentation. An important consideration for the configuration of policies is to understand the precedence of policies and how the policies are applied. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

After completing the setup of an Edge Server or Edge pool, you must enable the types of external user access that you want to provide, and configure the settings for the external access. In Lync Server 2013, you enable and configure external user access and policies using the Lync Server Control Panel, the Lync Server Management Shell or both, based on the task requirements.

To support external user access, you must do both of the following:

- **Enable support for your organization** To enable support for external user access in your deployment, you enable each type of external access that you want to support. You enable and disable support for external user access by editing the global settings or creating and configuring a site or user policy on the **External Access Policy** page in the **Federation and External Access** group of the Lync Server Control Panel or by using the Lync Server Management Shell and associated cmdlets. Cmdlets for managing the **External Access Policy** are found in the topic Federation and External Access Cmdlets. Enabling support for external access specifies that your servers running the Lync Server Access Edge service support communications with external users and servers. Internal and external users cannot communicate while external user access is disabled or if policies have not yet been configured to support it.
- **Configure and assign one or more policies** To support external user access, you configure policies to address requirements that include:
  - **External access policies** Created with either a site or user scope (a global policy exists by default and has no enabled settings). You create and configure policies to control the use of one or more types of external user access, including, federated user access (including, if selected, federated XMPP domains)remote users user access, and supported public IM service providers. You configure external policies in Lync Server Control Panel using

the global policy or one or more administratively created site and user policies, on the **External Access Policy** page in the **Federation and External Access** group. The global policy cannot be deleted. You create and configure any site and user policies that you want to use to limit external user access for specific sites or users. Global and site policies are automatically assigned. If you create and configure a user policy, you must then assign it to the specific users by using the user configuration page in the Lync Server Control Panel on the **Users** page. Find the user or users that you want this policy to apply to and assign the policy. to whom you want it to apply. To assign a configured user policy to a user, see Assign an External User Access Policy to a Lync Enabled User. Each external user access policy can support one or more of the following: remote user access, SIP federated user access, XMPP federated user access and public IM connectivity.

- **Conferencing policies** You create and configure policies to control conferencing in your organization, including which users in your organization can invite anonymous users to conferences that they host. On the Lync Server Control Panel **Conferencing** page are policy settings at the global, site and user scope that control settings for the actual conferences. For details, see Managing Meetings and Conferences. You enable anonymous users for conferencing, remote users and federated users on the **Access Edge Configuration** page. The policy on the **Access Edge Configuration** is global in scope. There are no options to define a site or user policy. The scope is controlled on the **External Access Policy** page through the use of global, site, or user policy settings.

  For example, if you want to allow users to create, invite and manage conferencing with remote users, you must set **Enable communications with remote users** on the **External Access Policy** global, site or user policy, and **Enable Communications with remote users** on the **Access Edge Configuration** page. Similarly, to allow conferencing with anonymous users or federated partners that you have a defined relationship with (such as configured federated SIP domains and providers – XMPP federation does not support conferencing), you set **Enable communications with public users** and **Enable communications with federated users** in the **External Access Policy** global, site or user policy. You then select complimentary global policy settings **Enable anonymous user access to conferences** and **Enable federated and public IM connectivity** on the **Access Edge Configuration** page.

You can configure external user access settings, including any policies that you want to use to control external user access, even if you have not enabled external user access for your organization. However, the policies and other settings that you configure are in effect only when you have external user access enabled for your organization. External users cannot communicate with users of your organization when external user access is disabled or if no external user access policies are configured to support it.

Your edge deployment authenticates the types of external users (except for anonymous users, who are authenticated by the conference ID and a passkey that is sent to the anonymous participant when you create the conference and invite participants) and controls access based on how you configure your edge support. In order to control communications, you can configure one or more policies and configure settings that define how users inside and outside your deployment communicate with each other. The policies and settings include the default global policy for external user access, in addition to site and user policies that you can create and configure to enable one or more types of external user access for specific sites or users.

- Configure Policies to Control Remote User Access
- Enable or Disable Remote User Access
- Enable or Disable Anonymous User Access
- Assign Conferencing Policies to Support Anonymous Users

Configure Policies to Control Remote User Access

Deployment > Deploying External User Access > Configuring Support for External User Access >

Topic Last Modified: *2012-10-18*

You configure one or more external user access policies to control whether remote users can collaborate with internal Lync Server users. To control remote user access, you can configure policies at the global, site, and user level. Site policies override the global policy, and user policies override site and global policies. For details about the types of policies that you can configure, see Managing Federation and External Access to Lync Server 2013. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

Note:

You can configure policies to control remote user access, even if you have not enabled remote user access for your organization. However, the policies that you configure are in effect only when you have remote user access enabled for your organization. For details about enabling remote user access, see Enable or Disable Federation and Public IM Connectivity. Additionally, if you specify a user policy to control remote user access, the policy applies only to users that are enabled for Lync Server and configured to use the policy. For details about specifying users that can sign in to Lync Server from remote locations, see Assign an External User Access Policy to a Lync Enabled User.

Use the following procedure to configure each external access policy that you want to use to control remote user access.

Note:

This procedure describes how to configure a policy only to enable communications with remote users, but each policy that you configure to support remote user access can also configure federated user access and public user access. For details about configuring policies to support federated users, see Configure Policies to Control Federated User Access. For details about configuring policies to support public users, see Create or Edit Public SIP Federated Providers.

⊟To configure an external access policy to support remote user access

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do one of the following:
   - To configure the global policy to support remote user access, click the global policy, click **Edit**, and then click **Show details**.
   - To create a new site policy, click **New**, and then click **Site policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
   - To create a new user policy, click **New**, and then click **User policy**. In **New External Access Policy**, create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnableRemoteUsers** for a user policy that enables communications for remote users).
   - To change an existing policy, click the appropriate policy listed in the table,

click **Edit**, and then click **Show details**.

5. (Optional) If you want to add or edit a description, specify the information for the policy in **Description**.
6. Do one of the following:
   - To enable remote user access for the policy, select the **Enable communications with remote users** check box.
   - To disable remote user access for the policy, clear the **Enable communications with remote users** check box.
7. Click **Commit**.

To enable remote user access, you must also enable support for remote user access in your organization. For details, see Enable or Disable Federation and Public IM Connectivity in the Deployment documentation or the Operations documentation.

If this is a user policy, you must also apply the policy to users that you want to be able to connect remotely. For details, see Assign an External User Access Policy to a Lync Enabled User in the Deployment documentation or the Operations documentation.

1.4.2.8.2 Enable or Disable Remote User Access

Enable or Disable Remote User Access

Deployment > Deploying External User Access > Configuring Support for External User Access >

Topic Last Modified: *2013-02-23*

Remote users are users in your organization who have a persistent Active Directory identity within the organization. Remote users often sign in to Lync Server from outside your network by using a virtual private network (VPN) when they are not connected to your organization’s network. Remote users include employees working at home or on the road and other remote workers, such as trusted vendors, who have been granted enterprise credentials. If you enable remote user access for remote users, supported remote users connect over the Internet and do not have to connect using a VPN in order to collaborate with internal users using Lync Server.

To support remote user access, you must enable remote user access. When you enable remote user access, you enable it for your entire organization. If you later want to temporarily or permanently prevent remote user access, you can disable it for your organization. Use the procedure in this section to enable or disable remote user access for your organization.

Note:

Enabling remote user access only specifies that your servers running the Access Edge service support communications with remote users, but remote users cannot participate in instant messaging (IM) or conferences in your organization until you also configure at least one policy to manage the use of remote user access. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object. For details about configuring policies for the use of remote user access, see Configure Policies to Control Remote User Access.

⊟To enable or disable remote user access for your organization

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync

Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Federation and External Access**, and then click **Access Edge Configuration**.
4. On the **Access Edge Configuration** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, do one of the following:
   - To enable remote user access for your organization, select the **Enable remote user access** check box.
   - To disable remote user access for your organization, clear the **Enable remote user access** check box.
6. Click **Commit**.

To enable remote users to sign in to your servers running Lync Server, you must also configure at least one external access policy to support remote user access. For details, see Configure Policies to Control Remote User Access in the Deployment documentation or the Operations documentation.

Enabling or Disabling Remote User Access by Using Windows PowerShell Cmdlets

Remote user access can be managed by using Windows PowerShell and the Set-CsAccessEdgeConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable remote user access

- To enable remote user access, set the value of the **AllowOutsideUsers** property to True ($True):

```
Set-CsAccessEdgeConfiguration -AllowOutsideUsers $True
```

To disable remote user access

- To disable remote user access, set the value of the **AllowOutsideUsers** property to False ($False):

```
Set-CsAccessEdgeConfiguration -AllowOutsideUsers $False
```

1.4.2.8.3 Enable or Disable Anonymous User Access

Enable or Disable Anonymous User Access

See Also

Deployment > Deploying External User Access > Configuring Support for External User Access >

Topic Last Modified: *2013-02-23*

Anonymous users are users who do not have a user account in your organization's Active Directory Domain Services (AD DS) or in a supported federated domain, but can be invited to participate remotely in an on-premises conference. By allowing anonymous participation in meetings you enable anonymous users (that is, users whose identity is verified through the meeting or conference key only) to join meetings. Allowing anonymous participation requires enabling it for your organization.

If you later want to temporarily or permanently prevent access by anonymous users, you can disable it for your organization. Use the procedure in this section to enable or disable anonymous user access for your organization.

Note:

By enabling anonymous user access for your organization you are only specifying that your servers running the Access Edge service support access by anonymous users. Anonymous users cannot participate in any meetings in your organization until you also configure at least one conferencing policy and apply it to one or more users or user groups. The only users that can invite anonymous users to meetings are those users that are assigned a conferencing policy that is configured to support anonymous users. For details about configuring conferencing policies to support inviting anonymous users, see Conferencing Policies.

⊟To enable or disable anonymous user access for your organization

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **Access Edge Configuration**.
4. On the **Access Edge Configuration** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, do one of the following:
   - To enable anonymous user access for your organization, select the **Enable communications with anonymous users** check box.
   - To disable anonymous user access for your organization, clear the **Enable communications with anonymous users** check box.
6. Click **Commit**.

Enabling or Disabling Anonymous User Access by Using Windows PowerShell Cmdlets

You can manage anonymous user access by using Windows PowerShell and the **Set-CsAccessEdgeConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To enable anonymous user access

- To enable anonymous user access, set the value of the **AllowAnonymousUsers** property to True ($True):

```
Set-CsAccessEdgeConfiguration -AllowAnonymousUsers $True
```

⊟To disable anonymous user access

- To disable anonymous user access, set the value of the **AllowAnonymousUsers** property to False ($False):

```
Set-CsAccessEdgeConfiguration -AllowAnonymousUsers $False
```

⊟See Also

Concepts

Conferencing Policy Settings Reference

1.4.2.8.4 Assign Conferencing Policies to Support Anonymous Users

Assign Conferencing Policies to Support Anonymous Users

Deployment > Deploying External User Access > Configuring Support for External User Access >

Topic Last Modified: *2012-10-19*

By default, all users are prevented from inviting anonymous users to participate in a meeting. You control who can invite anonymous users by configuring a conferencing policy to support anonymous users, and applying that conferencing policy to specific users. For details about how to configure a conferencing policies to support anonymous users, see Create or Modify a Conferencing Policy and Managing Federation and External Access to Lync Server 2013.

Use the procedure in this section to apply a conferencing policy that you have already created to one or more users or user groups.

Note:

In addition to configuring and applying a policy to enable users to invite anonymous users, you must also enable support for anonymous users for your organization. For details, see Configure Policies to Control Public User Access.

⊟To configure a user policy for anonymous participation in meetings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**, and then do one of the following:
   3.a. To create a new user policy, click **New**, and then click **User policy**. Create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnableAnonymous** for a user policy that enables communications with anonymous users).
   3.b. To configure an existing user policy, click the appropriate policy listed in the table, click **Edit**, and then click **Show details**.
4. In the **Conferencing Policies** dialog box, select the **Allow participants to invite anonymous users** check box.
5. Click **Commit**.
6. In the left navigation bar, click **Users**, search on the user account that you want to configure.
7. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
8. In **Edit Lync Server User** under **Conferencing policy**, select the user policy with the anonymous user access configuration that you want to apply to this user.

   Note:

   The **<Automatic>** settings apply the default server installation settings and are applied automatically by the server.

To enable users to invite anonymous users to conferences, you must also enable support for anonymous users in your organization. For details, see Configure Policies to Control Public User Access in the Deployment documentation or the Operations documentation.

1.4.2.9 Configuring Support for Autodiscover

Configuring Support for Autodiscover

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2013-01-21*

The Lync Server web services **Autodiscover service** first appeared in the Lync Server 2010 Cumulative Update: November 2011. This update was accompanied by the initial release of Lync Mobile clients. The autodiscover service exposed the mobility services, known as the Mcx service.

The autodiscover service acts as a single location for all clients to request information on what services and features are available, and how to contact the services – either by a fully qualified domain name or a web uniform resource locator reference. Autodiscover exposes a number of features, and each client will make requests based on the features that the client can use. For example, a desktop Lync 2013 client will use autodiscvoer to determine the external web services, but will not use the mobility (Mcx) services. To properly define and enable your clients to use the features available to them, the scenarios that allow a client to effectively find and use autodiscover entries should be defined. To use autodoscover, your deployment requires that a reverse proxy publishes the Lync Server web services, that DNS records are configured to resolve DNS queries for the Lync Server autodiscover service and Lync Server web services, and that certificate services are properly configured for your specific scenario.

Tip:
For technical details on what the elements within the autodiscover request/response do, see Understanding Autodiscover.

The following information and tables define, per scenario, what configurations (if any) you need to implement to provide the full and effective use of the autodiscover service. The information in the following topics is specific to Microsoft Lync Server 2013. If you are looking for guidance on how to plan Mobility for Lync Server 2010, see http://go.microsoft.com/fwlink/?LinkId=275113. To deploy Mobility for Lync Server 2010, see http://go.microsoft.com/fwlink/?LinkId=275114

- Configuring DNS for Autodiscover
- Configuring Certificates for Autodiscover
- Configuring a Reverse Proxy for Autodiscover
- Configuring Autodiscover for Hybrid Deployments

1.4.2.9.1 Configuring DNS for Autodiscover

Configuring DNS for Autodiscover

Deployment > Deploying External User Access > Configuring Support for Autodiscover >

Topic Last Modified: *2012-12-12*

To support autodiscovery for Lync clients, you need to create the following Domain Name System (DNS) records:

- An internal DNS record to support Lync clients who connect from within your organization's network

- An external, or public, DNS record to support Lync clients who connect from the Internet

You must create an internal DNS record and an external DNS record for each SIP domain.

The DNS records can be either A (host) records or CNAME records, based on your ability to create new certificates with the additional subject alternate name (SAN). If you are not able to request and deploy a new external (public) certificate with the lyncdiscover.<domain name> SAN, use the procedure for using HTTP/TCP port 80. The following procedures describe how to create internal and external DNS records.

⊟To create DNS CNAME records

1. Log on to a DNS server as follows:
   - To create an internal DNS record, log on to a DNS server in your network as a member of the Domain Admins group or a member of the DnsAdmins group.
   - To create an external DNS record, connect to your public DNS provider.
2. Open the DNS administrative snap-in: Click **Start**, click **Administrative Tools**, and then click **DNS**.
3. Do one of the following:
   - For an internal DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your Active Directory domain (for example, contoso.local).

     Note:
     This domain is the Active Directory domain where your Lync Server 2013 Director pool and Front End pool are installed.

   - For an external DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).
4. Verify that a host A record exists for your Director pool as follows:
   - For an internal DNS record, a host A record should exist for the internal Web Services fully qualified domain name (FQDN) for your Director pool (for example, lyncwebdir01.contoso.local).
   - For an external DNS record, a host A record should exist for the external web services FQDN for your Director pool (for example, lyncwebextdir.contoso.com).
5. Verify that a host A record exists for your Front End pool as follows:
   - For an internal DNS record, a host A record should exist for the internal Web Services FQDN for your Front End pool (for example, lyncwebpool01.contoso.local).
   - For an external DNS record, a host A record should exist for the external Web Services FQDN for your Front End pool (for example, lyncwebextpool01.contoso.com).
6. For an internal DNS record, in the console tree of your DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).

   Note:
   If you are creating an external DNS record, **Forward Lookup Zones** is already expanded for your SIP domain from step 3.

7. Right-click the SIP domain name, and then click **New Alias (CNAME)**.
8. In **Alias name**, type one of the following:
   - For an internal DNS record, type lyncdiscoverinternal as the host name for the internal Autodiscover Service URL.
   - For an external DNS record, type lyncdiscover as the host name for the external Autodiscover Service URL.
9. In **Fully qualified domain name (FQDN) for target host**, do one of the following:
   - For an internal DNS record, type or browse to the internal Web Services

FQDN for your Director pool (for example, lyncwebdir01.contoso.local), and then click **OK**.

- For an external DNS record, type or browse to the external Web Services FQDN for your Director pool (for example, lyncwebextdir.contoso.com), and then click **OK**.

Note:
If you do not use a Director, use the internal and external Web Services FQDN for the Front End pool, or, for a single server, the FQDN for the Front End Server or Standard Edition server.

Important:
You must create a new Autodiscover CNAME record in the forward lookup zone of each SIP domain that you support in your Lync Server 2013 environment.

To create DNS A records

1. Log on to a DNS server as follows:
   - To create an internal DNS record, log on to a DNS server in your network as a member of the Domain Admins group or a member of the DnsAdmins group.
   - To create an external DNS record, connect to your public DNS provider or external DNS server.
2. Open the DNS administrative snap-in: Click **Start**, click **Administrative Tools**, and then click **DNS**.
3. Do one of the following:
   - For an internal DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your Active Directory domain (for example, contoso.local).

     Note:
     This domain is the Active Directory domain where your Lync Server 2013 Director pool and Front End pool are installed.
   - For an external DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).
4. Verify that a host A (for IPv6, AAAA) record exists for your Director pool as follows:
   - For an internal DNS record, a host A (for IPv6, AAAA) record should exist for the internal Web Services FQDN for your Director pool (for example, lyncwebdir01.contoso.local).
   - For an external DNS record, a host A (for IPv6, AAAA) record should exist for the external Web Services FQDN for your Director pool (for example, lyncwebextdir.contoso.com).
5. Verify that a host A (for IPv6, AAAA) record exists for your Front End pool as follows:
   - For an internal DNS record, a host A (for IPv6, AAAA) record should exist for the internal Web Services FQDN for your Front End pool (for example, lyncwebpool01.contoso.local).
   - For an external DNS record, a host A (for IPv6, AAAA) record should exist for the external Web Services FQDN for your Front End pool (for example, lyncwebextpool01.contoso.com).
6. For an internal DNS record, in the console tree of your DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).

   Note:
   If you are creating an external DNS record, **Forward Lookup Zones** is already expanded for your SIP domain from step 3.
7. Right-click the SIP domain name, and then click **New Host (A or AAAA)**.
8. In **Name**, type the host name as follows:

- For an internal DNS record, type lyncdiscoverinternal as the host name for the internal Autodiscover Service URL.
- For an external DNS record, type lyncdiscover as the host name for the external Autodiscover Service URL.

Note:
The domain name is assumed from the zone in which the record is defined and, therefore, does not need to be entered as part of the A record.

9. In **IP Address**, type the IP address as follows:
   - For an internal DNS record, type the internal Web Services IP address of the Director (or, if you use a load balancer, type the virtual IP (VIP) of the Director load balancer).

     Note:
     If you do not use a Director, type the IP address of the Front End Server or Standard Edition server, or, if you use a load balancer, type the VIP of the Front End pool load balancer.

   - For an external DNS record, type the external or public IP address of the reverse proxy.
10. Click **Add Host**, and then click **OK**.
11. To create an additional A record, repeat steps 8 through 10.

Important:
You must create a new lyncdiscover and lyncdiscoverinternal A records in the forward lookup zone of each SIP domain that you support in your Lync Server 2013 environment.

12. When you are finished creating A (for IPv6, AAAA) records, click **Done**.

1.4.2.9.2 Configuring Certificates for Autodiscover

Configuring Certificates for Autodiscover

Deployment > Deploying External User Access > Configuring Support for Autodiscover >

Topic Last Modified: *2012-12-12*

The certificates for your Director pool, Front End pool, and reverse proxy require additional subject alternative name entries to support secure connections with Lync clients.

Note:
You can use the **Get-CsCertificate** cmdlet to view information about the currently assigned certificates. However, the default view truncates the properties of the certificate and does not display all values in the SubjectAlternativeNames property. You can use the **Get-CsCertificate** , **Request-**CsCertificate and the **Set-CsCertificate** cmdlets to view some information and to request and assign certificates. However, it’s not the best method to use if you are unsure of the properties of the subject alternative names (SAN) on the current certificate. To view the certificate and all property members, it is suggested to use the Certificates snap-in the *Microsoft Management Console (MMC)* or to use the Lync Server Deployment Wizard. In the Lync Server Deployment Wizard, you can use the Certificate Wizard to view the certificate properties. The procedures for viewing, requesting and assigning a certificate using the Lync Server Management Shell and the *Microsoft Management Console (MMC)* are detailed in the following procedures. To use the Lync Server Deployment Wizard, see details here if you have deployed the optional Director or Director pool: Configure Certificates for the Director. For the Front End Server or Front End pool, see the details here: Configure Certificates for Servers.
The initial steps in this procedure are preparation steps, to orient you as to what role the current certificates play. By default, the certificates will not have a lyncdiscover.<sipdomain> or lyncdiscoverinternal.<internal domain name> entry unless you have previously installed Mobility Services or have prepared your certificates in

advance. This procedure uses the example SIP domain name 'contoso.com' and the example internal domain name 'contoso.net'.
The default certificate configuration for Lync Server 2013 and Lync Server 2010 is to use a single certificate (named 'Default') with the purposes Default (for all purposes except for the web services), WebServicesExternal and WebServicesInternal. An optional configuration is to use separate certificates for each purpose. Certificates can be managed by using the Lync Server Management Shell and Windows PowerShell cmdlets, or by using the Certificate Wizard in the Lync Server Deployment Wizard.

To update certificates with new subject alternative names using the Lync Server Management Shell

1. Log on to the computer using an account that has local administrator rights and permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Find out what certificates have been assigned to the server and for which type of use. You need this information in the next step to assign the updated certificate. At the command line, type:

```
Get-CsCertificate
```

4. Look in the output from the previous step to see whether a single certificate is assigned for multiple uses or whether a different certificate is assigned for each use. Look in the Use parameter to find out how a certificate is used. Compare the Thumbprint parameter for the displayed certificates to see if the same certificate has multiple uses.
5. Update the certificate. At the command line, type:

```
Set-CsCertificate -Type <type of certificate as displayed in the Use p
```

For example, if the **Get-CsCertificate** cmdlet displayed a certificate with Use of Default, another with a Use of WebServicesInternal, and another with a Use of WebServicesExternal, and they all had the same Thumbprint value, at the command line, type:

```
Set-CsCertificate -Type Default,WebServicesInternal,WebServicesExterna
```

Important:
If a separate certificate is assigned for each use (the Thumbprint value is different for each certificate), it is important that you do not run the **Set-CsCertificate** cmdlet with multiple types. In this case, run the **Set-CsCertificate** cmdlet separately for each use. For example:

```
Set-CsCertificate -Type Default -Thumbprint <Certificate Thumbprint>
Set-CsCertificate -Type WebServicesInternal -Thumbprint <Certificate T
Set-CsCertificate -Type WebServicesExternal -Thumbprint <Certificate T
```

6. To view the certificate, click **Start**, click **Run...**. Type MMC to open the Microsoft Management Console.
7. From the MMC menu, select **File**, select **Add/Remove snap-in...**, select Certificates. Click **Add**. When prompted, select **Computer account**, then click **Next**.
8. If the certificate is located on this computer, select **Local computer**. If the certificate is located on another computer, select **Another computer**, type in the fully qualified domain name of the computer or click **Browse** In **Enter the object name to select**, type the name of the computer. Click **Check Names**. When the name of the computer is resolved, it will be underlined. Click **OK**, then click **Finish**. Click **OK** to commit the selection and close the **Add or Remove Snap-ins** dialog.

Important:
If the certificate does not show up in the console, ensure that you have not selected User or Service. You must select Computer, or you will not be able

to locate the probper certificate.

9. To view the properties of the certificate, expand **Certificates**, expand **Personal**, and select **Certificates**. Select the certificate to view, right-click on the certificate and select **Open**.
10. In the **Certificate** view, select **Details**. From here, you can select the certificate subject name by selecting **Subject** and the assigned subject name and associated properties are displayed.
11. To view the assigned subject alternative names, select **Subject Alternative Name**. All assigned subject alternative names are displayed. The subject alternative names that are found in the property are of type **DNS Name** by default. You should see the following members (all of which should be fully qualified domain names as represented in DNS host (A or, if IPv6 AAAA) records:
    - Pool name for this pool, or the single server name if this is not a pool
    - Server name that the certificate is assigned to
    - Simple URL records, typically meet and dialin
    - Web services internal and Web services external names (for example, webpool01.contoso.net, webpool01.contoso.com), based on choices made in Topology Builder and over-ridden web services selections.
    - If already assigned, the lyncdiscover.<sipdomain> and lyncdiscoverinternal.<sipdomain> records.

    The last item is what you are most interested in – if there is a lyncdiscover and lyncdiscoverinternal SAN entry.

    Once you have this information, you can close the certificate view and the MMC.
12. If an Autodiscover Service, meaning the lyncdiscover.>domain name> and lyncdiscoverinternal.<domain name> (based on if this is an external or internal certificate) subject alternative name is missing, and you are using a single Default certificate for the Default, WebServicesInternal and WebServiceExternal types, do the following:
    - At the Lync Server Management Shell command line prompt, type:

      ```
      Request-CsCertificate -New -Type Default,WebServicesInterna
      ```

      If you have many SIP domains, you cannot use the new AllSipDomain parameter. Instead, you must use DomainName parameter. When you use the DomainName parameter, you must define the FQDN for the lyncdiscoverinternal and lyncdiscover records. For example:

      ```
      Request-CsCertificate -New -Type Default,WebServicesInterna
      ```

    - To assign the certificate, type the following:

      ```
      Set-CsCertificate -Type Default,WebServicesInternal,WebServi
      ```

      Where “Thumbprint” is the thumbprint displayed for the newly issued certificate.

13. For a missing internal Autodiscover subject alternative names when using separate certificates for Default, WebServicesInternal, and WebServicesExternal, do the following:
    - At the Lync Server Management Shell command line prompt, type:

      ```
      Request-CsCertificate -New -Type WebServicesInternal -Ca dc\
      ```

      If you have many SIP domains, you cannot use the new AllSipDomain parameter. Instead, you must use DomainName parameter. When you use the DomainName parameter, you must use an appropriate prefix for the SIP domain FQDN. For example:

      ```
      Request-CsCertificate -New -Type WebServicesInternal -Ca dc\
      ```

    - For a missing external Autodiscover subject alternative name, at the command line, type:

```
Request-CsCertificate -New -Type WebServicesExternal -Ca dc\
```

If you have many SIP domains, you cannot use the new AllSipDomain parameter. Instead, you must use DomainName parameter. When you use the DomainName parameter, you must use an appropriate prefix for the SIP domain FQDN. For example:

```
Request-CsCertificate -New -Type WebServicesExternal -Ca dc\
```

- To assign the individual certificate types, type the following:

```
Set-CsCertificate -Type Default -Thumbprint <Certificate Thu
Set-CsCertificate -Type WebServicesInternal -Thumbprint <Cer
Set-CsCertificate -Type WebServicesExternal -Thumbprint <Cer
```

Where "Thumbprint" is the thumbprint displayed for the newly issued individual certificates.

1.4.2.9.3 Configuring a Reverse Proxy for Autodiscover

Configuring a Reverse Proxy for Autodiscover

See Also

Deployment > Deploying External User Access > Configuring Support for Autodiscover >

Topic Last Modified: *2012-12-12*

Autodiscover and the support of clients using autodiscover requires modification of an existing web publishing rule or creating a new web publishing rule for the reverse proxy. The modification or creation of a new publishing rule is not dependent on the decision to update or not update the subject alternative name lists on the reverse proxy certificates.

If you decide to use HTTPS for initial Lync Server 2013 Autodiscover Service requests and update the subject alternative names lists on the reverse proxy certificates, you need to assign the updated public certificate to the Secure Sockets Layer (SSL) Listener on your reverse proxy. The required update to the external (public) certificate will include the subject alternate name (SAN) entry for lyncdiscover.<domain name>. You then need to modify the existing listener for the external web services or create a new web publishing rule for the external Autodiscover Service URL, for example **lyncdiscover.contoso.com**. If you do not already have a web publishing rule for the external Lync Server 2013 Web Services URL for your Front End pool and Director pool (if you have deployed Directors), you also need to publish a rule for that.

Note:

The reverse proxy publishing rule and listener can service both the external web services and the Autodiscover Service, as long as the certificate assigned to the listener contains the necessary subject name and subject alternative names for both. For details on the default configuration of the web listener and publishing rule, see Setting Up Reverse Proxy Servers for more details.

If you decide to use HTTP for initial Autodiscover Service requests so that you do not need to update subject alternative names for the reverse proxy, you need to create or modify a web publishing rule for port 80.

The procedures in this section describe how to create or modify the web publishing rules in Microsoft Forefront Threat Management Gateway 2010 for automatic discovery.

Note:

These procedures assume that you have installed the Standard Edition of Forefront Threat Management Gateway (TMG) 2010. If you are using another reverse proxy, the procedures are similar, but will need to be mapped to the documentation for the third-party product.

⊟To create a web publishing rule for the external Autodiscover URL

1. Click **Start**, point to **Programs**, point to **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, point to **New**, and then click **Web Site Publishing Rule**.
3. On the **Welcome to the New Web Publishing Rule** page, type a display name for the new publishing rule (for example, LyncDiscoveryURL).
4. On the **Select Rule Action** page, select **Allow**.
5. On the **Publishing Type** page, select **Publish a single Web site or load balancer**.
6. On the **Server Connection Security** page, select **Use SSL to connect to the published Web server or server farm**.
7. On the **Internal Publishing Details** page, in **Internal Site name**, type the fully qualified domain name (FQDN) of your Director pool (for example, lyncdir01.contoso.local). If you are creating a rule for the external Web Services URL on the Front End pool, type the FQDN of the Front End pool (for example, lyncpool01.contoso.local).
8. On the **Internal Publishing Details** page, in **Path (optional)**, type **/*** as the path of the folder to be published, and then select **Forward the original host header**.
9. On the **Public Name Details** page, do the following:
   - Under **Accept Requests for**, select **This domain name**.
   - In **Public Name**, type **lyncdiscover.**<*sipdomain*> (the external Autodiscover Service URL). If you are creating a rule for the external Web Services URL on the Front End pool, type the FQDN for the external Web Services on your Front End pool (for example, lyncwebextpool01.contoso.com).
   - In **Path**, type **/***.
10. On **Select Web Listener** page, in **Web Listener**, select your existing SSL Listener with the updated public certificate.
11. On the **Authentication Delegation** page, select **No delegation, but client may authenticate directly**.
12. On the **User Set** page, select **All Users**.
13. On the **Completing the New Web Publishing Rule Wizard** page, verify that the web publishing rule settings are correct, and then click **Finish**.
14. In the Forefront TMG list of web publishing rules, double-click the new rule you just added to open **Properties**.
15. On the **To** tab, do the following:
    - Select **Forward the original host header instead of the actual one**.
    - Select **Requests appear to come from the Forefront TMG computer**.
16. On the **Bridging** tab, configure the following:
    - Select **Web server**.
    - Select **Redirect requests to HTTP port**, and type **8080** for the port number.
    - Select **Redirect requests to SSL port**, and type **4443** for the port number.
17. Click **OK**.
18. Click **Apply** in the details pane to save the changes and update the configuration.
19. Click **Test Rule** to verify that your new rule is set up correctly.

⊟To modify an existing web publishing rule to add the external Autodiscover SAN and URL

1. Click **Start**, point to **Programs**, point to **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.

   Important:

You will repeat the modification for each publishing rule and listener that you have. Typically, this will be one rule and listener for the Front End pools and one for the optional Directors or Director pools, if you have deployed them.

2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, click the applicable rule. On the **Tasks** tab, click **Edit Selected rule**.
3. On the **Public Name** tab, in **This rule applies to**, select **Requests for the following Web sites**.
4. Click **Add**, type the name of the new Autodiscover site (for example, "lyncdiscover.contoso.com"), and then click **OK**.
5. On the **Listener** tab, click **Select Certificate** and assign the new certificate with the added Autodiscover SAN entries. Close the Listener and Web Publishing properties.
6. Click **Apply** in the details pane to save the changes and update the configuration.
7. Click **Test Rule** to verify that your new rule is set up correctly.

⊟To create a web publishing rule for port 80

1. Click **Start**, point to **Programs**, point to **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, point to **New**, and then click **Web Site Publishing Rule**.
3. On the **Welcome to the New Web Publishing Rule** page, type a display name for the new publishing rule (for example, Lync Autodiscover (HTTP)).
4. On the **Select Rule Action** page, select **Allow**.
5. On the **Publishing Type** page, select **Publish a single Web site or load balancer**.
6. On the **Server Connection Security** page, select **Use non-secured connections to connect to the published Web server or server farm**.
7. On the **Internal Publishing Details** page, in **Internal Site name**, type the internal Web Services FQDN for your Front End pool (for example, lyncpool01.contoso.local).
8. On the **Internal Publishing Details** page, in **Path (optional)**, type **/*** as the path of the folder to be published, and then select **Forward the original host header instead of the one specified in the Internal site name field**.
9. On the **Public Name Details** page, do the following:
   - Under **Accept Requests for**, select **This domain name**.
   - In **Public Name**, type **lyncdiscover.**<*sipdomain*> (the external Autodiscover Service URL).
   - In **Path**, type **/***.
10. On **Select Web Listener** page, in **Web Listener**, select a Web Listener or use the New Web Listener Definition Wizard to create a new one.
11. On the **Authentication Delegation** page, select **No delegation, and client cannot authenticate directly**.
12. On the **User Set** page, select **All Users**.
13. On the **Completing the New Web Publishing Rule Wizard** page, verify that the web publishing rule settings are correct, and then click **Finish**.
14. In the Forefront TMG list of web publishing rules, double-click the new rule you just added to open **Properties**.
15. On the **Bridging** tab, configure the following:
    - Select **Web server**.
    - Select **Redirect requests to HTTP port**, and type **8080** for the port number.
    - Verify that **Redirect requests to SSL port** is not selected.
16. Click **OK**.
17. Click **Apply** in the details pane to save the changes and update the configuration.
18. Click **Test Rule** to verify that your new rule is set up correctly.
19. Verify that the external Autodiscover Service URL is not defined on any other web publishing rule.

Concepts

Setting Up Reverse Proxy Servers

1.4.2.9.4 Configuring Autodiscover for Hybrid Deployments

Configuring Autodiscover for Hybrid Deployments

See Also

Deployment > Deploying External User Access > Configuring Support for Autodiscover >

***Topic Last Modified:** 2012-12-12*

Hybrid Deployments are configurations that use both the Microsoft Lync Online cloud service and the on premises deployment. In this type of configuration, the Autodiscover service must be able to locate where the user is actually located. That is to say, Autodiscover aids in finding the user account and where the server that hosts the user's account is, regardless if it is in the on premises deployment or in the Lync Online deployment.

For example, if a user's account is hosted on a server in Lync Online, the attempt to locate the user will happen as follows, in a process known as *discoverability*:

- User initiates a connection attempt to the on premises deployment, **contoso.com**.
- The attempt is sent to lyncdiscover.contoso.com, the DNS name associated with the Autodiscover service.
- Autodiscover refers to the assumed registrar pool at the contoso.com on premises deployment and is given information on the user's actual home server hosted in Lync Online. Autodiscover then sends the user a referral to the **lync.com** online Autodiscover service.
- The user initiates a connection attempt to the lync.com online Autodiscover service and is able to locate the user's account and the user's home server.

To enable clients to discover the deployment where the user home server is located, you must configure the Autodiscover service with a new uniform resource locator (URL). Do the following to configure the Autodiscover service.

⊟Configuring Autodiscover for Hybrid Deployments

1. In the topic, Autodiscover Service Requirements, you use Get-CsHostingProvider to retrieve the value of the attribute ProxyFQDN.
2. From the Lync Server Management Shell, type

```
Set-CsHostingProvider -Identity [identity] -AutodiscoverUrl https://we
```

Where [identity] is replaced with the domain name of the shared SIP address space.

Other Resources

Get-CsHostingProvider
Set-CsHostingProvider

1.4.2.10 Publishing Office Web Apps Server Using a Reverse Proxy Server

Publishing Office Web Apps Server Using a Reverse Proxy Server

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2013-02-25*

If you want external users (that is, users logging on from outside your organization’s firewall) to have access to Office Web Apps Server PowerPoint presentations then you will need to use Office Web Apps Server and a reverse proxy server such as Microsoft Forefront Threat Management Gateway. That also means that you will need to create and configure a website publishing rule; that rule will help ensure that users are able to connect to the server. If you do not need to provide access to external users then you do not need to configure a website publishing rule.

To configure a website publishing rule in Forefront Threat Management Gateway complete the following procedure:

1. Click **Start**, click **All Programs**, click **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In Forefront TMG, right-click **Firewall Policy**, point to **New**, and then click **Web Site Publishing Rule**.
3. In the New Web Publishing Rule Wizard, on the **Welcome to the New Web Publishing Rule Wizard** page, type a name for your new rule in the **Web publishing rule name** box (for example, **Office Web Apps Server Rule**) and then click **Next**.
4. On the **Specify Rule Action** page, select **Allow** and then click **Next**.
5. On the **Publishing Type** page, select **Publish a single Web site or load balancer** and then click **Next**.
6. On the **Server Connection Security** page, select **Use SSL to connect to the published Web server or server farm** and then click **Next**.
7. On the **Internal Publishing Details** page, type the FQDN of your Office Web Apps server (for example, **officewebapps01.contoso.com**) in the **Internal site name** box and then click **Next**. The name entered in the **Internal site name** box must appear in the Subject field or the Subject Alternative Name field of the certificate you have assigned to Office Web Apps Server.
8. On the **Internal Publishing Details** page, type **/*** in the **Path (optional)** box and then click **Next**. The /* syntax will help ensure that all the folders and subfolders for the site are published.
9. On the **Public Name Details** page, select **This domain name (type below)** from the **Accept requests for** drop-down list and then type the fully qualified for your Office Web Apps Server in the Public name box. This name should be the name used to access your website. For example, if your site is accessed using the URL http://officewebapps01.contoso.com then you should enter **officewebapps01.contoso.com** in the **Public name** box.
10. Click **Next**.
11. On the **Select Web Listener** page, click **New**.
12. In the New Web Listener Definition Wizard, type a name for the new Web listener (for example, **SSL**) in the **Web listener name** box and then click **Next**.
13. On the **Client Connection Security** page, select **Require SSL secured connections with clients** and then click **Next**.
14. On the **Web Listener IP Addresses** page, select **External**, select **Internal**, and then click **Next**.
15. On the **Listener SSL Certificates** page, select **Use a single certificate for this Web Listener** and then click **Select Certificate**.
16. In the **Select Certificate** dialog box, select the certificate to be used for this Web Listener and then click **Select**.
17. On the **Listener SSL Certificates** page, click **Next**.
18. On the **Authentication Settings** page, select **No Authentication** from the **Select how clients will provide credentials to Forefront TMG** drop-down list, and then click **Next**.
19. On the **Single Sign On Settings** page, click **Next**.
20. On the **Completing the New Web Listener Wizard** page, review the summary of the configuration choices you have made. When ready, click

Finish.

21. On the **Select Web Listener** page, click **Next**.
22. On the **Authentication Delegation** page, select **No delegation, but client may authenticate directly** from the **Select the method used by Forefront TMG to authenticate to the published Web server** drop-down list and then click **Next**.
23. On the **User Sets** page, confirm that the appropriate user sets are listed. By default, this is the **All Users** user set. Click **Add** to add other user sets you may have defined. When complete, click **Next**.
24. On the **Completing the New Web Publishing Rule Wizard** page, click **Finish**.

Note that clicking **Finish** does not mean that you completed the process; that is, this does not automatically apply and enable the new rule. Instead, you will need to click the **Apply** button that will appear in the Forefront TMG user interface. When you click **Apply** the **Configuration Change Description** dialog box will appear. Click **Apply** in that dialog box to enable the new publishing rule.

After your new rule has been applied, you will then need to make some minor modifications to the rule to make sure that users can use the new PowerPoint presentation capabilities. To do that, complete the following procedure:

1. In Forefront TMG, right-click the name of the new publishing rule and then click **Properties**.
2. In the **Properties** dialog box, on the **To** tab, select the option **Forward the original host header instead of the actual one**.
3. On the **Traffic** tab, click **Filtering** and then click **Configure HTTP**.
4. In the **Configuring HTTP policy for rule** dialog box, clear the **Verify normalization** check box and then click **OK**.
5. In the **Properties** dialog box, click **OK**.
6. In Forefront TMG, click **Apply** to enable the changes. When the **Configuration Change Description** dialog box appears, click **Apply**.

After completing the installation you can test your Office Web Apps Server using the procedures in the topic Validating the Configuration of Office Web Apps Server.

1.4.2.11 Configuring SIP Federation, XMPP Federation and Public Instant Messaging

Configuring SIP Federation, XMPP Federation and Public Instant Messaging

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2012-10-16*

Federation, public instant messaging connectivity and Extensible Messaging and Presence Protocol (XMPP) define a different class of external users – Federated users. Users of a federated Lync Server deployment or XMPP deployment have access to a limited set of services and are authenticated by the external deployment. Remote users are members of your Lync Server deployment and have access to all services offered by your deployment.

Public instant messaging connectivity is a special type of federation that allows a Lync Server client to access configured public Instant Messaging partners using the Lync 2013. The current public instant messaging connectivity partners are:

- America Online
- Windows Live
- Yahoo!

A public instant messaging connectivity configuration allows Lync users access to public instant messaging connectivity users by:

- IM and Presence
- Visibility of public instant messaging connectivity contacts in Lync client
- Person to person IM conversations with contacts
- Audio and video calls with Windows Live users

Lync Server federation defines an agreement between your Lync Server deployment and other Office Communications Server 2007 R2 or Lync Server deployments. A Lync Server federated configuration allows Lync users access to federated users by:

- IM and Presence
- Creation of federated contacts in the Lync client

XMPP federation defines an external deployment based on the eXtensible Messaging and Presence Protocol. An XMPP configuration allows Lync users access to allowed XMPP domain users by:

- IM and Presence – person to person only
- Creation of XMPP federated contacts in the Lync client

Important:

The XMPP capability of Lync Server 2013 is tested and supported by Microsoft for instant messaging federation with Google Talk. For any other XMPP systems contact the third-party vendor to verify that they support federation with Lync Server 2013, and for any deployment or troubleshooting recommendations.

Edge Server External Federation, Public Instant Messaging Connectivity and XMPP Users Deployment Process

Phase	Steps	Permissions	Documentation
Determine the options to add to the existing Edge deployment	Run Topology Builder to edit Edge Server settings and create and publish the topology. Your existing Edge topology will replicate changes from the Central Management store to the Edge Server.	Domain Admins group and RTCUniversalServerAdmins group **Note:** You can edit a topology using an account that is a member of the local users group, but publishing a topology requires an account that is a member of the Domain Admins group and the RTCUniversalServerAdmins group	Building an Edge and Director Topology
Prepare for setup	1. Ensure that system prerequisites are met. 2. Configure internal and external DNS records, to support public instant	As appropriate to your organization, as these roles are typically split amongst numerous work groups	Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation

	messaging connectivity, Lync Federation and XMPP Federation 3. Configure ports and protocols at the firewall to support the types of federation that you are deploying 4. Obtain and install public certificates. The time required to obtain certificates depends on which certification authority (CA) issues the certificate. This step is optional at this point in the deployment. If you do not perform this step at this point, you must do it during Edge Server configuration. The Edge Server service cannot be started until certificates are obtained		
Set up Edge Servers for Federation Scenarios	1. Transport the exported topology configuration file to each Edge Server or allow replication to complete 2. Re-Run the Deployment Wizard to install supporting components for Federation 3. Configure the Edge Servers 4. Request and install certificates for each Edge Server 5. Restart the Edge Server services	Administrators group	Setting Up Lync Federation Setting Up Public Instant Messaging Connectivity Setting Up XMPP Federation
Configure support for external user access.	1. Use the Lync Server Control Panel External User Access 2. Configure External Access Policy to enable Communications with federated users or public users	RTCUniversalServer Admins group or user account that is assigned to the CSAdministrator role	Configuring Support for External User Access Configure Media Encryption for Public Providers

	3. Configure SIP Federated Domains to Allow or Block domains 4. Enable SIP Federated Providers for public instant messaging connectivity providers 5. Configure XMPP Federated Partners per XMPP domain		
Verify your Edge Server configuration	Verify server connectivity and replication of configuration data from internal servers	For verification of replication, RTCUniversalServerAdmins group or user account that is assigned to the CSAdministrator roleFor verification of user connectivity, a user for each type of Federated user	Verifying Your Edge Deployment Example XMPP Configuration – XMPP Federation with Google Talk

1.4.2.11.1 Setting Up Lync Federation

Setting Up Lync Federation

See Also

Deployment > Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging >

Topic Last Modified: *2013-01-11*

If you have already deployed you Edge server or servers, adding the federated scenarios features is straight forward. If you have not set up Edge Servers, you must do that first. For details, see: Planning for External User Access in the Planning documentation and Deploying External User Access in the Deployment documentation.

Note:

If you intend to setup any combination of XMPP federation, Lync Federation, or public instant messaging connectivity, you can deploy them concurrently or one at a time. If you configure the options through the Topology Builder and the Lync Server Management shell, then run the Deployment Wizard at the Edge server after configuring the options for one, two or all three federation types, you can reduce the number of steps required.

Setting Up Lync Federation in Topology Builder and the Deployment Wizard

1. On a Front End server, open Topology Builder. Expand Edge pools, then right click your Edge server or Edge server pool. Select Edit properties.
2. In Edit Properties under General, select Enable federation for this Edge pool (Port 5061). Click OK.
3. Click Action, select Topology, select Publish. When prompted on Publish the topology, click Next. When the Publish is finished, click Finish.
4. On the Edge server, open the Lync Server Deployment wizard. Click Install or Update Lync Server System, then click Setup or Remove Lync Server Components. Click Run Again.

5. At Setup Lync Server components, click Next. The summary screen will show actions as they are executed. Once the deployment is done, click View Log to view available log files. Click Finish to complete the deployment.

Important:

You can select this option, but only one Edge pool or Edge Server in your organization can be published externally for federation. All access by federated users, including public instant messaging (IM) users, go through the same Edge pool or single Edge Server. For example, if your deployment includes an Edge pool or single Edge Server deployed in New York and one deployed in London and you enable federation support on the New York Edge pool or single Edge Server, signal traffic for federated users will go through the New York Edge pool or single Edge Server. This is true even for communications with London users, although a London internal user calling a London federated user uses the London pool or Edge Server for A/V traffic.

Configuring Federation with Partners

1. To setup a successful federation with another Microsoft Lync Server 2013, Lync Server 2010, Office Communications Server 2007 R2, or Office Communicator 2007, select the type of federation from the following table and define DNS SRV records, DNS host (A or AAAA for IPv6) and configure policies applicable to the type of federation:

Federation type	DNS Records	Policy Definition	Notes
Discovered Partner Domain	Configure SRV record of the format _sipfederationtls._tcp.<external domain name>Where the port value for the SRV record is TCP 5061 and the **Host offering this service** is defined as sip.<external domain name> – the FQDN of your Access Edge service. See Configure DNS for Edge Support for details on creating the SRV record	Enable or Disable Federation and Public IM Connectivity Enable or Disable Discovery of Federation Partners	Previous versions referred to this type of federation as **Open Enhanced Federation**. The creation of the SRV record is required for this type of federation and is to allow other partners to discover your federation.
Allowed Partner Domain	Configure SRV record of the format _sipfederationtls._tcp.<external domain name>Where the port value for the SRV	Enable or Disable Federation and Public IM Connectivity	Previous versions referred to this type of federation as **Enhanced Federation**. The creation of the SRV record is optional for this type of federation and is to allow other partners to discover your federation. Of course, this is then an **Open Enhanced**

	record is TCP 5061 and the **Host offering this service** is defined as sip.<external domain name> – the FQDN of your Access Edge service. See Configure DNS for Edge Support for details on creating the SRV record		**Federation**, or **Discovered Partner Domain**
Allowed Partner Server	Configure the SIP domain name and the partner Edge Server FQDN as a federation partner in Policies	Enable or Disable Federation and Public IM Connectivity Configure Support for Allowed External Domains Configure Support for Blocked External Domains	This federation type is the definition of a one to one relationship and does not allow for discovery of other federation partners. Each federation partner is configured explicitly. In previous versions, this was known as **Direct Federation**
Hosting Provider and Public IM Provider	No specific DNS requirements are defined for this type of federation	Enable or Disable Federation and Public IM Connectivity Create or Edit Public SIP Federated Providers Create or Edit Hosted SIP Federated Providers	This federation type defines services and hosting providers that you want to configure for your users. Typical uses include configuration for public IM providers like Windows Live Messenger, Yahoo! and AOL, as well as hosting providers such as Lync Online and Office 365 **Important:** • As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License (“PIC USL”) is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to

			continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013). • The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft’s ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down. • More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

1. Define and configure any required DNS host (A or AAAA for IPv6) and DNS SRV records

2. Define and configure any policies using the Lync Server Control Panel or by using the Lync Server Management Shell and the appropriate cmdlets. For details on the Lync Server Management Shell cmdlets, see Federation and External Access Cmdlets

Other Resources

Scenarios for Federation, Public Instant Messaging Connectivity, and XMPP Federation
Managing Federation and External Access to Lync Server 2013

1.4.2.11.1.1 Configure Policies to Control Federated User Access

Configure Policies to Control Federated User Access

See Also

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up Lync Federation >

Topic Last Modified: *2012-11-01*

When you configure policies to support communications with federated partners, the policies apply to users of federated domains. You can configure one or more external user access policies to control whether users of federated domains can collaborate with your Lync Server 2013 users. To control federated user access, you can configure policies at the global, site, and user level. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

Note:

You can configure policies to control federated user access, even if you have not enabled federation for your organization. However, the policies that you configure are in effect only when you have federation enabled for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation. Additionally, if you specify a user policy to control federated user access, the policy applies only to users that are enabled for Lync Server 2013 and configured to use the policy. For details about specifying federated users that can sign in to Lync Server 2013, see Assign an External User Access Policy to a Lync Enabled User in the Deployment documentation or the Operations documentation.

To configure a policy to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do one of the following:
   - To configure the global policy to support federated user access, click the global policy, click **Edit**, and then click **Show details**.
   - To create a new site policy, click **New**, and then click **Site policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
   - To create a new user policy, click **New**, and then click **User policy**. In **New External Access Policy**, create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnableFederatedUsers** for a user policy that enables communications for federated domain users).

- To change an existing policy, click the appropriate policy listed in the table, click **Edit**, and then click **Show details**.

5. (Optional) If you want to add or edit a description, specify the information for the policy in **Description**.
6. Do one of the following:
    - To enable federated user access for the policy, select the **Enable communications with federated users** check box.
    - To disable federated user access for the policy, clear the **Enable communications with federated users** check box.
7. Click **Commit**.

To enable federated user access, you must also enable support for federation in your organization. For details, see Enable or Disable Federation and Public IM Connectivity.

If this is a user policy, you must also apply the policy to users that you want to be able to collaborate with federated users. For details, see Assign an External User Access Policy to a Lync Enabled User.

To configure an existing policy using Windows PowerShell to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

```
Set-CsExternalAccessPolicy -Identity <name of global, site or user pol
```

An example command that will set the global policy for Federated user access to enabled, XMPP domain access to enabled, Remote user access to enabled, Public provider access to enabled, and grant the ability to use audio and video for public providers that support it:

```
Set-CsExternalAccessPolicy -Identity global -EnableFederationAccess $t
```

Tip:

The parameter "EnablePublicCloudAudioVideoAccess" does not have a corresponding selection in the Lync Server Control Panel

To create a new policy using Windows PowerShell to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

```
New-CsExtenalAccessPolicy -Identity <name of site or user policy - you
```

An example of creating a new site policy:

```
New-CsExternalAccessPolicy -Identity site:Redmond -EnableFederationAcc
```

To delete or reset a policy using Windows PowerShell to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins

group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.

2. Type the following in the Lync Server Management Shell

```
Remove-CsExternalAccessPolicy -Identity <name of global, site or user
```

An example of resetting the global policy (The global policy can only have its setting removed. The policy cannot be deleted):

```
Remove-CsExternalAccessPolicy -Identity global
```

To remove a site policy, type:

```
Remove-CsExternalAccessPolicy -Identity site:Redmond
```

Deletes the site policy Redmond. To delete a user policy named UserEAPPolicy, type:

```
Remove-CsExternalAccessPolicy -Identity UserEAPPolicy
```

Tasks

Enable or Disable Federation and Public IM Connectivity
Assign an External User Access Policy to a Lync Enabled User

Other Resources

Manage SIP Federated Domains for Your Organization
Manage SIP Federated Providers for Your Organization
Set-CsExternalAccessPolicy
New-CsExternalAccessPolicy
Get-CsExternalAccessPolicy
Remove-CsExternalAccessPolicy
Grant-CsExternalAccessPolicy

1.4.2.11.2 Setting Up Public Instant Messaging Connectivity

Setting Up Public Instant Messaging Connectivity

Deployment > Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging >

Topic Last Modified: *2012-09-08*

If your organization wants to support public instant messaging (IM) connectivity with AOL, you cannot use the Lync Server Deployment Wizard to request the certificate. Instead, perform the steps in the following procedure.

Setting Up Public Instant Messaging Connectivity

1. On a Front End server, open Topology Builder. Expand Edge pools, then right click your Edge server or Edge server pool. Select Edit properties.
2. In Edit Properties under General, select Enable federation for this Edge pool (Port 5061). Click OK.
3. Click Action, select Topology, select Publish. When prompted on Publish the topology, click Next. When the Publish is finished, click Finish.
4. On the Edge server, open the Lync Server Deployment wizard. Click Install or Update Lync Server System, then click Setup or Remove Lync Server Components. Click Run Again.
5. At Setup Lync Server components, click Next. The summary screen will show actions as they are executed. Once the deployment is done, click View Log to view available log files. Click Finish to complete the deployment.

To create a certificate request for the external interface of the Edge Server to support public IM connectivity with AOL

1. When the required template is available to the CA, use the following

Windows PowerShell cmdlet from at the Edge Server to request the certificate

```
Request-CsCertificate -New -Type AccessEdgeExternal  -Output C:\ <cert
```

The default certificate name of the template used for Lync Server is Web Server. Only specify the <template name> if you need to use a template that is different from the default template.

Important:

If your organization wants to support public IM connectivity with AOL, you must use Windows PowerShell instead of the Certificate Wizard to request the certificate to be assigned to the external edge for the Access Edge service. This is because the Certificate Authority (CA) Web Server template that the Certificate Wizard uses to request a certificate does not support client EKU configuration. Before using Windows PowerShell to create the certificate, the CA administrator must create and deploy a new template that supports client EKU.

1.4.2.11.2.1 Configure Media Encryption for Public Providers

Configure Media Encryption for Public Providers

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up Public Instant Messaging Connectivity >

***Topic Last Modified:** 2012-12-23*

For details about licensing requirements and how to complete the provisioning process, see the "Public IM Connectivity Provisioning Guide for Microsoft Lync Server, Office Communications Server, and Live Communications Server" at http://go.microsoft.com/fwlink/p/?linkId=155970

If you are implementing audio/video (A/V) federation with Windows Live Messenger, there are two parameters that you need to modify: the Lync Server encryption level and the EnablePublicCloudAccess policy. By default, the encryption level is set to Required. You must change this setting to Supported. If the EnablePublicCloudAccess policy is set to false, this needs to be set to **True**. You can do this from the Lync Server Management Shell.

Important:

More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard Client Access License (CAL). Next year, Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

Configure Federation for Windows Live

1. Start the Lync Server Management Shell on the Front End server: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. From the command prompt, type the following commands:

```
Set-CsMediaConfiguration -EncryptionLevel SupportEncryption
```

```
Set-CsExternalAccessPolicy Global -EnablePublicCloudAccess $true -Enab
```

Note:

This is required step because Windows Live Messenger does not support encryption of audio/video. The command sets your global policy to a support encryption setting instead of requiring encryption of the audio/video data. Clients that support encryption will still use encryption, such as Lync 2013.

1.4.2.11.2.2 Configure Policies to Control Public User Access

Configure Policies to Control Public User Access

See Also

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up Public Instant Messaging Connectivity >

Topic Last Modified: *2013-01-11*

Public instant messaging (IM) connectivity enables users in your organization to use IM to communicate with users of IM services provided by public IM service providers, including the Windows Live network of Internet services, Yahoo!, and AOL. You configure one or more external user access policies to control whether public users can collaborate with internal Lync Server users. Public instant messaging connectivity is an added feature that relies on configuration of your deployment and users. It also depends on the provisioning of the service at the public IM provider. For information on how to provision your deployment to use the public providers, see the "Public IM Connectivity Provisioning Guide for Microsoft Lync Server, Office Communications Server, and Live Communications Server" guide: http://go.microsoft.com/fwlink/?LinkId=269821

◆Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

To access the Microsoft Lync Server Public IM Connectivity Provisioning site, use the following link: http://go.microsoft.com/fwlink/p/?linkId=212638

To control public user access, you can configure policies at the global, site, and user level. For details about the types of policies that you can configure, see Configuring Support for External User Access in the Deployment documentation or the Planning documentation. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

In the case of IM invitations, the response depends on the client software. The request is accepted unless external senders are explicitly blocked by a user-configured rule (that is, the settings in the user's client **Allow** and **Block** lists). Additionally, IM invitations can be blocked if a user elects to block all IM from users who are not on his or her **Allow** list.

Note:
You can configure policies to control public user access, even if you have not enabled federation for your organization. However, the policies that you configure are in effect only when you have federation enabled for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation. Additionally, if you specify a user policy to control public user access, the policy applies only to users that are enabled for Lync Server and configured to use the policy. For details about specifying public users that can sign in to Lync Server, see Assign an External User Access Policy to a Lync Enabled User in the Deployment documentation or the Operations documentation.

Use the following procedure to configure a policy to support access by users of one or more public IM providers.

⊟To configure an external access policy to support public user access

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do one of the following:
   - To configure the global policy to support public user access, click the global policy, click **Edit**, and then click **Show details**.
   - To create a new site policy, click **New**, and then click **Site policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
   - To create a new user policy, click **New**, and then click **User policy**. In **New External Access Policy**, create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnablePublicUsers** for a user policy that enables communications for public users).
   - To change an existing policy, click the appropriate policy listed in the table, click **Edit**, and then click **Show details**.
5. (Optional) If you want to add or edit a description, specify the information for the policy in **Description**.
6. Do one of the following:
   - To enable public user access for the policy, select the **Enable communications with public users** check box.
   - To disable public user access for the policy, clear the **Enable communications with public users** check box.
7. Click **Commit**.

To enable public user access, you must also enable support for federation in your organization. For details, see Configure Policies to Control Federated User Access.

If this is a user policy, you must also apply the policy to public users that you want to be able to collaborate with public users. For details, see Assigning Per-User Policies.

Tasks

Create or Edit Public SIP Federated Providers

Other Resources

Manage SIP Federated Providers for Your Organization

1.4.2.11.3 Setting Up XMPP Federation

Setting Up XMPP Federation

See Also

Deployment > Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging >

Topic Last Modified: *2012-12-03*

To deploy the XMPP Proxy on the Edge Server, you must configure the Edge Server for XMPP federation. To do this, you do the following steps.

⊟Setting Up XMPP Federation

1. Log on to the computer where the Lync Server Deployment Wizard is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. On the Front End server, open the Lync Server Deployment wizard. Click Install or Update Lync Server System, then click Setup or Remove Lync Server Components. Click Run Again.
3. At Setup Lync Server components, click Next. The summary screen will show actions as they are executed. Once the deployment is done, click View Log to view available log files. Click Finish to complete the deployment.
4. On the Edge server, open the Lync Server Deployment wizard. Click Install or Update Lync Server System, then click Setup or Remove Lync Server Components. Click Run Again.
5. At Setup Lync Server components, click Next. The summary screen will show actions as they are executed. Once the deployment is done, click View Log to view available log files. Click Finish to complete the deployment.
6. On the Edge Server, in the Deployment Wizard, next to Step 3: Request, Install, or Assign Certificates, click Run again.

   Tip:

   If you are deploying the Edge Server for the first time, you will see Run instead of Run Again.

7. On the Available Certificate Tasks page, click Create a new certificate request.
8. On the Certificate Request page, click External Edge Certificate.
9. On the Delayed or Immediate Request page, select the Prepare the request now, but send it later check box.
10. On the Certificate Request File page, type the full path and file name of the file to which the request is to be saved (for example, c:\cert_exernal_edge.cer).
11. On the Specify Alternate Certificate Template page, to use a template other than the default WebServer template, select the Use alternative certificate template for the selected certification authority check box.
12. On the Name and Security Settings page, do the following:
    12.a. In Friendly name, type a display name for the certificate
    12.b. In Bit length, specify the bit length (typically, the default of 2048)
    12.c. Verify that the Mark certificate private key as exportable check box is selected
13. On the Organization Information page, type the name for the organization and the organizational unit (for example, a division or department)
14. On the Geographical Information page, specify the location information
15. On the Subject Name/Subject Alternate Names page, the information to be automatically populated by the wizard is displayed. If additional subject alternative names are needed, you specify them in the next two steps
16. On the SIP Domain Setting on Subject Alternate Names (SANs) page, select the domain check box to add a sip.<sipdomain> entry to the subject alternative names list.

17. On the Configure Additional Subject Alternate Names page, specify any additional subject alternative names that are required

> **Tip:**
>
> If the XMPP proxy is installed, by default the domain name (such as contoso.com) is populated in the SAN entries. If you require more entries, add them in this step.

18. On the Request Summary page, review the certificate information to be used to generate the request.
19. After the commands finish running, you can View Log, or click Next to continue.
20. On the Certificate Request File page, you can view the generated certificate signing request (CSR) file by clicking View or exit the Certificate Wizard by clicking Finish.
21. Copy the request file and submit to your public certification authority.
22. After receiving, importing and assigning the public certificate, you must stop and restart the Edge Server services. You do this by typing in the Lync Server Management console:

```
Stop-CsWindowsService
```

```
Start-CsWindowsService
```

23. To configure DNS for XMPP federation, you add the following SRV record to external DNS:_xmpp-server._tcp.<domain name> The SRV record will resolve to the access edge FQDN of the Edge server, with a port value of 5269. Additionally, you configure an 'A' host record (for example, xmpp.contoso.com) that points to the IP address of the Access Edge Server.

> **Important:**
>
> If you have Edge pools in multiple sites, we recommend that you add multiple SRV records for XMPP federation. Add a SRV record for every Edge pool in your organization, and give each of those SRV records a different priority. When all Edge pools are running, XMPP requests will all be handled by the Edge pool with the first priority, but if that Edge pool goes down you won't then have to add a new SRV record to regain XMPP federation functionality.

24. Configure a new External Access Policy to enable all users by opening the Lync Server Management Shell on the Front End and typing:

```
New-CsExternalAccessPolicy -Identity <name of policy to create.  If si
```

```
New-CsExternalAccessPolicy -Identity FedPic -EnableFederationAcces $tr
```

```
Get-CsUser | Grant-CsExternalAccessPolicy -PolicyName FedPic
```

Enable XMPP Access for External Users by typing:

```
Set-CsExternalAccessPolicy -Identity <name of the policy being used> E
```

```
Set-CsExternalAccessPolicy -Identity FedPic -EnableXmppAccess $true
```

25. On the Edge Server where the XMPP Proxy is deployed, open a Command Prompt or a Windows PowerShell™ command-line interface and type the following:

```
Netstat -ano | findstr 5269
```

```
Netstat -ano | findstr 23456
```

The command **netstat –ano** is a network statistics command, the parameters **–ano** request that netstat display all connections and listening ports, address and ports are displayed in a numerical form, and that the owning process ID is associated with each connection. The character **|** defines a pipe to the next command, **findstr**, or find string. The number 5269 and 23456 that is passed to findstr as a parameter instructs findstr to search the output of netstat for the strings 5269 and 23456. If XMPP is correctly configured, the result of the commands should result in listening and established connections, both on the external (port 5269) and the internal (port 23456) interfaces of the Edge Server.

If the commands do not return established or listening ports on 5269 and 23456, check the following:

⊟Troubleshooting XMPP Federation

1. To determine if the XMPP Proxy is running, do the following:
2. Log on to the Edge server that is running the XMPP Proxy service as a member of the local administrator’s group.
3. Click **Start**, click **All Programs**, click **Administrative Tools**, click **Services**
4. In Services, locate Lync Server XMPP Translating Gateway Proxy. The service should be in the **Started** state. If it is not started, click the **Start** icon in the toolbar. The icon appears as a green, right-pointing arrow.
5. Confirm that the service has changed to **Started**. If it has successfully started, close **Services** and continue.

   If ther service has not successfully started, from Administrative Tools, open Event Viewer and refer to the errors and warnings in the **Lync Server** portion under **Applications and Services Logs**.
6. Once the **Lync Server XMPP Translating Gateway** service is running, recheck the netstat commands used previously. If you are not seeing established or listening sessions, check and ensure that the **XMPP Federation Route** is correctly configured in Topology Builder
7. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
8. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
9. In Topology Builder, select the site for the XMPP federation route and review to confirm that the **Site federation route assignment** for **XMPP federation** shows your Edge Server or Edge pool as the selected XMPP federation route assignment.

   If the route assignment is incorrect or is not set, right-click the site, click **Edit Properties**. Select the XMPP federation check box and then select the correct Edge Server or Edge pool.
10. Publish the topology. For details, see Publish Your Topology

Tip:
Though not required and typically not necessary, you may find that you will need to restart the Edge Servers

11. Using the netstat process used previously, confirm that the Edge Server is now listening or has established sessions on port 5269 and port 23456.
12. If you still are not seeing the expected sessions, check the Event Viewer for possible contributing causes for the communication problem.

Tasks

Example XMPP Configuration – XMPP Federation with Google Talk

Other Resources

Manage XMPP Federated Partners for Your Organization

1.4.2.11.3.1 Configure Policies to Control XMPP Federated User Access

Configure Policies to Control XMPP Federated User Access

See Also

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up XMPP Federation >

Topic Last Modified: *2012-11-01*

This is preliminary documentation and is subject to change. Blank topics are included as placeholders.

When you configure policies for support of extensible messaging and presence protocol (XMPP) federated partners, the policies apply to users of XMPP federated domains, but not to users of session initiation protocol (SIP) instant messaging (IM) service providers (for example, Windows Live), or SIP federated domains. You configure an **XMPP Federated Partner** for each XMPP federated domain that you want to allow your users to add contacts and communicate with. XMPP federated partners policies are only available in a single scope, though it is not defined as a global policy, acts as a global policy. To define a global, site or user policy for XMPP Federation Partners, you configure the policy scope by first creating and configuring the External Access Policy for the scope you require. For details about the types of policies that you can configure for external access and federation, see Managing Federation and External Access to Lync Server 2013 in the Operations documentation.

Note:

All **Federation and External Access** policies are applied through in-band provisioning. The policies that apply to the user, belong to a site, or are global in scope are communicated to the client during login. You can configure policies to control XMPP federated partner access, even if you have not enabled XMPP federation for your organization. However, the policies that you configure take effect only when you have XMPP partner federation deployed, enabled and configured for your organization. For details about deploying and configuring XMPP partner federation, see Configuring SIP Federation, XMPP Federation and Public Instant Messaging in the Deployment documentation. Additionally, if you specify a user policy in External Access Policy to control XMPP federated partners, the policy applies only to users that are enabled for Lync Server 2013 and configured to use the policy.

⊟To edit a global policy for XMPP federated partners

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do the following for the global policy:
5. Click the global policy, click **Edit**, and then click Show details.
6. Provide a description for the Global policy (optional).
7. Select **Enable communications with federated users**.
8. Select **Enable communications with XMPP federated users**.
9. Click **Commit** to save your changes to the Global policy.

⊟To create a site or user policy for XMPP federated partners

1. Click **New**, and then click **Site policy** or **User policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
2. Provide a description for the Site policy (optional).
3. In the site or user policy, select **Enable communications with federated users**.
4. Select **Enable communications with XMPP federated users**.
5. Click **Commit** to save your changes to the site or user policy.

⊟To edit an existing policy for XMPP federated partners

1. To change an existing policy, select the appropriate policy in the list, click

Edit, and then click **Show details**.

2. Change or update the description for the policy (optional).
3. Select or unselect **Enable communications with federated users**.
4. Select or unselect **Enable communications with XMPP federated users**.
5. Click **Commit** to save your changes to the policy.

⊟To edit an existing policy for XMPP federated partners by using Windows PowerShell

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   Set-CsExternalAccessPolicy -Identity <name of global, site or user pol
   ```

   An example command that will set the global policy for Federated user access to True (enabled) and XMPP domain access to True (enabled):

   ```
   Set-CsExternalAccessPolicy -Identity global -EnableFederationAccess $t
   ```

⊟To create a site or user policy for XMPP federated partners using Windows PowerShell

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   New-CsExternalAccessPolicy -Identity <name of global, site or user pol
   ```

   An example command that will set a site policy for the Redmond site for Federated user access to enabled and XMPP domain access to enabled:

   ```
   New-CsExternalAccessPolicy -Identity site:Redmond -EnableFederationAcc
   ```

⊟To delete an existing policy for XMPP federated partners by using Windows PowerShell

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   Remove-CsExternalAccessPolicy -Identity <name of global, site or user
   ```

   An example command that will delete a user policy:

   ```
   Remove-CsExternalAccessPolicy -Identity EAPUserPolicySetXMPP
   ```

4. An example command that will reset the global policy to defaults:

   ```
   Remove-CsExternalAccessPolicy -Identity global
   ```

Tasks

Assign an External User Access Policy to a Lync Enabled User
Enable or Disable Federation and Public IM Connectivity

Other Resources

Manage XMPP Federated Partners for Your Organization
Set-CsExternalAccessPolicy
New-CsExternalAccessPolicy
Get-CsExternalAccessPolicy
Remove-CsExternalAccessPolicy
Grant-CsExternalAccessPolicy

1.4.2.12 Deploying Mobility

Deploying Mobility

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2012-09-08*

When you deploy the Lync Server 2013 mobility feature, mobile users can use supported mobile devices for Lync functionality such as instant messaging (IM), presence, and contacts.

For details about requirements for deploying the mobility feature, see Planning for Mobility.

This section guides you through the steps for deploying and verifying the mobility and automatic discovery features.

- Creating DNS Records for the Autodiscover Service
- Modifying Certificates for Mobility
- Configuring the Reverse Proxy for Mobility
- Configuring Autodiscover for Mobility with Hybrid Deployments
- Verifying Your Mobility Deployment
- Configuring for Push Notifications
- Configuring Mobility Policy

1.4.2.12.1 Creating DNS Records for the Autodiscover Service

Creating DNS Records for the Autodiscover Service

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2012-10-05*

To support autodiscovery for Lync Mobile users, you need to create the following Domain Name System (DNS) records:

- An internal DNS record to support mobile users who connect from within your organization's network
- An external, or public, DNS record to support mobile users who connect from the Internet

Or

- An external, or public, DNS record to support mobile users who connect from the Internet

You must create an internal DNS record and an external DNS record for each SIP domain.

The DNS records can be either A (host) records or CNAME records. The following procedures describe how to create internal and external DNS records. For more details about the DNS requirements for mobile users, see Technical Requirements for Mobility.

⊟To create DNS CNAME records

1. Log on to a DNS server as follows:
   - To create an internal DNS record, log on to a DNS server in your network as a member of the Domain Admins group or a member of the DnsAdmins group.
   - To create an external DNS record, connect to your public DNS provider.
2. Open the DNS administrative snap-in: Click **Start**, click **Administrative Tools**, and then click **DNS**.
3. Do one of the following:
   - For an internal DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your Active Directory domain (for example, contoso.local).

     > **Note:**
     > This domain is the Active Directory domain where your Lync Server 2013 Director pool and Front End pool are installed.

   - For an external DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).
4. Verify that a host A record exists for your Director pool as follows:
   - For an internal DNS record, a host A record should exist for the internal Web Services fully qualified domain name (FQDN) for your Director pool (for example, lyncwebdir01.contoso.local).
   - For an external DNS record, a host A record should exist for the external web services FQDN for your Director pool (for example, lyncwebextdir.contoso.com).
5. Verify that a host A record exists for your Front End pool as follows:
   - For an internal DNS record, a host A record should exist for the internal Web Services FQDN for your Front End pool (for example, lyncwebpool01.contoso.local).
   - For an external DNS record, a host A record should exist for the external Web Services FQDN for your Front End pool (for example, lyncwebextpool01.contoso.com).
6. For an internal DNS record, in the console tree of your DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).

   > **Note:**
   > If you are creating an external DNS record, **Forward Lookup Zones** is already expanded for your SIP domain from step 3.

7. Right-click the SIP domain name, and then click **New Alias (CNAME)**.
8. In **Alias name**, type one of the following:
   - For an internal DNS record, type lyncdiscoverinternal as the host name for the internal Autodiscover Service URL.
   - For an external DNS record, type lyncdiscover as the host name for the external Autodiscover Service URL.
9. In **Fully qualified domain name (FQDN) for target host**, do one of the following:
   - For an internal DNS record, type or browse to the internal Web Services FQDN for your Director pool (for example, lyncwebdir01.contoso.local), and then click **OK**.
   - For an external DNS record, type or browse to the external Web Services FQDN for your Director pool (for example, lyncwebextdir.contoso.com), and then click **OK**.

   > **Note:**
   > If you do not use a Director, use the internal and external Web Services FQDN for the Front End pool, or, for a single server, the FQDN for the Front End Server or Standard Edition server.

Important:
You must create a new Autodiscover CNAME record in the forward lookup zone of each SIP domain that you support in your Lync Server 2013 environment.

To create DNS A records

1. Log on to a DNS server as follows:
   - To create an internal DNS record, log on to a DNS server in your network as a member of the Domain Admins group or a member of the DnsAdmins group.
   - To create an external DNS record, connect to your public DNS provider.
2. Open the DNS administrative snap-in: Click **Start**, click **Administrative Tools**, and then click **DNS**.
3. Do one of the following:
   - For an internal DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your Active Directory domain (for example, contoso.local).

     Note:
     This domain is the Active Directory domain where your Lync Server 2013 Director pool and Front End pool are installed.
   - For an external DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).
4. Verify that a host A (for IPv6, AAAA) record exists for your Director pool as follows:
   - For an internal DNS record, a host A (for IPv6, AAAA) record should exist for the internal Web Services FQDN for your Director pool (for example, lyncwebdir01.contoso.local).
   - For an external DNS record, a host A (for IPv6, AAAA) record should exist for the external Web Services FQDN for your Director pool (for example, lyncwebextdir.contoso.com).
5. Verify that a host A (for IPv6, AAAA) record exists for your Front End pool as follows:
   - For an internal DNS record, a host A (for IPv6, AAAA) record should exist for the internal Web Services FQDN for your Front End pool (for example, lyncwebpool01.contoso.local).
   - For an external DNS record, a host A (for IPv6, AAAA) record should exist for the external Web Services FQDN for your Front End pool (for example, lyncwebextpool01.contoso.com).
6. For an internal DNS record, in the console tree of your DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).

   Note:
   If you are creating an external DNS record, **Forward Lookup Zones** is already expanded for your SIP domain from step 3.
7. Right-click the SIP domain name, and then click **New Host (A or AAAA)**.
8. In **Name**, type the host name as follows:
   - For an internal DNS record, type lyncdiscoverinternal as the host name for the internal Autodiscover Service URL.
   - For an external DNS record, type lyncdiscover as the host name for the external Autodiscover Service URL.

   Note:
   The domain name is assumed from the zone in which the record is defined and, therefore, does not need to be entered as part of the A record.
9. In **IP Address**, type the IP address as follows:
   - For an internal DNS record, type the internal Web Services IP address of the Director (or, if you use a load balancer, type the virtual IP (VIP) of the

Director load balancer).

Note:
If you do not use a Director, type the IP address of the Front End Server or Standard Edition server, or, if you use a load balancer, type the VIP of the Front End pool load balancer.

- For an external DNS record, type the external or public IP address of the reverse proxy.

10.Click **Add Host**, and then click **OK**.
11.To create an additional A record, repeat steps 8 through 10.

Important:
You must create a new Autodiscover A record in the forward lookup zone of each SIP domain that you support in your Lync Server 2013 environment.

12.When you are finished creating A (for IPv6, AAAA) records, click **Done**.

1.4.2.12.2 Modifying Certificates for Mobility

Modifying Certificates for Mobility

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2012-10-18*

The certificates for your Director pool, Front End pool, and reverse proxy require additional subject alternative name entries to support secure connections with mobile clients. For details about certificate requirements for mobility, see Technical Requirements for Mobility.

Note:
You can use the **Get-CsCertificate** cmdlet to view information about the currently assigned certificates. However, the default view truncates the properties of the certificate and does not display all values in the SubjectAlternativeNames property. You can use the **Get-CsCertificate** , **Request-**CsCertificate and the **Set-CsCertificate** cmdlets to view some information and to request and assign certificates. However, it’s not the best method to use if you are unsure of the properties of the subject alternative names (SAN) on the current certificate. To view the certificate and all property members, it is suggested to use the Certificates snap-in the *Microsoft Management Console (MMC)* or to use the Lync Server Deployment Wizard. In the Lync Server Deployment Wizard, you can use the Certificate Wizard to view the certificate properties. The procedures for viewing, requesting and assigning a certificate using the Lync Server Management Shell and the *Microsoft Management Console (MMC)* are detailed in the following procedures. To use the Lync Server Deployment Wizard, see details here if you have deployed the optional Director or Director pool: Configure Certificates for the Director. For the Front End Server or Front End pool, see the details here: Configure Certificates for Servers
The initial steps in this procedure are preparation steps, to orient you as to what role the current certificates play. By default, the certificates will not have a lyncdiscover.<sipdomain> or lyncdiscoverinternal.<internal domain name> entry unless you have previously installed Mobility Services or have prepared your certificates in advance. This procedure uses the example SIP domain name ‘contoso.com’ and the example internal domain name ‘contoso.net’.
The default certificate configuration for Lync Server 2013 and Lync Server 2010 is to use a single certificate (named ‘Default’) with the purposes Default (for all purposes except for the web services), WebServicesExternal and WebServicesInternal. An optional configuration is to use separate certificates for each purpose. Certificates can be managed by using the Lync Server Management Shell and Windows PowerShell cmdlets, or by using the Certificate Wizard in the Lync Server Deployment Wizard.

⊟To update certificates with new subject alternative names using the Lync

Server Management Shell

1. Log on to the computer using an account that has local administrator rights and permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Find out what certificates have been assigned to the server and for which type of use. You need this information in the next step to assign the updated certificate. At the command line, type:

   ```
   Get-CsCertificate
   ```

4. Look in the output from the previous step to see whether a single certificate is assigned for multiple uses or whether a different certificate is assigned for each use. Look in the Use parameter to find out how a certificate is used. Compare the Thumbprint parameter for the displayed certificates to see if the same certificate has multiple uses.
5. Update the certificate. At the command line, type:

   ```
   Set-CsCertificate -Type <type of certificate as displayed in the Use p
   ```

   For example, if the **Get-CsCertificate** cmdlet displayed a certificate with Use of Default, another with a Use of WebServicesInternal, and another with a Use of WebServicesExternal, and they all had the same Thumbprint value, at the command line, type:

   ```
   Set-CsCertificate -Type Default,WebServicesInternal,WebServicesExterna
   ```

   Important:

   If a separate certificate is assigned for each use (the Thumbprint value is different for each certificate), it is important that you do not run the **Set-CsCertificate** cmdlet with multiple types. In this case, run the **Set-CsCertificate** cmdlet separately for each use. For example:

   ```
   Set-CsCertificate -Type Default -Thumbprint <Certificate Thumbprint>
   Set-CsCertificate -Type WebServicesInternal -Thumbprint <Certificate T
   Set-CsCertificate -Type WebServicesExternal -Thumbprint <Certificate T
   ```

6. To view the certificate, click **Start**, click **Run...**. Type MMC to open the Microsoft Management Console.
7. From the MMC menu, select **File**, select **Add/Remove snap-in...**, select Certificates. Click **Add**. When prompted, select **Computer account**, then click **Next**.
8. If this is the computer where the certificate is located, select **Local computer**. If the certificate is located on another computer, select **Another computer**, type in the fully qualified domain name of the computer or click **Browse** In **Enter the object name to select**, type the name of the computer. Click **Check Names**. When the name of the computer is resolved, it will be underlined. Click **OK**, then click **Finish**. Click **OK** to commit the selection and close the **Add or Remove Snap-ins** dialog.
9. To view the properties of the certificate, expand **Certificates**, expand **Personal**, and select **Certificates**. Select the certificate to view, right-click on the certificate and select **Open**.
10. In the **Certificate** view, select **Details**. From here, you can select the certificate subject name by selecting **Subject** and the assigned subject name and associated properties are displayed.
11. To view the assigned subject alternative names, select **Subject Alternative Name**. All assigned subject alternative names are displayed. The subject alternative names that are found in the property are of type **DNS Name** by default. You should see the following members (all of which should be fully qualified domain names as represented in DNS host (A or, if IPv6 AAAA) records:
    - Pool name for this pool, or the single server name if this is not a pool
    - Server name that the certificate is assigned to

- Simple URL records, typically meet and dialin
- Web services internal and Web services external names (for example, webpool01.contoso.net, webpool01.contoso.com), based on choices made in Topology Builder and over-ridden web services selections.
- If already assigned, the lyncdiscover.<sipdomain> and lyncdiscoverinternal.<sipdomain> records.

The last item is what you are most interested in – if there is a lyncdiscover and lyncdiscoverinternal SAN entry.

Once you have this information, you can close the certificate view and the MMC.

12. If an Autodiscover Service subject alternative name is missing, and you are using a single Default certificate for the Default, WebServicesInternal and WebServiceExternal types, do the following:
    - At the Lync Server Management Shell command line prompt, type:

      ```
      Request-CsCertificate -New -Type Default,WebServicesInternal
      ```

      If you have many SIP domains, you cannot use the new AllSipDomain parameter. Instead, you must use DomainName parameter. When you use the DomainName parameter, you must define the FQDN for the lyncdiscoverinternal and lyncdiscover records. For example:

      ```
      Request-CsCertificate -New -Type Default,WebServicesInternal
      ```

    - To assign the certificate, type the following:

      ```
      Set-CsCertificate -Type Default,WebServicesInternal,WebServi
      ```

      Where "Thumbprint" is the thumbprint displayed for the newly issued certificate.

13. For a missing internal Autodiscover subject alternative names when using separate certificates for Default, WebServicesInternal, and WebServicesExternal, do the following:
    - At the Lync Server Management Shell command line prompt, type:

      ```
      Request-CsCertificate -New -Type WebServicesInternal -Ca dc\
      ```

      If you have many SIP domains, you cannot use the new AllSipDomain parameter. Instead, you must use DomainName parameter. When you use the DomainName parameter, you must use an appropriate prefix for the SIP domain FQDN. For example:

      ```
      Request-CsCertificate -New -Type WebServicesInternal -Ca dc\
      ```

    - For a missing external Autodiscover subject alternative name, at the command line, type:

      ```
      Request-CsCertificate -New -Type WebServicesExternal -Ca dc\
      ```

      If you have many SIP domains, you cannot use the new AllSipDomain parameter. Instead, you must use DomainName parameter. When you use the DomainName parameter, you must use an appropriate prefix for the SIP domain FQDN. For example:

      ```
      Request-CsCertificate -New -Type WebServicesExternal -Ca dc\
      ```

    - To assign the individual certificate types, type the following:

      ```
      Set-CsCertificate -Type Default -Thumbprint <Certificate Thu
      Set-CsCertificate -Type WebServicesInternal -Thumbprint <Cer
      Set-CsCertificate -Type WebServicesExternal -Thumbprint <Cer
      ```

      Where "Thumbprint" is the thumbprint displayed for the newly issued individual certificates.

Configuring the Reverse Proxy for Mobility

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2012-09-08*

If you want to use automatic discovery for mobile device clients, you need to modify an existing or create a new web publishing rule for the reverse proxy whether or not you update the subject alternative name lists on the reverse proxy certificates.

If you decide to use HTTPS for initial Lync Server 2013 Autodiscover Service requests and update the subject alternative names lists on the reverse proxy certificates, you need to assign the updated public certificate to the Secure Sockets Layer (SSL) Listener on your reverse proxy. For details about the required subject alternative name entries, see Technical Requirements for Mobility. You then need to modify the existing listener for the external web services or create a new web publishing rule for the external Autodiscover Service URL. If you do not already have a web publishing rule for the external Lync Server 2013 Web Services URL for your Front End pool, you also need to publish a rule for that.

Note:

The reverse proxy publishing rule and listener can service both the external web services and the Autodiscover Service, as long as the certificate assigned to the listener contains the necessary subject name and subject alternative names for both. For details on the default configuration of the web listener and publishing rule, see Setting Up Reverse Proxy Servers for more details.

If you decide to use HTTP for initial Autodiscover Service requests so that you do not need to update subject alternative names for the reverse proxy, you need to create or modify a web publishing rule for port 80.

The procedures in this section describe how to create or modify the web publishing rules in Microsoft Forefront Threat Management Gateway 2010 for automatic discovery.

Note:

These procedures assume that you have installed the Standard Edition of Forefront Threat Management Gateway (TMG) 2010. If you are using another reverse proxy, the procedures are similar, but will need to be mapped to the documentation for the third-party product.

⊟To create a web publishing rule for the external Autodiscover URL

1. Click **Start**, point to **Programs**, point to **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, point to **New**, and then click **Web Site Publishing Rule**.
3. On the **Welcome to the New Web Publishing Rule** page, type a display name for the new publishing rule (for example, LyncDiscoveryURL).
4. On the **Select Rule Action** page, select **Allow**.
5. On the **Publishing Type** page, select **Publish a single Web site or load balancer**.
6. On the **Server Connection Security** page, select **Use SSL to connect to the published Web server or server farm**.
7. On the **Internal Publishing Details** page, in **Internal Site name**, type the fully qualified domain name (FQDN) of your Director pool (for example, lyncdir01.contoso.local). If you are creating a rule for the external Web Services URL on the Front End pool, type the FQDN of the Front End pool (for example, lyncpool01.contoso.local).

8. On the **Internal Publishing Details** page, in **Path (optional)**, type **/*** as the path of the folder to be published, and then select **Forward the original host header**.
9. On the **Public Name Details** page, do the following:
   - Under **Accept Requests for**, select **This domain name**.
   - In **Public Name**, type **lyncdiscover.**<*sipdomain*> (the external Autodiscover Service URL). If you are creating a rule for the external Web Services URL on the Front End pool, type the FQDN for the external Web Services on your Front End pool (for example, lyncwebextpool01.contoso.com).
   - In **Path**, type **/***.
10. On **Select Web Listener** page, in **Web Listener**, select your existing SSL Listener with the updated public certificate.
11. On the **Authentication Delegation** page, select **No delegation, but client may authenticate directly**.
12. On the **User Set** page, select **All Users**.
13. On the **Completing the New Web Publishing Rule Wizard** page, verify that the web publishing rule settings are correct, and then click **Finish**.
14. In the Forefront TMG list of web publishing rules, double-click the new rule you just added to open **Properties**.
15. On the **To** tab, do the following:
    - Select **Forward the original host header instead of the actual one**.
    - Select **Requests appear to come from the Forefront TMG computer**.
16. On the **Bridging** tab, configure the following:
    - Select **Web server**.
    - Select **Redirect requests to HTTP port**, and type **8080** for the port number.
    - Select **Redirect requests to SSL port**, and type **4443** for the port number.
17. Click **OK**.
18. Click **Apply** in the details pane to save the changes and update the configuration.
19. Click **Test Rule** to verify that your new rule is set up correctly.

To modify an existing web publishing rule to add the external Autodiscover SAN and URL

1. Click **Start**, point to **Programs**, point to **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.

   > **Important:**
   >
   > You will repeat the modification for each publishing rule and listener that you have. Typically, this will be one rule and listener for the Front End pools and one for the optional Directors or Director pools, if you have deployed them.

2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, click the applicable rule. On the **Tasks** tab, click **Edit Selected rule**.
3. On the **Public Name** tab, in **This rule applies to**, select **Requests for the following Web sites**.
4. Click **Add**, type the name of the new Autodiscover site (for example, “lyncdiscover.contoso.com”), and then click **OK**.
5. On the **Listener** tab, click **Select Certificate** and assign the new certificate with the added Autodiscover SAN entries. Close the Listener and Web Publishing properties.
6. Click **Apply** in the details pane to save the changes and update the configuration.
7. Click **Test Rule** to verify that your new rule is set up correctly.

To create a web publishing rule for port 80

1. Click **Start**, point to **Programs**, point to **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, point to **New**, and then click **Web Site Publishing Rule**.

3. On the **Welcome to the New Web Publishing Rule** page, type a display name for the new publishing rule (for example, Lync Autodiscover (HTTP)).
4. On the **Select Rule Action** page, select **Allow**.
5. On the **Publishing Type** page, select **Publish a single Web site or load balancer**.
6. On the **Server Connection Security** page, select **Use non-secured connections to connect to the published Web server or server farm**.
7. On the **Internal Publishing Details** page, in **Internal Site name**, type the internal Web Services FQDN for your Front End pool (for example, lyncpool01.contoso.local).
8. On the **Internal Publishing Details** page, in **Path (optional)**, type **/*** as the path of the folder to be published, and then select **Forward the original host header instead of the one specified in the Internal site name field**.
9. On the **Public Name Details** page, do the following:
   - Under **Accept Requests for**, select **This domain name**.
   - In **Public Name**, type **lyncdiscover.**<*sipdomain*> (the external Autodiscover Service URL).
   - In **Path**, type **/***.
10. On **Select Web Listener** page, in **Web Listener**, select a Web Listener or use the New Web Listener Definition Wizard to create a new one.
11. On the **Authentication Delegation** page, select **No delegation, and client cannot authenticate directly**.
12. On the **User Set** page, select **All Users**.
13. On the **Completing the New Web Publishing Rule Wizard** page, verify that the web publishing rule settings are correct, and then click **Finish**.
14. In the Forefront TMG list of web publishing rules, double-click the new rule you just added to open **Properties**.
15. On the **Bridging** tab, configure the following:
    - Select **Web server**.
    - Select **Redirect requests to HTTP port**, and type **8080** for the port number.
    - Verify that **Redirect requests to SSL port** is not selected.
16. Click **OK**.
17. Click **Apply** in the details pane to save the changes and update the configuration.
18. Click **Test Rule** to verify that your new rule is set up correctly.
19. Verify that the external Autodiscover Service URL is not defined on any other web publishing rule.

Concepts

Setting Up Reverse Proxy Servers
Technical Requirements for Mobility

1.4.2.12.4 Configuring Autodiscover for Mobility with Hybrid Deployments

Configuring Autodiscover for Mobility with Hybrid Deployments

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2013-01-24*

Hybrid Deployments are configurations that use both the Microsoft Lync Online cloud service and the on premises deployment. In this type of configuration, the Autodiscover service must be able to locate where the user is actually located. That is to say, Autodiscover aids in finding the user account and where the server that hosts the user’s account is, regardless if it is in the on premises deployment or in the Lync Online deployment.

For example, if a user’s account is hosted on a server in Lync Online, the attempt to locate the user will happen as follows, in a process known as *discoverability*:

- User initiates a connection attempt to the on premises deployment, **contoso.com**.
- The attempt is sent to lyncdiscover.contoso.com, the DNS name associated with the Autodiscover service.
- Autodiscover refers to the assumed registrar pool at the contoso.com on premises deployment and is given information on the user’s actual home server hosted in Lync Online. Autodiscover then sends the user a referral to the **lync.com** online Autodiscover service.
- The user initiates a connection attempt to the lync.com online Autodiscover service and is able to locate the user’s account and the user’s home server.

To enable mobile clients to discover the deployment where the user home server is located, you must configure the Autodiscover service with a new uniform resource locator (URL). Do the following to configure the Autodiscover service.

Configuring Autodiscover for Hybrid Deployments

1. You use Get-CsHostingProvider to retrieve the value of the attribute ProxyFQDN.
2. From the Lync Server Management Shell, type

   ```
   Set-CsHostingProvider -Identity [identity] -AutodiscoverUrl https://we
   ```

   Where [identity] is replaced with the domain name of the shared SIP address space.

Other Resources

Get-CsHostingProvider
Set-CsHostingProvider

1.4.2.12.5 Verifying Your Mobility Deployment

Verifying Your Mobility Deployment

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2013-02-12*

```
Some information in this topic pertains to Cumulative Updates for Lync Server 201
```

After you deploy the Lync Server Mobility Service and Lync Server Autodiscover Service, run a test transaction to verify that your deployment works correctly. You can run **Test-CsUcwaConference** to test the ability of two users who are using Lync 2013 Mobile clients to create, join and communicate in a conference. To use this test transaction, you need two actual users or test users, and their full credentials.

You use **Test-CsMcxP2PIM** to test sending an instant message between two users who are using Lync 2010 Mobile. Similar to **Test-CsUcwaConference**, you use two actual users or two predefined test users.

To test conferencing for Lync 2013 Mobile clients

1. Log on as a member of the CsAdministrator role on any computer where Lync Server Management Shell and Ocscore are installed.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

3. At the command line, type:

   ```
   Test-CsUcwaConference -TargetFqdn <FQDN of Front End pool> -Authentica
   ```

   You can set credentials in a script and pass them to the test cmdlet. For example:

   ```
   $passwd1 = ConvertTo-SecureString "Password01" -AsPlainText -Force
   $passwd2 = ConvertTo-SecureString "Password02" -AsPlainText -Force
   $testuser1 = New-Object Management.Automation.PSCredential("contoso\Us
   $testuser2 = New-Object Management.Automation.PSCredential("contoso\Us
   Test-CsUcwaConference -TargetFqdn pool01.contoso.com -Authentication N
   ```

To test person-to-person instant messaging (IM) for Lync 2010 Mobile

1. Log on as a member of the CsAdministrator role on any computer where Lync Server Management Shell and Ocscore are installed.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. At the command line, type:

   ```
   Test-CsMcxP2PIM -TargetFqdn <FQDN of Front End pool> -Authentication <
   ```

   You can set credentials in a script and pass them to the test cmdlet. For example:

   ```
   $passwd1 = ConvertTo-SecureString "Password01" -AsPlainText -Force
   $passwd2 = ConvertTo-SecureString "Password02" -AsPlainText -Force
   $tuc1 = New-Object Management.Automation.PSCredential("contoso\UserNam
   $tuc2 = New-Object Management.Automation.PSCredential("contoso\UserNam
   Test-CsMcxP2PIM -TargetFqdn pool01.contoso.com -Authentication Negotia
   ```

Other Resources

Test-CsMcxP2PIM
Test-CsUcwaConference

1.4.2.12.6 Configuring for Push Notifications

Configuring for Push Notifications

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2013-02-12*

Push notifications, in the form of badges, icons, or alerts, can be sent to a mobile device even when the mobile application is inactive. Push notifications notify a user of events such as a new or missed IM invitation and voice mail. The Lync Server 2013 Mobility Service sends the notifications to the cloud-based Lync Server Push Notification Service, which then sends the notifications to the Apple Push Notification Service (APNS) (for an Apple device running the Lync 2010 Mobile client) or the Microsoft Push Notification Service (MPNS) (for a Windows Phone device running the Lync 2010 Mobile or the Lync 2013 Mobile client).

Important:

If you use Windows Phone with Lync 2010 Mobile or Lync 2013 Mobile client, push notification is an important consideration.
If you use Lync 2010 Mobile on Apple devices, push notification is an important consideration.
If you use Lync 2013 Mobile on Apple devices, you no longer need push notification.

Configure your topology to support push notifications by doing the following:

- If your environment has a Lync Server 2010 or Lync Server 2013 Edge Server,

you need to add a new hosting provider, Microsoft Lync Online, and then set up hosting provider federation between your organization and Lync Online.
- If your environment has a Office Communications Server 2007 R2 Edge Server, you need to set up direct SIP federation with push.lync.com.

> **Note:**
>
> Push.lync.com is a Microsoft Office 365 domain for Push Notification Service.

- To enable push notifications, you need to run the **Set-CsPushNotificationConfiguration** cmdlet. By default, push notifications are turned off.
- Test the federation configuration and push notifications.

To configure for push notifications with Lync Server 2013 or Lync Server 2010 Edge Server

1. Log on to a computer where Lync Server Management Shell and Ocscore are installed as a member of the RtcUniversalServerAdmins group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Add a Lync Server online hosting provider. At the command line, type:

   ```
   New-CsHostingProvider -Identity <unique identifier for Lync Online hos
   ```

   For example:

   ```
   New-CsHostingProvider -Identity "LyncOnline" -Enabled $True -ProxyFqdn
   ```

   > **Note:**
   >
   > You cannot have more than one federation relationship with a single hosting provider. That is, if you have already set up a hosting provider that has a federation relationship with sipfed.online.lync.com, do not add another hosting provider for it, even if the identity of the hosting provider is something other than LyncOnline.

4. Set up hosting provider federation between your organization and the Push Notification Service at Lync Online. At the command line, type:

   ```
   New-CsAllowedDomain -Identity "push.lync.com"
   ```

To configure for push notifications with Office Communications Server 2007 R2 Edge Server

1. Log on to the Edge Server as a member of the RtcUniversalServerAdmins group.
2. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Computer Management**.
3. In the console tree, expand **Services and Applications**, right-click **Microsoft Office Communications Server 2007 R2**, and then click **Properties**.
4. On the **Allow** tab, click **Add**.
5. In the **Add Federated Partner** dialog box, do the following:
   - In **Federated partner domain name**, type **push.lync.com**.
   - In **Federated partner Access Edge Server**, type **sipfed.online.lync.com**.
   - Click **OK**.

To enable push notifications

1. Log on to a computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Enable push notifications. At the command line, type:

```
Set-CsPushNotificationConfiguration -EnableApplePushNotificationServic
```

4. Enable federation. At the command line, type:

```
Set-CsAccessEdgeConfiguration -AllowFederatedUsers $True
```

⊟To test federation and push notifications

1. Log on to a computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Test the federation configuration. At the command line, type:

```
Test-CsFederatedPartner -TargetFqdn <FQDN of Access Edge server used f
```

For example:

```
Test-CsFederatedPartner -TargetFqdn accessproxy.contoso.com -Domain pu
```

4. Test push notifications. At the command line, type:

```
Test-CsMcxPushNotification -AccessEdgeFqdn <Access Edge service FQDN>
```

For example:

```
Test-CsMcxPushNotification -AccessEdgeFqdn accessproxy.contoso.com
```

Other Resources

Test-CsFederatedPartner
Test-CsMcxPushNotification

1.4.2.12.7 Configuring Mobility Policy

Configuring Mobility Policy

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2013-02-13*

```
Some information in this topic pertains to Cumulative Updates for Lync Server 201
```

Lync Server 2013 provides mobility policies that determine who can use mobility features, Call via Work, voice over IP (VoIP) or video, and whether WiFi will be required for either VoIP or video. The Call via Work feature enables a mobile user to make and receive calls on a mobile phone by using a work phone number instead of the mobile phone number. This feature prevents the called party from seeing the caller's mobile phone number and enables a user to avoid outbound calling charges. Configuring VoIP and video makes it possible for users to receive and make VoIP calls and video. Settings for WiFi usage define if a user’s device will be required to use a WiFi network over a cellular data network.

By default, mobility, Call via Work, and the VoIP and video features are enabled. The settings to require WiFi for VoIp and video are disabled. Administrators can determine who has access to these features by running a cmdlet. You can turn options off globally, by site, or by user.

To be able to use mobility features and Call via Work, users must meet the following prerequisites:

- Users must be enabled for Lync Server 2013.
- Users must be enabled for Enterprise Voice.
- Users must be assigned a mobility policy that has the **EnableMobility** option set to True.

For users to be able to use Call via Work, they must meet the following two additional prerequisites:

- Users must be assigned a voice policy that has the **Enable simultaneous ringing of phones** option selected.
- Users must be assigned a mobility policy that has the **EnableOutsideVoice** option set to True.

Note:

Users who are not enabled for Enterprise Voice can use their mobile devices to make Lync to Lync Voice over IP (VoIP) calls, or can join conferences by using the Click to Join link on their mobile devices, if you assign those users the appropriate options for voice policy. For details, see Defining Your Mobility Requirements.

For details about enabling users for Lync Server 2013, see Disable or Re-Enable User Account for Lync Server. For details about enabling users for Enterprise Voice, see Enable Users for Enterprise Voice. For details about setting voice policy options, see Modify a Voice Policy and Configure PSTN Usage Records.

To modify global mobility policy

1. Log on to any computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Turn off access to mobility and Call via Work globally. At the command line, type:

```
Set-CsMobilityPolicy -EnableMobility $False -EnableOutsideVoice $False
```

Note:

You can turn off Call via Work without turning off access to mobility. However, you cannot turn off mobility without also turning off Call via Work.

To modify mobility policy by site

1. Log on to any computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Create a site-level policy, and turn off VoIP and video, and enable Require WiFi for IP Audio and for IP Video by site. At the command line, type:

```
New-CsMobilityPolicy -Identity site:<site identifier> -EnableIPAudioVi
```

To modify mobility policy by user

1. Log on to any computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Create user level mobility policies and turn off mobility and Call via Work by user. At the command line, type:

```
New-CsMobilityPolicy -Identity <policy name> -EnableMobility $False -E
Grant-CsMobilityPolicy -Identity <user identifier> -PolicyName <policy
```

You can turn off Call via Work without turning off access to mobility. However, you cannot turn off mobility without also turning off Call via Work.

For example:

```
New-CsMobilityPolicy "tag:disableOutsideVoice" -EnableOutsideVoice $Fa
Grant-CsMobilityPolicy -Identity -MobileUser1@contoso.com -PolicyName
```

Tasks

Disable or Re-Enable User Account for Lync Server
Enable Users for Enterprise Voice
Modify a Voice Policy and Configure PSTN Usage Records

Concepts

Defining Your Mobility Requirements

Other Resources

New-CsMobilityPolicy
Set-CsMobilityPolicy
Get-CsMobilityPolicy
Grant-CsMobilityPolicy
Remove-CsMobilityPolicy

1.4.2.13 Verifying Your Edge Deployment

Verifying Your Edge Deployment

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2010-11-07*

After completing the installation and configuration of your edge components, you need to verify the configuration and connectivity of servers and to verify connectivity for each type of external user that you support.

- Verify Connectivity Between Internal Servers and Edge Servers
- Verify Connectivity for External Users

1.4.2.13.1 Verify Connectivity Between Internal Servers and Edge Servers

Verify Connectivity Between Internal Servers and Edge Servers

Deployment > Deploying External User Access > Verifying Your Edge Deployment >

Topic Last Modified: *2012-09-08*

In Lync Server 2013, a separate validation wizard was available to help validate connectivity between Edge Servers and internal servers. In Lync Server 2013 validation of connectivity is done automatically when you install your Edge Servers.

You can validate the replication of configuration information to the edge by running the Windows PowerShell **Get-CsManagementStoreReplicationStatus** cmdlet on the internal computer on which the Central Management store is located (or any domain joined computer on which Lync Server 2013 Core Components (OcsCore.msi) is installed. Initial results may indicate the status as "False" instead of "True" for replication. If so, run the **Invoke-CsManagementStoreReplication** cmdlet and allow time for the replication to complete before running the **Get-CsManagementStoreReplicationStatus** again.

You can verify external user connectivity separately, including using the Office Communications Server Remote Connectivity Analyzer to verify remote user connectivity. For details, see Verify Connectivity for External Users.

1.4.2.13.2 Verify Connectivity for External Users

Verify Connectivity for External Users

Deployment > Deploying External User Access > Verifying Your Edge Deployment >

Topic Last Modified: *2012-10-19*

Validating connectivity for external users requires ensuring connectivity from users to the server and port for the Access Edge service.

A valuable resource for confirming your configuration and the ability to connect, send and receive the correct messages for the scenarios that external user access requires is the Remote Connectivity Analyzer site (http://www.testocsconnectivity.com). The site is managed and maintained by Microsoft Support. To reach the Remote Connectivity Analyzer, open the Web site in a browser and follow the instructions to select the scenario.

Test Connectivity of External Users and External access

Tests for external user access should include each type of external user that your organization supports, including any or all of the following:

- Users from at least one federated domain, and test IM, presence, A/V and desktop sharing.
- Users of each public IM service provider that your organization supports (and for which provisioning has been completed).
- Anonymous users.
- Users within your organization who are logged into Lync remotely, but not using VPN.

These tests determine whether your Edge Server is:

- Listening on the necessary ports by using a telnet client from outside your network.
  - Example: telnet sip.contoso.com 443
  - Perform the preceding test on ports you are using on the Edge Server or Edge Server pool depending on your deployment.
- Performing accurate external DNS resolution.
  - From outside your network ping each of the external FQDN's of your Edge or Edge pool. Even if the ping fails you will see the IP addresses, which you can compare to the ones you have assigned.

1.4.3 Deploying Enterprise Voice

Deploying Enterprise Voice

See Also

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-10-03*

Lync Server 2013, Enterprise Voice is part of the Lync Server 2013 infrastructure.

Deploying Enterprise Voice requires that you:

1. Review the Planning for Enterprise Voice section of the Planning documentation.

2. Finalize plans for features and components to deploy with this workload.
3. Run Planning Tool to design a topology that reflects your deployment decisions.
4. Open the topology design in Topology Builder, as described in Defining and Configuring the Topology in the Deployment documentation.

Note:
Installation of Topology Builder is part of the deployment process for the internal pool. For details, see Install Lync Server Administrative Tools in the Deployment documentation.

Additionally, you must have already deployed Lync Server, Enterprise Edition at central sites and branch sites that correspond to the reference topology that you choose to deploy. You can't deploy Enterprise Voice components until you have defined, published, and installed files for at least one internal pool, and you must use Topology Builder to define and publish an internal pool.

To view reference topologies with examples of where Enterprise Voice server roles can be deployed (and their relationship to one another and other Lync Server 2013 server roles), see Reference Topologies in the Planning documentation.

To view a reference topology that illustrates and explains a sample call admission control deployment, including network regions, network sites, and subnets, see Example: Gathering Your Organization's Requirements for Call Admission Control in the Planning documentation.

Important:
To deploy Enterprise Voice at a central site, continue reading the topics in this section. To deploy Enterprise Voice at a branch site, skip to Deploying Branch Sites in the Deployment documentation.

This section includes procedures for deployments in which a Mediation Server is collocated on each Front End Server or Standard Edition server, as recommended, and also for deployments with a stand-alone Mediation Server pool.

You can skip the following content if you used Topology Builder to define and publish a topology that collocates a Mediation Server on each Front End Server or Standard Edition server, because Deployment Wizard already automatically installed the files for Mediation Server when you installed files for your Front End Server pool or Standard Edition server:

- Configuring Trunks

If you used Topology Builder to define and publish a Mediation Server in a stand-alone pool, you can use the following content:

- Verify that your topology meets the software and environment prerequisites, as described in Enterprise Voice Prerequisites.

In This Section

- Enterprise Voice Prerequisites
- Deploying Mediation Servers and Defining Peers
- Configuring Trunks
- Configuring Dial Plans
- Configuring Voice Policies, PSTN Usage Records, and Voice Routes
- Exporting and Importing Voice Routing Configuration
- Test Voice Routing
- Publish Pending Changes to the Voice Routing Configuration
- Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail
- Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM
- Configuring On-premises Lync Server 2013 Integration with Exchange Online

- Deploying Advanced Enterprise Voice Features
  - About Network Regions, Sites, and Subnets
  - Create or Modify a Network Region
  - Create or Modify a Network Site
  - Associate a Subnet with a Network Site
  - Configure Call Admission Control
  - Configure Enhanced 9-1-1
  - Configure Media Bypass
- Enable Users for Enterprise Voice

⊟See Also

Other Resources

Deploying Branch Sites
Configuring Dial-in Conferencing
Configuring Call Park
Configuring Announcements for Unassigned Numbers
Deploying Monitoring

1.4.3.1 Enterprise Voice Prerequisites

Enterprise Voice Prerequisites

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-08-06*

For the best experience when deploying Enterprise Voice, be sure that your IT infrastructure, network, and systems meet the prerequisites described in the topics in this section.

- Software Prerequisites for Enterprise Voice
- Security and Configuration Prerequisites for Enterprise Voice

1.4.3.1.1 Software Prerequisites for Enterprise Voice

Software Prerequisites for Enterprise Voice

Deployment > Deploying Enterprise Voice > Enterprise Voice Prerequisites >

Topic Last Modified: *2012-10-03*

Verify that the infrastructure in which you intend to deploy Enterprise Voice meets the following software prerequisites:

- Lync Server 2013 Standard Edition or Enterprise Edition is installed and operational on your network.
- All Edge Servers are deployed and operational in your perimeter network, including Edge Servers running Access Edge service, A/V Edge service, Web Conferencing Edge service, and a reverse proxy.
- Either Microsoft Exchange Server 2007 Service Pack 3 (SP3), Microsoft Exchange Server 2010 or Microsoft Exchange Server 2013 is required for integrating Exchange Unified Messaging with Lync Server and to provide rich notifications and call log information to the Lync endpoints.
- One or more users have been created and enabled for Lync Server.
- Lync clients and devices have been successfully deployed.
- Topology Builder is installed on a server on your network.

Next Steps: Verify Security and

Configuration Prerequisites

After verifying software prerequisites for Enterprise Voice, you can use the documentation to continue preparing for deploying Enterprise Voice:

1. Verify security, user configuration, and hardware perquisites, as described in Security and Configuration Prerequisites for Enterprise Voice.
2. Install the Mediation Server, as described in Install the Files for Mediation Server, but *only* if you want to deploy a stand-alone Mediation Server or pool because Mediation Servers are installed as part of the Front End pool or Standard Edition server deployment process when collocated.
3. Configure trunk connections to provide PSTN connectivity for users, as described in Configuring Trunks.

1.4.3.1.2 Security and Configuration Prerequisites for Enterprise Voice

Security and Configuration Prerequisites for Enterprise Voice

Deployment > Deploying Enterprise Voice > Enterprise Voice Prerequisites >

Topic Last Modified: *2012-10-18*

Verify that your infrastructure meets the following security, user configuration, and scenario-specific hardware prerequisites.

Administrative Rights and Certificate Infrastructure

Be sure that your environment is configured with the following administrative user groups and certificate infrastructure for use during the Enterprise Voice deployment process.

- Administrators deploying Enterprise Voice should be members of the RTCUniversalServerAdmins group.
- Administrators performing the configuration tasks must have adequate rights:
  - **CsVoiceAdministrator:** This administrator role can perform voice configuration tasks, manage voice applications, and assign voice policies to end users.
  - **CsUserAdministrator:** This administrator role can manage user properties, such as enabling Enterprise Voice for a user. This administrator role can also assign per-user policies, with the exception of the archiving policy; move users; and manage common area phones and analog devices.
  - **CsAdministrator:** This administrator role can perform all of the tasks of CsVoiceAdministrator and CsUserAdministrator.

  Note:

  Delegation enables more administrators to participate in your Lync Server deployment without opening up unnecessary access to resources.
- Managed key infrastructure (MKI) is deployed and configured, by using either a Microsoft or a third-party certification authority (CA) infrastructure.

  Note:

  For details about certificate requirements in Lync Server, see Certificate Infrastructure Requirements in the Planning documentation.

User Configuration

If you collocated the Mediation Server with each Front End pool or Standard Edition server during Front End deployment, user settings necessary for Enterprise Voice were configured automatically during installation of the files for those server roles.

If you are newly deploying the Enterprise Voice workload at this time, before you begin the deployment process, designate a primary phone number for each user who you plan to enable for Enterprise Voice. As the administrator, you are responsible for ensuring that this number is unique. Before implementation, all primary phone numbers must be normalized (correctly formatted) and copied to each user's **Line URI** property using Lync Server Control Panel.

Note:

For examples of primary phone numbers required for Enterprise Voice deployment, see the Dial Plans and Normalization Rules section of Dial Plans and Normalization Rules in the Planning documentation.

Next Steps: Install Files or Configure PSTN Connectivity

After verifying software and environmental prerequisites for Enterprise Voice, you can use the following content to either:

- Install the Mediation Server, as described in Install the Files for Mediation Server, but only if you want to deploy a stand-alone Mediation Server or pool because Mediation Servers are installed as part of the Front End pool or Standard Edition server deployment process when collocated.
- Or, begin configuring settings to route calls for Enterprise Voice users, as described in Configuring Trunks.

1.4.3.2 Deploying Mediation Servers and Defining Peers

Deploying Mediation Servers and Defining Peers

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-09-21*

The Enterprise Voice workload, dial-in conferencing, and advanced Enterprise Voice applications (Response Group application, Call Park application, call admission control (CAC), and so on), are available in Front End pools. With Lync Server 2013, the functionality of the Mediation Server is built into the Front End Server. A separate stand-alone Mediation Server is no longer necessary. Front End pools can communicate directly with supported gateways (a public switched telephone network (PSTN) gateway or an IP-PBX), removing the need for a Mediation Server to serve as an intermediary.

The only exception is if you configure a SIP trunk to connect to a Session Border Controller for an Internet Telephony Service Provider. To connect your Enterprise Voice infrastructure to your SIP trunk provider, a separate Mediation Server must be deployed.

The connection between Lync Server (the Mediation Server component on a Front End pool or stand-alone Mediation Server) and a gateway is defined as a logical association called a *trunk*. The topics in this section describe how to define a trunk and how to deploy a stand-alone Mediation Server, if you connect to a SIP trunk.

- Define a Mediation Server in Topology Builder
- Define a Gateway in Topology Builder
- Install the Files for Mediation Server
- Define additional Trunks in Topology Builder

⊟Related Sections

Configuring Dial-in Conferencing

1.4.3.2.1 Define a Mediation Server in Topology Builder

Define a Mediation Server in Topology Builder

Deployment > Deploying Enterprise Voice > Deploying Mediation Servers and Defining Peers >

Topic Last Modified: *2013-02-24*

Follow the steps in this topic to use Topology Builder to define a stand-alone Mediation Server or pool collocated with a Front End pool at a site for which you did not previously deploy Enterprise Voice.

You can define a topology using an account that is a member of the Administrators group.

Define Mediation Server collocated to a Front End pool

Follow the steps in this topic to use Topology Builder to define a Mediation Server collocated to a Front End pool in a site where Enterprise Voice has not been previously deployed.

⊟To Add a Mediation Server to a Front End pool

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In Topology Builder, in the console tree, expand the name of the site for which you want to define a Front End pool.
3. In the console tree, right-click the type of Front End pool you want, and then click **New Front End pool...**.
4. Navigate through the **Define New Front End Pool** wizard until you reach the **Select collocated server roles** page.
5. In **Select collocated server roles**, check the option **Collocate Mediation Server**.

Note:

- If the type of Front End pool you selected is the Enterprise Edition, then the Mediation Server component will be installed on all the Front End Servers of that Front End pool.
- The **Next hop pool** used by the Mediation Server will be the Front End pool where the Mediation Server is collocated on.
- The **Edge pool** used by the Mediation Server will be the same Edge pool associated with the Front End pool where the Mediation Server is collocated on.

1. Click **Make Default** to use this Front End pool to route calls from Microsoft Office Communications Server 2007 R2 to the PSTN.
2. Click **Finish** when you are finished associating one or more peers to the Front End pool.

Note:

Before you proceed to the next step in the Enterprise Voice deployment process, make sure that the Mediation Server pool (i.e. Front End pool with the Mediation Server component collocated) is using the FQDNs that you specified.

3. Next, follow the procedures in Publish the Topology in the Deployment Guide documentation to add the Mediation Server to your topology before proceeding to the next step of modifying the listening ports of the Mediation Server if needed. You must publish your topology each time you use Topology Builder to define or modify your topology.

Define stand-alone Mediation Server

Follow the steps in this topic to use Topology Builder to define a stand-alone Mediation Server or pool at a site where Enterprise Voice has not been previously deployed.

If you already deployed Mediation Servers collocated to Front End pools at this site, you can skip this section and Install the Files for Mediation Server before proceeding to Configuring Trunks.

Note:

This section assumes that you have already setup at least one Front End pool, as described in Define and Configure a Front End Pool or Standard Edition Server and Publish the Topology in the Deployment Guide documentation.

To Add a Mediation Server

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In Topology Builder, in the console tree, expand the name of the site for which you want to define a Mediation Server.
3. In the console tree, right-click the **Mediation pools** node, and then click **Mediation Server pool**.
4. In **Define New Mediation Pool**, type the Mediation Server pool fully qualified domain name (FQDN).
5. Next, do one of the following:
   - If you want to deploy multiple Mediation Servers in the pool to provide high availability, then select **Multiple computer pool**.

     Note:

     You must deploy DNS load balancing to support Mediation Server pools that have multiple Mediation Servers. For details, see the Using DNS Load Balancing on Mediation Server Pools section of DNS Load Balancing in the Planning documentation.

   - If you want to deploy only one Mediation Server in the pool because you do not require high availability, then select **Single computer pool**. Skip the following step.
6. If you selected **Multiple computer pool** in the previous step, on the **Define the computers in this pool** item, click **Computer FQDN**, type the FQDN of each server in the pool, and then click **Add**. Repeat this step for all other Mediation Servers that you want to add to the pool. When you have defined all the computers in the pool, click **Next**.
7. On the **Select the next hop** page, click **Next hop pool**, click the FQDN of the Front End pool that will use this Mediation Server pool, and then click **Next**.
8. On the **Select an Edge Server** page, do one of the following:
   - If you want to provide PSTN connectivity to external users enabled for Enterprise Voice, under **Select Edge Pool used by this Mediation Server**, click the FQDN of the Edge Server pool that will use this Mediation Server pool to provide PSTN connectivity to those external users, and then click **Next**.
   - If you do not plan to enable external users for Enterprise Voice, or if you do not want to provide PSTN connectivity to users when they are outside the internal network, click **Next**.
9. Next, follow the procedures in Publish the Topology in the Deployment documentation to add the Mediation Server to the topology. You must publish

your topology each time you use Topology Builder to build or modify your topology so that the data can be used to install the files for servers that are running Lync Server. Then continue to the next steps to modify the listening ports on the Mediation Server, if necessary.

Define the Mediation Server Listening Ports

Follow the steps in this topic to use Topology Builder to define the listening ports a Mediation Server or pool will accept incoming connections from a gateway peer.

⊟To Modify the Mediation Server Listening Ports

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In Topology Builder, in the console tree, expand the **Mediation pools** node, and right-click the Mediation Server previously created.
3. By default, the SIP listening ports on the Mediation Server are 5070 for TLS traffic from Lync Server, 5067 for TLS traffic from peers (gateways, PBXes, or SBCs). TCP port is disabled by default. You must enable TCP port if you have gateways that do not support TLS.
4. Specify the desired TLS or TCP listening port range the Mediation Server will accept incoming connections from PSTN gateways.

Note:

Entering a TCP port range is not required if **Enable TCP port** is not checked. This setting is optional.

Next, Define a Gateway in Topology Builder and install the files on each Mediation Server in the pool by following the procedures in Install the Files for Mediation Server.

1.4.3.2.2 Define a Gateway in Topology Builder

Define a Gateway in Topology Builder

See Also

Deployment > Deploying Enterprise Voice > Deploying Mediation Servers and Defining Peers >

Topic Last Modified: *2012-10-04*

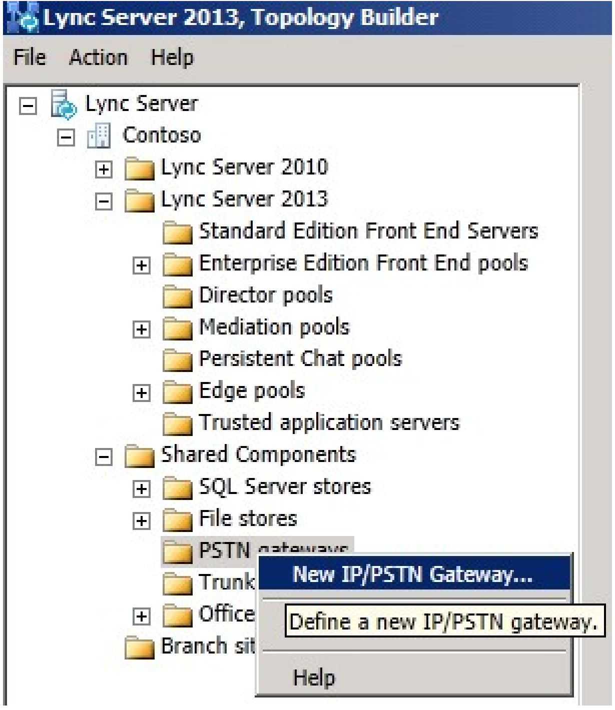
Follow these steps to use Topology Builder to define a *peer* with which you can associate a Mediation Server to provide connectivity to the public switched telephone network (PSTN) for users enabled for Enterprise Voice. A peer to the Mediation Server can be a PSTN gateway, an IP-PBX, or a Session Border Controller (SBC) for an Internet Telephony Service Provider (ITSP) to which you connect by configuring a SIP trunk.

Note:

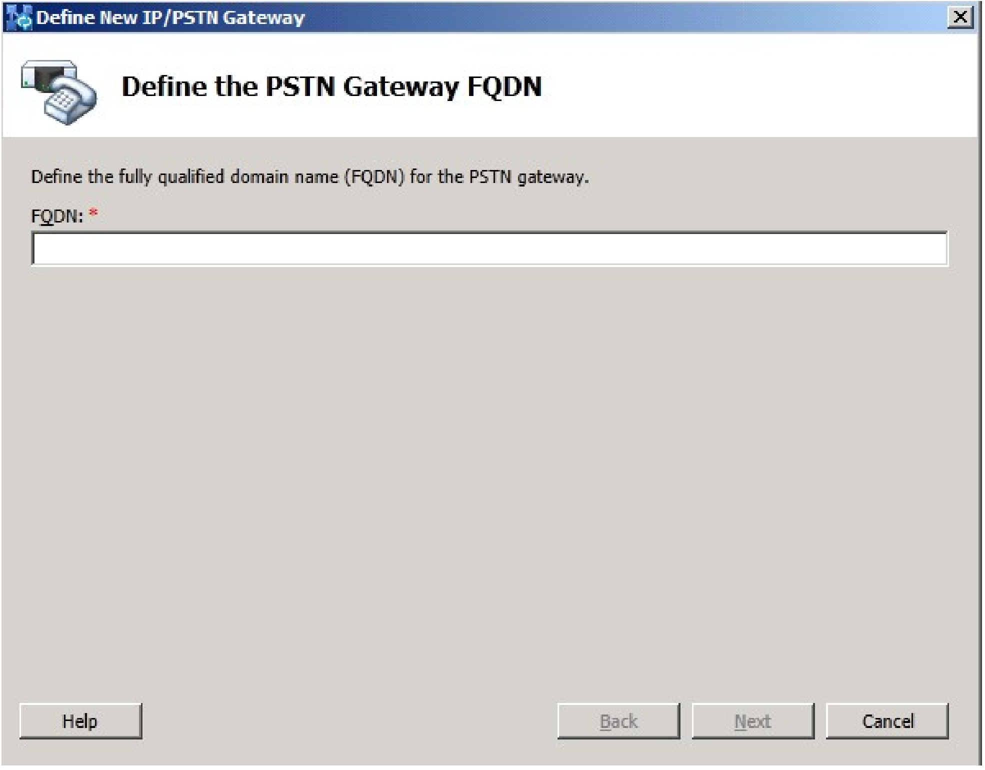
This topic assumes that you have set up at least one internal Front End pool or Standard Edition server in at least one central site with a collocated or stand-alone Mediation Server, as described in Define and Configure a Front End Pool or Standard Edition Server and Publish the Topology in the Deployment documentation. This topic also assumes that you have verified that your infrastructure meets the prerequisites described in Software Prerequisites for Enterprise Voice and Security and Configuration Prerequisites for Enterprise Voice.

⊟To Define a Peer for the Mediation Server

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. Under Lync Server 2013, your site name, Shared Components, right-click the **PSTN Gateways** node, and then click **New PSTN Gateway**.



3. In **Define New IP/PSTN Gateway**, type the fully qualified domain name (FQDN) or IP address of the peer, and click **Next**.



Define the PSTN Gateway FQDN

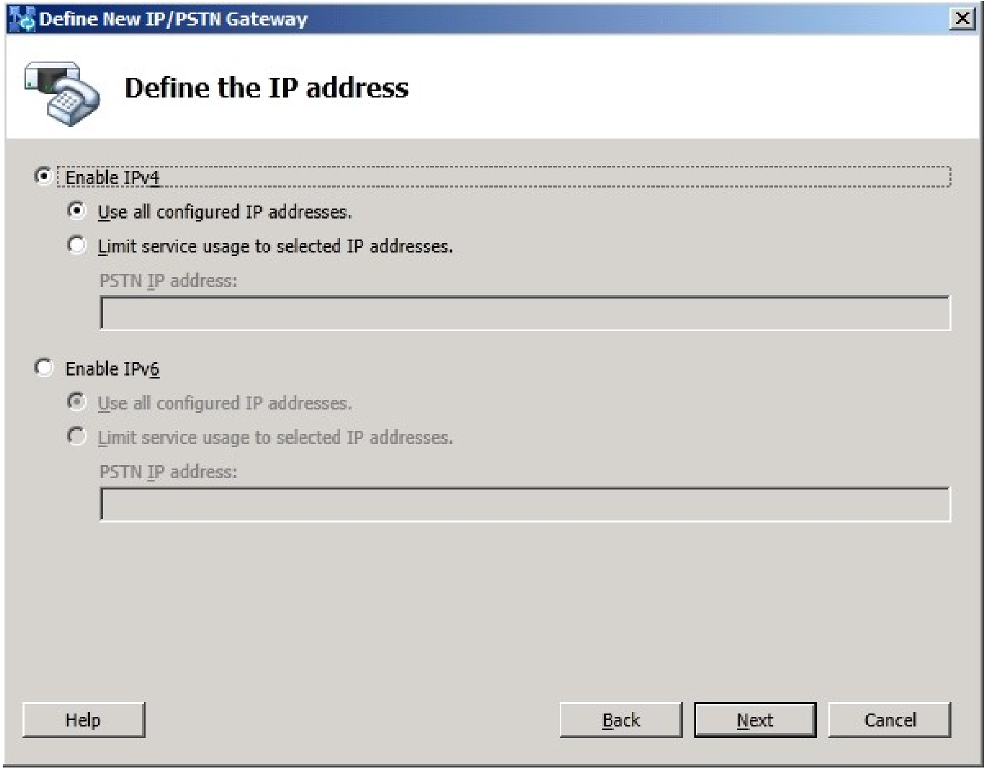
Define the fully qualified domain name (FQDN) for the PSTN gateway.

FQDN: *

Note:

If you specify Transport Layer Security (TLS) as the transport type, you must specify the FQDN instead of the IP address of the peer of the Mediation Server.

4. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and click **Next**.



Define New IP/PSTN Gateway

Define the IP address

● Enable IPv4

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

PSTN IP address:

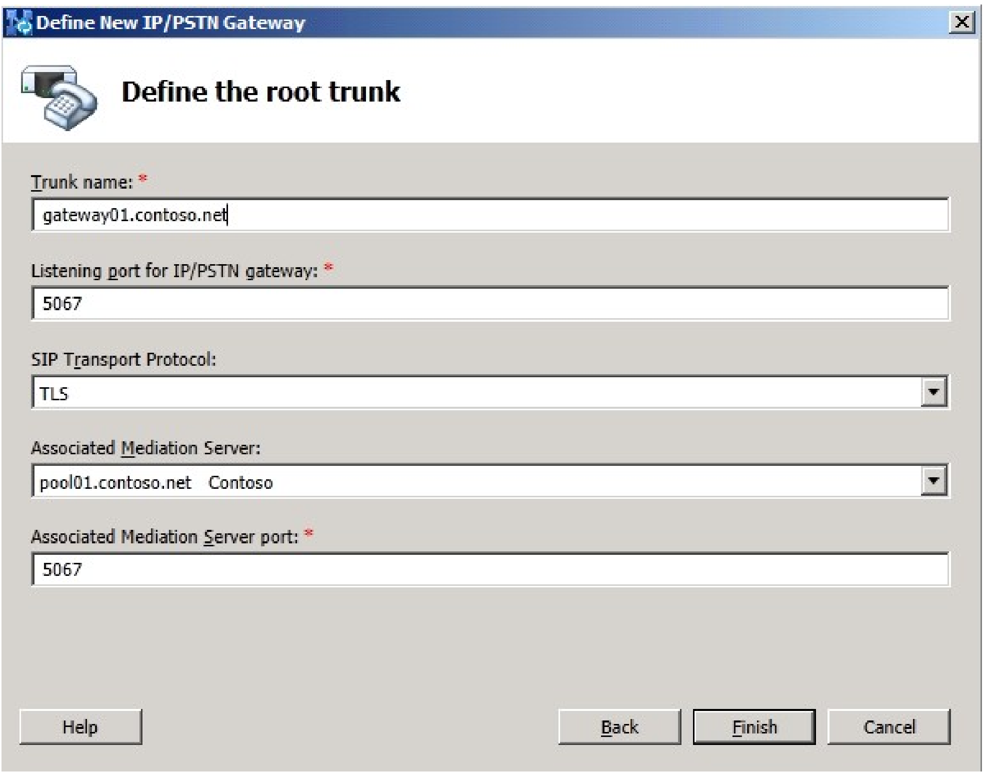
○ Enable IPv6

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

PSTN IP address:

5. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between a Mediation Server and a gateway uniquely identified by the tuple. {Mediation Server FQDN, Mediation Server listening port (TLS or TCP) : gateway IP and FQDN, gateway listening port}
   - When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
   - The root trunk cannot be removed until the associated PSTN gateway is removed.



Trunk name: *
gateway01.contoso.net

Listening port for IP/PSTN gateway: *
5067

SIP Transport Protocol:
TLS

Associated Mediation Server:
pool01.contoso.net Contoso

Associated Mediation Server port: *
5067

6. Under **Listening Port for IP/PSTN Gateway**, type the listening port that the gateway, PBX, or SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway. (By default, the ports are 5066 for Transmission Control Protocol (TCP) and 5067 for Transport Layer Security (TLS) on a PSTN gateway, PBX or SBC. On a Survivable Branch Appliance at a branch site, the default ports are 5081 for TCP and 5082 for TLS.)
7. Under **SIP Transport Protocol**, click the transport type that the peer uses, and then click **OK**.

Note:
For security reasons, we strongly recommend that you deploy a peer to the Mediation Server that can use TLS.

8. Under **Associated Mediation Server**, select the Mediation Server pool to associate with the root trunk of this this PSTN Gateway.
9. Under **Associated Mediation Server port**, type the listening port that the Mediation Server will use for SIP messages from the gateway.

Note:
With multiple trunk support in Lync Server 2013, multiple SIP signaling ports can be defined on the Mediation Server to be used for communication with multiple PSTN gateways. When defining a trunk, the **Associated Mediation Server port** must be within the range of the listening ports for the respective protocol allowed by the Mediation Server. This port range is defined under Lync Server 2013 and Mediation Pools. Right-click the Mediation Server pool of interest, and select **Edit Properties**. Specify the port range in the **Listening ports** field.

10. Click **Finish**.

Important:
Before you finish this step, be sure that the peer that you defined is running and using the FQDN or IP address that you specified.

Next, to add the peer to the topology, follow the procedures in Publish the Topology in the Deployment documentation. You must publish your topology each time that you use Topology Builder to build or modify your topology, so that the data can be used to install the files for servers that are running Lync Server.

Tasks

Modify a Trunk in Topology Builder

1.4.3.2.2.1 Modify a Trunk in Topology Builder

Modify a Trunk in Topology Builder

Deploying Enterprise Voice > Deploying Mediation Servers and Defining Peers > Define a Gateway in Topology Builder >

Topic Last Modified: *2012-09-21*

Follow these steps to modify the alternate media IP address and alternate bypass identifier of a trunk.

To Modify the Alternate Media IP Address of a Trunk

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsPstnGateway cmdlet and modify the AlternateBypassId field in the Lync Server Management Shell.

```
Set-CsPstnGateway -Identity "PstnGateway:<peer FQDN> -RepresentativeMe
```

To Modify the Alternate BypassID of a Trunk

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsPstnGateway cmdlet and modify the AlternateBypassId field in the Lync Server Management Shell.

```
Set-CsPstnGateway -Identity "PstnGateway:<peer FQDN> -AlternateBypassI
```

1.4.3.2.3 Define additional Trunks in Topology Builder

Define additional Trunks in Topology Builder

See Also

Deployment > Deploying Enterprise Voice > Deploying Mediation Servers and Defining Peers >

Topic Last Modified: *2012-10-04*

Follow these steps to use Topology Builder to define an additional trunk to which you can associate a *peer* with a Mediation Server. A peer provides users enabled for Enterprise Voice with connectivity to the public switched telephone network (PSTN). A peer can be a PSTN gateway, an IP-PBX, or a Session Border Controller (SBC) for an Internet Telephony Service Provider (ITSP). The trunk defines this connection between the Mediation Server and peer. Multiple trunks can be defined per Mediation Server. A Mediation Server can be associated with multiple peers.

A trunk is a logical connection between a Mediation Server and a gateway uniquely identified by the tuple:

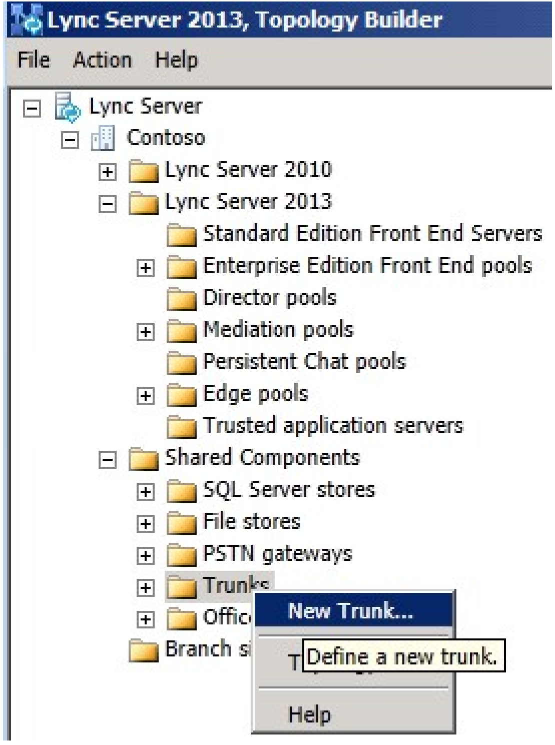
{Mediation Server FQDN, Mediation Server listening port (TLS or TCP) : gateway IP and FQDN, gateway listening port}

Note:
This topic assumes that you have setup a PSTN gateway and root trunk with at least one collocated or stand-alone Mediation Server or pool as described in Define a Gateway in Topology Builder in the Deployment documentation.

Note:
This topic assumes that you have set up at least one Front End pool or Standard Edition server in at least one central site, as described in Define and Configure a Front End Pool or Standard Edition Server and Publish the Topology in the Deployment documentation.

⊟To Define an additional Trunk between a Mediation Server and a Gateway Peer

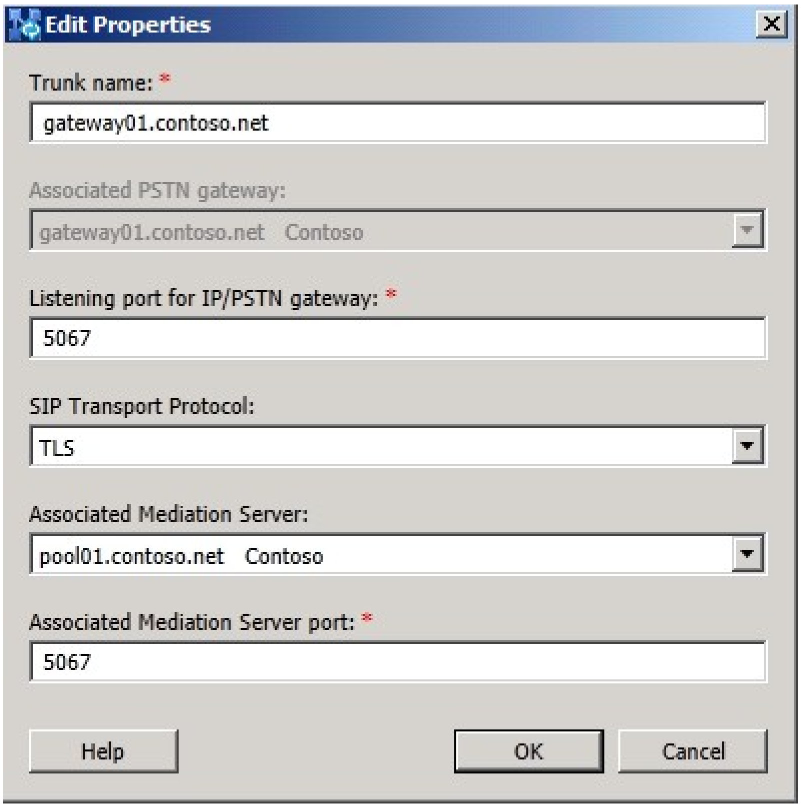
1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. Under Lync Server 2013, your site name, **Shared Components**, right-click the **Trunks** node, and then click **New Trunk**.



3. In **Define New Trunk**, specify a friendly name to uniquely identify the trunk. You cannot have two trunks with the same name.

Note:
If you specify Transport Layer Security (TLS) as the transport type, you must specify the FQDN instead of the IP address of the peer of the Mediation Server.

4. Under **Associated PSTN gateway**, select the PSTN gateway peer to associate with this trunk.



Trunk name: *
gateway01.contoso.net

Associated PSTN gateway:
gateway01.contoso.net Contoso

Listening port for IP/PSTN gateway: *
5067

SIP Transport Protocol:
TLS

Associated Mediation Server:
pool01.contoso.net Contoso

Associated Mediation Server port: *
5067

5. Under **Listening Port for PSTN gateway**, type the listening port that the peer (PSTN gateway, IP-PBX, or SBC) will receive SIP messages from the Mediation Server that is to be associated with this trunk. The default peer ports are 5066 for Transmission Control Protocol (TCP) and 5067 for Transport Layer Security (TLS). The default Survivable Branch Appliance ports are 5081 for TCP and 5082 for TLS.
6. Under **SIP Transport Protocol**, click the transport type that the peer uses.

Note:
For security reasons, we strongly recommend that you deploy a peer to the Mediation Server that can use TLS.

7. Under **Associated Mediation Server**, select the Mediation Server pool to associate with the root trunk of this peer
8. Under **Associated Mediation Server port**, type the listening port that the Mediation Server will receive SIP messages from the peer.

Note:
With multiple trunk support in Lync Server 2013, two trunks with different trunk names cannot be configured with the same **Associated Mediation Server port** and **Listening Port for IP/PSTN gateway**

Note:
With multiple trunk support in Lync Server 2013, multiple SIP signaling ports can be defined on the Mediation Server for communication with multiple peers. When defining a trunk, the **Associated Mediation Server port** number must be within the range of the listening ports for the respective protocol allowed by the Mediation Server. This port range is defined under Lync Server 2013 and Mediation Server pools. Right-click the relevant Mediation Server pool, and select **Edit Properties**. Specify the port range in the **Listening ports** field.

9. Click **OK**.

Tasks

Modify a Trunk in Topology Builder

1.4.3.2.3.1 Modify a Trunk in Topology Builder

Modify a Trunk in Topology Builder

Deploying Enterprise Voice > Deploying Mediation Servers and Defining Peers > Define a Gateway in Topology Builder >

Topic Last Modified: *2012-09-21*

Follow these steps to modify the alternate media IP address and alternate bypass identifier of a trunk.

To Modify the Alternate Media IP Address of a Trunk

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsPstnGateway cmdlet and modify the AlternateBypassId field in the Lync Server Management Shell.

```
Set-CsPstnGateway -Identity "PstnGateway:<peer FQDN> -RepresentativeMe
```

To Modify the Alternate BypassID of a Trunk

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsPstnGateway cmdlet and modify the AlternateBypassId field in the Lync Server Management Shell.

```
Set-CsPstnGateway -Identity "PstnGateway:<peer FQDN> -AlternateBypassI
```

1.4.3.2.4 Install the Files for Mediation Server

Install the Files for Mediation Server

See Also

Deployment > Deploying Enterprise Voice > Deploying Mediation Servers and Defining Peers >

Topic Last Modified: *2012-08-06*

To successfully complete this procedure, you should be logged on to the server, at the minimum, as a local administrator and a domain user who has membership in at least the RTCUniversalReadOnlyAdmins group.

Use the steps in this topic to run Lync Server 2013 Deployment Wizard to install the files for Mediation Server on a computer that you added to a Mediation Server pool when you used Topology Builder to define and publish the pool. When installing files Mediation Server, you also install and assign the certificate required by each computer in a Mediation Server pool.

At this site, if you have already deployed Mediation Servers collocated on the Front End pools or Standard Edition server, you can skip this topic and, instead, continue to Configuring Trunks.

Note:
This topic assumes that you have already defined and published a stand-alone Mediation Server pool as described in Define a Mediation Server in Topology Builder and Publish the Topology in the Deployment documentation, and that you have verified that the computers in the Mediation Server pool meet the prerequisites described in Software Prerequisites for Enterprise Voice and Security and Configuration Prerequisites for Enterprise Voice.

To install the files for a stand-alone Mediation Server pool

1. From the installation media, right-click <*installation media*>**\Setup\amd64\Setup.exe**, and then click **Run as Administrator**.
2. On the **Installation Location** page, click **OK**.
3. On the **End User License Agreement** page, click **I accept**, and then click **OK**. (Required to continue.)
4. On the **Lync Server 2010 Deployment Wizard** page, click **Install or Update Lync Server System**.
5. Next to **Step 1: Install Local Configuration Store**, click **Run**, and then follow the instructions on the screen.
6. On the **Configure Local Replica of Central Management Store** page, accept the default **Retrieve directly from the Central Management Store**, and then click **Next**.
7. On the **Executing Commands** page, when the task status is shown as **Completed**, click **Finish**.
8. Next to **Step 2: Setup or Remove Lync Server Components**, click **Run**, and then click **Next**.
9. On the **Executing Commands** page, when the task status is shown as **Completed**, click **Finish**.
10. Next to **Step 3: Request, Install or Assign Certificates**, click **Run**. Follow the instructions on the screen, accepting the default settings. The Mediation Server requires one certificate, and so you will run **Step 3** twice: once to issue the required certificate, and once more to assign it.
11. When the certificate has been issued and assigned correctly, beside **Step 4: Start Services**, click **Run**, and then follow the instructions on the screen.
12. When **Step 4** has completed successfully, restart the server, and log on to the server as a member of the DomainAdmins group.
13. On the computer where you are running Lync Server Control Panel, verify on the **Topology** page of Lync Server Control Panel that the service status of the Mediation Server is shown as a green check mark. If a red X appears instead, select the Mediation Server. On the **Action** menu, click **Start All Services**.

If you added more than one computer to the Mediation Server pool, perform the steps in this procedure on all other computers in the Mediation Server pool. If you do not need to install files for Mediation Server for any other computers, then follow the procedures in Configuring Trunks to configure settings for the trunk connection between this Mediation Server pool (or all Mediation Servers at a site) and its peer.

Concepts

Certificate Requirements for Internal Servers

1.4.3.3 Configuring Trunks

Configuring Trunks

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-11-01*

As part of Enterprise Voice deployment, you can configure a trunk between a Mediation Server and one or more of the following peers to provide public switched telephone network (PSTN) connectivity for Enterprise Voice clients and devices in your organization:

- SIP trunk connection to an Internet telephony service provider (ITSP)
- PSTN gateway
- Private branch exchange (PBX)

For details, see Planning for PSTN Connectivity in the Planning documentation.

Important:

Before you begin trunk configuration, verify that the topology has been created and that the Mediation Server and its peer have been configured and associated with one another. For details, see Define a Gateway in Topology Builder in the Deployment documentation.

Note:

As a part of trunk configuration, you can enable the Lync Server 2013 media bypass feature, which enables media to bypass the Mediation Server. Trunks can be configured either with or without media bypass enabled, but we strongly recommend that you enable it. For details, see Planning for Media Bypass in the Planning documentation.

- Multiple Trunk Support
- Inter-Trunk Routing
- View Trunk Configuration Information
- Configure a Trunk with Media Bypass
- Configure a Trunk without Media Bypass
- Create a New Collection of Trunk Configuration Settings
- Delete an Existing Collection of SIP Trunk Configuration Settings
- Modify SIP Trunk Configuration Settings
- Test SIP Trunk Configuration Settings
- View Information about Individual SIP Trunks

See Also

Tasks

Define a Gateway in Topology Builder

Other Resources

Planning for PSTN Connectivity
Planning for Media Bypass

1.4.3.3.1 Multiple Trunk Support

Multiple Trunk Support

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2012-11-01*

Lync Server 2013 functionality supports multiple associations between gateways and Mediation Servers. These associations are made by defining a trunk, which is a logical association between a Mediation Server pool and a public switched telephone network (PSTN) gateway, Session Border Controller (SBC), or IP-PBX. Use the Topology Builder to associate gateways with Mediation Servers (that is, trunks).

- To assign or remove a trunk in Lync Server 2013, you must first define a trunk in Topology Builder. A trunk consists of the following association: Mediation Server fully qualified domain name (FQDN), the Mediation Server listening port, the gateway FQDN, and the gateway listening port.
- To configure multiple trunks, you can create multiple associations between the same gateway and the Mediation Server. This provides additional resiliency to

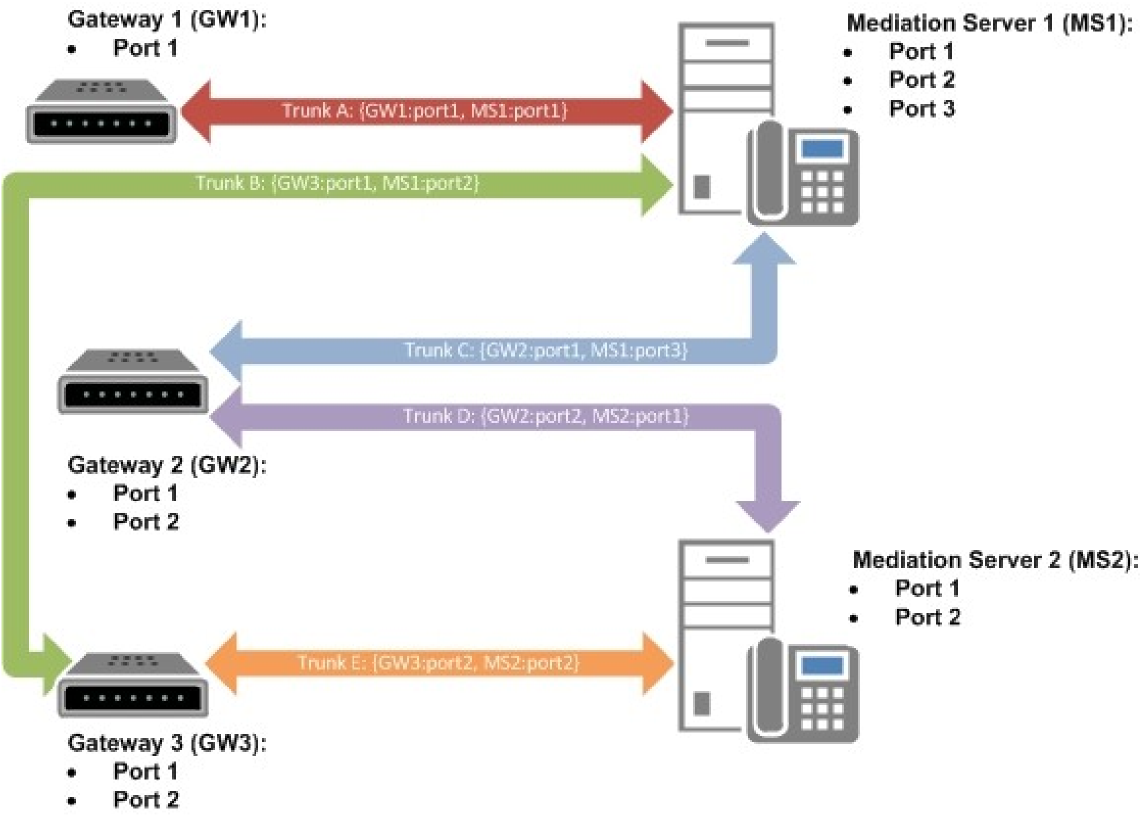
the Enterprise Voice infrastructure, which is especially useful in private branch exchange (PBX) interoperational scenarios.

When a trunk is defined, it must be associated to a route. To associate a trunk to a route, you define a simple name for the trunk in Topology Builder. This simple name is used as the trunk name in the Lync Server Control Panel, where trunks can be associated with routes. The simple trunk name is used as the gateway name from the Lync Server Management Shell.

```
New-CsVoiceRoute -Identity <RouteId> -NumberPattern <String> -PstnUsages @{add="<
```

The administrator must select a default trunk associated with a Mediation Server. From the Topology Builder, right-click the associated Mediation Server, and then click **Properties**. Specify the default gateway for the Mediation Server.

The following diagram illustrates the multiple trunks that are defined for each Mediation Server and gateway.


Gateway 1 (GW1):
• Port 1
Mediation Server 1 (MS1):
• Port 1
• Port 2
• Port 3
Trunk A: {GW1:port1, MS1:port1}
Trunk B: {GW3:port1, MS1:port2}
Trunk C: {GW2:port1, MS1:port3}
Trunk D: {GW2:port2, MS2:port1}
Gateway 2 (GW2):
• Port 1
• Port 2
Mediation Server 2 (MS2):
• Port 1
• Port 2
Trunk E: {GW3:port2, MS2:port2}
Gateway 3 (GW3):
• Port 1
• Port 2

1.4.3.3.2 Configure a Trunk w ith Media Bypass

Configure a Trunk with Media Bypass

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2013-02-24*

Follow these steps to configure a trunk with media bypass enabled. To configure a trunk with media bypass disabled, see Configure a Trunk without Media Bypass.

We strongly recommend that you enable media bypass. However, before you enable media bypass on a SIP trunk, confirm that your qualified SIP trunk provider supports media bypass and is able to accommodate the requirements for successfully enabling the scenario. Specifically, the provider must have the IP addresses of servers in your organization's internal network. If the provider cannot support this scenario, media bypass will not succeed. For details, see Planning for Media Bypass in the Planning documentation.

Note:
Media bypass will not interoperate with every public switched telephone network (PSTN) gateway, IP-PBX, and Session Border Controller (SBC). Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions that are listed on Unified Communications Open Interoperability Program – Lync Server at http://go.microsoft.com/fwlink/p/?linkId=214406.

A trunk configuration as described below groups a set of parameters that are applied to trunks assigned this trunk configuration. A particular trunk configuration can be scoped globally (to all trunks that do not have more specific site or pool configuration), or to a site, or to a pool. The pool-level trunk configuration is used to scope a specific trunk configuration to a single trunk.

⊟To configure a trunk with media bypass

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
4. On the **Trunk Configuration** page, use one of the following methods to configure a trunk:
   - Double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
   - Click **New**, and then select a scope for the new trunk configuration:
     - **Site trunk:** Choose the site for this trunk configuration from **Select a Site**, and then click **OK**. Note that if a trunk configuration has already been created for a site, the site does not appear in **Select a Site**. This trunk configuration will be applied to all trunks in the site.
     - **Pool trunk:** Choose the name of the trunk that this trunk configuration applies to. This trunk can be the root trunk or any additional trunks defined in Topology Builder. From **Select a Service**, click **OK**. Note that if a trunk configuration has already been created for a specific trunk, the trunk does not appear in **Select a Service**.

   Note:
   After you select the scope of the trunk configuration, it cannot be changed. The **Name** field is prepopulated with the name of the trunk configuration's associated site or service and cannot be changed.
5. Specify a value in **Maximum early dialogs supported**. This is the maximum number of forked responses a public switched telephone network (PSTN) gateway, IP-PBX, or ITSP Session Border Controller (SBC) can receive to an INVITE that it sent to the Mediation Server. The default value is 20.

   Note:

Before you change this value, consult your service provider or equipment manufacturer for details about the capabilities of your system.

6. Select one of the following **Encryption support level** options:
   - **Required:** Secure real-time transport protocol (SRTP) encryption must be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
   - **Optional:** SRTP encryption will be used if the service provider or equipment manufacturer supports it.
   - **Not Supported:** SRTP encryption is not supported by the service provider or equipment manufacturer and therefore will not be used.
7. Select the **Enable media bypass** check box if you want media to bypass the Mediation Server for processing by the trunk peer.

   Important:

   For media bypass to work successfully, the PSTN gateway, IP-PBX, or ITSP Session Border Controller must support certain capabilities. For details, see Planning for Media Bypass in the Planning documentation.
8. Select the **Centralized media processing** check box if there is a well-known media termination point (for example, a PSTN gateway where the media termination has the same IP as the signaling termination). Clear this check box if the trunk does not have a well-known media termination point.
9. If the trunk peer supports receiving SIP REFER requests from the Mediation Server, select the **Enable sending refer to the gateway** check box.

   Note:

   If you disable this option while the **Enable media bypass** option is selected, additional settings are required. If the trunk peer does not support receiving SIP REFER requests from the Mediation Server and media bypass is enabled, you must also run the **Set-CsTrunkConfiguration** cmdlet to disable RTCP for active and held calls in order to support proper conditions for media bypass. For details, see the Lync Server Management Shell documentation. Alternatively, you can select **Enable refer using third-party-call control** if you want transferred calls to be media bypassed, and the gateway does not support SIP REFER requests.
10. (Optional) To enable inter-trunk routing, associate and configure PSTN usage records to this trunk configuration. The PSTN usages associated to this trunk configuration will be applied for all incoming calls through the trunk that is not originating from a Lync endpoint. To manage PSTN usage records associated to a trunk configuration, use one of the following methods:
    - To select one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records you want to associate with this trunk configuration and then click **OK**.
    - To remove a PSTN usage record from this trunk configuration, select the record and click **Remove**.
    - To define a new PSTN usage record and associate it with this trunk configuration, do the following:
      - Click **New**.
      - In the **Name** field, specify a descriptive name for the record that is unique.

        Note:

        The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.
      - Use one of the following methods to associate and configure routes for this PSTN usage record:
        - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.

        - To remove a route from the PSTN usage record, select the route, and click **Remove**.
        - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
        - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
    - Click **OK**.
- To edit a PSTN usage record that is already associated with this trunk configuration, do the following:
    - Select the PSTN usage record you want to edit, and click **Show details**.
    - Use one of the following methods to associate and configure routes for this PSTN usage record:
        - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
        - To remove a route from the PSTN usage record, select the route, and click **Remove**.
        - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
        - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
    - Click **OK**.

> **Important:**
>
> It important to associate PSTN usage records according to the Mediation Server peer that is associated to the trunk being configured. If the Mediation Server peer is a PSTN gateway or a Session Border Controller (SBC), it is strongly recommended that the trunk configuration is not associated to a PSTN usage record that routes to a PSTN destination or any other downstream systems connected via Lync Server.

11. Arrange the PSTN usage records for optimum performance. To change a record’s position in the list, select the PSTN usage record, and click the up or down arrows.

> **Important:**
>
> The order in which PSTN usage records are listed in the trunk configuration is significant. Lync Server traverses the list from top to down.

12. **Enable RTP Latching** should be selected to enable bypass media for clients behind a network address translation (NAT) or firewall and an SBC that supports latching.
13. **Enable forward call history** should be selected to enable sending of call history information to the gateway peer of the Mediation Server.
14. **Enable forward P-Asserted-Identity data** should be selected to enable the P-Asserted-Identity (PAI) call originator information to be forwarded between the Mediation Server side and gateway side (and vice versa), when present.
15. **Enable outbound routing failover timer** should be selected to enable fast failover. The gateway associated with this trunk can give notification within 10 seconds that it is processing an outbound call. Rerouting to another trunk will occur if this notification is not received by the Mediation Server. On networks where latency may delay the response time or the gateway takes longer than 10 seconds to respond, the fast failover should be disabled.
16. (Optional) Associate and configure **calling number translation rules** for the trunk. These translation rules apply to the calling number for outbound calls
    - To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
    - To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the

Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

> ⚠**Warning:**
>
> Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

17.(Optional) Associate and configure **called number translation rules** for the trunk. The translation rules apply to the called number in an outbound call.
- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

> ⚠**Warning:**
>
> Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

18.Make sure that the trunk’s translation rules are arranged in the correct order. To change a rule’s position in the list, highlight the rule name and then click the up or down arrow.

> **Important:**
>
> Lync Server 2013 traverses the translation rule list from the top down and uses the first rule that matches the dialed number. If you configure a trunk so that a dialed number can match more than one translation rule, be sure that the more restrictive rules are sorted above the less restrictive rules. For example, if you have included a translation rule that matches any 11-digit number and a translation rule that matches only 11-digit numbers that start with +1425, be sure that the rule that matches any 11-digit number is sorted *below* the more restrictive rule.

19.When you are finished configuring the trunk, click **OK**.
20.On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

> **Note:**
>
> Whenever you create or modify a trunk configuration, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

After you have configured the trunk, continue configuring media bypass by choosing between global media bypass options, as described in Global Media Bypass Options in the Deployment documentation.

Tasks

Configure a Trunk without Media Bypass

Concepts

Configure Media Bypass
Global Media Bypass Options

Other Resources

Defining Translation Rules

1.4.3.3.3 Configure a Trunk w ithout Media Bypass

Configure a Trunk without Media Bypass

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2013-02-24*

If you want to configure a trunk with media bypass disabled, follow these steps. If you want to configure a trunk with media bypass enabled, see Configure a Trunk with Media Bypass.

A trunk configuration, as described below, groups a set of parameters that are applied to trunks assigned this trunk configuration. A particular trunk configuration can be scoped globally (to all trunks that do not have more specific site or pool configuration), or to a site, or to a pool. The pool-level trunk configuration is used to scope a specific trunk configuration to a single trunk.

⊟To configure a trunk without media bypass

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
4. On the **Trunk Configuration** page, use one of the following methods to configure a trunk:
   - Double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
   - Click **New**, and then select a scope for the new trunk configuration:
     - **Site trunk:** Choose the site for this trunk configuration in **Select a Site** , and then click **OK**. Note that if a trunk configuration has already been created for a site, the site does not appear in **Select a Site**. This trunk configuration will be applied to all trunks in the site.
     - **Pool trunk:** Choose the name of the trunk that this trunk configuration applies to in **Select a Service** and click **OK**. This trunk can be the root trunk, or any additional trunks defined in Topology Builder. Note that if a trunk configuration has already been created for a specific trunk, the trunk does not appear in **Select a Service**.

   Note:

After you select the scope of the trunk configuration, it cannot be changed. The **Name** field is prepopulated with the name of the trunk configuration’s associated site or service and cannot be changed.

5. Select one of the following **Encryption support level** options:
   - **Required:** Secure real-time transport protocol (SRTP) encryption must be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
   - **Optional:** SRTP encryption will be used if the service provider or equipment manufacturer supports it.
   - **Not Supported:** SRTP encryption is not supported by the service provider or equipment manufacturer and therefore will not be used.
6. Be sure that the **Enable media bypass** check box is cleared.
7. Select the **Centralized media processing** check box if there is a well-known media termination point (for example, a public switched telephone network (PSTN) gateway where the media termination has the same IP as the signaling termination). Clear this check box if the trunk does not have a well-known media termination point.
8. If the trunk peer supports receiving SIP REFER requests from the Mediation Server, select the **Enable sending refer to the gateway** check box.
9. (Optional) To enable inter-trunk routing, associate and configure PSTN usage records to this trunk configuration. The PSTN usages associated to this trunk configuration will be applied for all incoming calls through the trunk that is not originating from a Lync endpoint. To manage PSTN usage records associated to a trunk configuration, use one of the following methods:
   - To select one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records you want to associate with this trunk configuration and then click **OK**.
   - To remove a PSTN usage record from this trunk configuration, select the record and click **Remove**.
   - To define a new PSTN usage record and associate it with this trunk configuration, do the following:
     - Click **New**.
     - In the **Name** field, specify a descriptive name for the record that is unique.

       Note:

       The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

     - Use one of the following methods to associate and configure routes for this PSTN usage record:
       - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
       - To remove a route from the PSTN usage record, select the route, and click **Remove**.
       - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
       - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
     - Click **OK**.
   - To edit a PSTN usage record that is already associated with this trunk configuration, do the following:
     - Select the PSTN usage record you want to edit, and click **Show details**.
     - Use one of the following methods to associate and configure routes for this PSTN usage record:
       - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you

want to associate with this PSTN usage record, and click **OK**.

- To remove a route from the PSTN usage record, select the route, and click **Remove**.
- To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
- To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.

- Click **OK**.

> ◆**Important:**
>
> It important to associate PSTN usage records according to the Mediation Server peer that is associated to the trunk being configured. If the Mediation Server peer is a PSTN gateway or a Session Border Controller (SBC), it is strongly recommended that the trunk configuration is not associated to a PSTN usage record that routes to a PSTN destination or any other downstream systems connected via Lync Server.

10. Arrange the PSTN usage records for optimum performance. To change a record’s position in the list, select the PSTN usage record, and click the up or down arrows.

> ◆**Important:**
>
> The order in which PSTN usage records are listed in the trunk configuration is significant. Lync Server traverses the list from top to down.

11. **Enable RTP Latching** should be selected to enable bypass media for clients behind a NAT or firewall and an SBC that supports latching.
12. **Enable forward call history** should be selected to enable sending of call history information to the gateway peer of the Mediation Server.
13. **Enable forward P-Asserted-Identity data** should be selected to enable PAI call originator information to be forwarded between the Mediation Server side and gateway side (and vice versa), when present.
14. **Enable outbound routing failover timer** should be selected to enable fast failover. The gateway associated with this trunk can give notification within 10 seconds that it is processing an outbound call. Rerouting to another trunk will occur if this notification is not received by the Mediation Server. On networks where latency may delay the response time or the gateway takes longer than 10 seconds to respond, the fast failover should be disabled.
15. (Optional) Associate and configure **calling number translation rules** for the trunk. These translation rules apply to the calling number for outbound calls
    - To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
    - To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
    - To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
    - To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
    - To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

> 🔒**Security Note:**
>
> Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

16. (Optional) Associate and configure **called number translation rules** for the trunk. The translation rules apply to the called number in an outbound call.

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

Caution:
Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

17. Make sure that the trunk's translation rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name, and then click the up or down arrow.

Important:
Lync Server traverses the translation rule list from the top down and uses the first rule that matches the dialed number. If you configure a trunk so that a dialed number can match more than one translation rule, be sure that the more restrictive rules are sorted above the less restrictive rules. For example, if you have included a translation rule that matches any 11-digit number and a translation rule that matches only 11-digit numbers that start with +1425, be sure that the rule that matches any 11-digit number is sorted *below* the more restrictive rule.

18. When you are finished configuring the trunk, click **OK**.
19. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

Note:
Whenever you create or modify a trunk configuration, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Configure a Trunk with Media Bypass

Other Resources

Defining Translation Rules

1.4.3.3.4 Defining Translation Rules

Defining Translation Rules

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2013-02-22*

Lync Server 2013 Enterprise Voice routes calls based on phone numbers normalized to E.164 format. This means that all dialed strings must be normalized to E.164 format for the purpose of performing reverse number lookup (RNL) so they can be translated to their matching SIP URI. Lync Server 2013 provides the ability to manipulate the called ID and the caller ID presentation.

This section discusses how to manipulate the called ID and caller ID.

- Caller ID Presentation
- Called ID Presentation

⊟See Also

Other Resources

Defining Normalization Rules

1.4.3.3.4.1 Caller ID Presentation

Caller ID Presentation

Deploying Enterprise Voice > Configuring Trunks > Defining Translation Rules >

Topic Last Modified: *2013-02-22*

With Lync Server 2010, the called party’s phone number (that is, the phone number called) can be translated from E.164 format to the local dialing format that is required by the *trunk peer* (that is, the associated gateway, private branch exchange (PBX), or SIP trunk). To do this, you must define one or more translation rules to translate the Request URI before routing it to the trunk peer.

Lync Server 2013 introduces the option to also translate the calling party’s phone number (that is, the phone number that the caller is calling from) from E.164 format to the local dialing format that is required by the trunk peer. For example, you can write a translation rule to remove +44 from the beginning of a dial string and replace it with 0144.

To configure Caller ID by using Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
4. On the **Trunk Configuration** page, double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
5. To configure caller ID presentation:
   - To choose one or more rules from a list of all translation rules available in your Enterprise Voice deployment, click **Select**. In **Calling number translation rules**, click the rules that you want to associate with the trunk, and then click **OK**.
   - To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
   - To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
   - To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
   - To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

⚠Warning:

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

1.4.3.3.4.2 Called ID Presentation

Called ID Presentation

See Also

Deploying Enterprise Voice > Configuring Trunks > Defining Translation Rules >

Topic Last Modified: *2012-09-21*

With Lync Server 2010, the called party's phone number (that is, the phone number called) can be translated from E.164 format to the local dialing format that is required by the *trunk peer* (that is, the associated gateway, private branch exchange (PBX), or SIP trunk). To do this, you must define one or more translation rules to translate the Request URI before routing it to the trunk peer.

Important:

The ability to associate one or more translation rules with an Enterprise Voice trunk configuration is intended to be used as an *alternative* to configuring translation rules on the trunk peer. Do not associate translation rules with an Enterprise Voice trunk configuration if you have configured translation rules on the trunk peer because the two rules might conflict.

You can use either of the following methods to create or modify a translation rule:

- Use the **Build a Translation Rule** tool to specify values for the starting digits, length, digits to remove and digits to add, and then let Lync Server Control Panel generate the corresponding matching pattern and translation rule for you.
- Write regular expressions manually to define the matching pattern and translation rule.

Note:

For information about how to write regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.

- Create or Modify a Translation Rule by Using the Build a Translation Rule Tool
- Create or Modify a Translation Rule Manually

See Also

Concepts

Caller ID Presentation

Create or Modify a Translation Rule by Using the Build a Translation Rule Tool

See Also

Configuring Trunks > Defining Translation Rules > Called ID Presentation >

Topic Last Modified: *2012-10-05*

Follow these steps if you want to define a translation rule by entering a set of values in the **Build a Translation Rule** tool and enabling Lync Server Control Panel to generate the corresponding matching pattern and translation rule for you. Alternatively, you can a write regular expression manually to define the matching pattern and translation rule. For details, see Create or Modify a Translation Rule Manually.

⊟To define a rule by using the Build a Translation Rule tool

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. To begin defining a translation rule, follow the steps in Configure a Trunk with Media Bypass through step 10 or Configure a Trunk without Media Bypass through step 9.
4. Under **Name** on the **New Translation Rule** or **Edit Translation Rule** page, type a name that describes the number pattern being translated.
5. (Optional) Under **Description**, type a description of the translation rule, for example **US International long-distance dialing**.
6. In the **Build a Translation Rule** section of the dialog box, enter values in the following fields:
   - **Starting digits**: (Optional) Specify the leading digits of numbers you want the pattern to match. For example, enter **+** in this field to match numbers in E.164 format (which begin with +).
   - **Length**: Specify the number of digits in the matching pattern and select whether you want the pattern to match numbers that are this length exactly, at least this length, or any length. For example, enter **11** and select **At least** in the drop-down list to match numbers that are at least 11 digits in length.
   - **Digits to remove**: (Optional) Specify the number of starting digits to be removed. For example, enter **1** to strip out the **+** from the beginning of the number.
   - **Digits to add**: (Optional) Specify digits to be prepended to the translated numbers. For example, enter **011** if you want 011 to be prepended to the translated numbers when the rule is applied.

   The values you enter in these fields are reflected in the **Pattern to match** and **Translation rule** fields. For example, if you specify the preceding example values, the resulting regular expression in the **Pattern to match** field is:

   ^\+(\d{9}\d+)$

   The **Translation rule** field specifies a pattern for the format of translated numbers. This pattern has two parts:
   - A value (for example, **$1**) that represents the number of digits in the matching pattern
   - (Optional) A value that you can prepend by entering it in the **Digits to add** field

   Using the preceding example values, **011$1** appears in the **Translation rule** field.

   When this translation rule is applied, +441235551010 becomes 011441235551010.
7. Click **OK** to save the translation rule.
8. Click **OK** to save the trunk configuration.
9. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

> **Note:**
>
> Whenever you create or modify a translation rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Translation Rule Manually
Configure a Trunk with Media Bypass
Configure a Trunk without Media Bypass
Publish Pending Changes to the Voice Routing Configuration

Concepts

Global Media Bypass Options

Create or Modify a Translation Rule Manually

See Also

Configuring Trunks > Defining Translation Rules > Called ID Presentation >

Topic Last Modified: *2012-08-06*

Follow these steps if you want to define a translation rule by writing a regular expression for the matching pattern and translation rule. Alternatively, you can enter a set of values in the **Build a Translation Rule** tool and enable Lync Server Control Panel to generate the corresponding matching pattern and translation rule for you. For details, see Create or Modify a Translation Rule by Using the Build a Translation Rule Tool.

⊟To define a translation rule manually

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. To begin defining a translation rule, follow the steps in Configure a Trunk with Media Bypass through step 10 or Configure a Trunk without Media Bypass through step 9.
4. In the **Name** field on the **New Translation Rule** or **Edit Translation Rule** page, type a name that describes the number pattern being translated.
5. (Optional) In **Description**, type a description of the translation rule, for example **US International long-distance dialing**.
6. Click **Edit** at the bottom of the **Build a Translation Rule** section.
7. Enter the following in **Type a Regular Expression**:
   - In **Match this pattern**, specify the pattern that will be used to match the numbers to be translated.
   - In **Translation rule**, specify a pattern for the format of translated numbers.

   For example, if you enter **^\+(\d{9}\d+)$** in **Match this pattern** and **011$1** in **Translation rule**, the rule will translate +441235551010 to 011441235551010.
8. Click **OK** to save the translation rule.
9. Click **OK** to save the trunk configuration.
10. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

Note:
Whenever you create or modify a translation rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Translation Rule by Using the Build a Translation Rule Tool
Configure a Trunk with Media Bypass
Configure a Trunk without Media Bypass
Publish Pending Changes to the Voice Routing Configuration

Concepts

Global Media Bypass Options

1.4.3.3.5 Inter-Trunk Routing

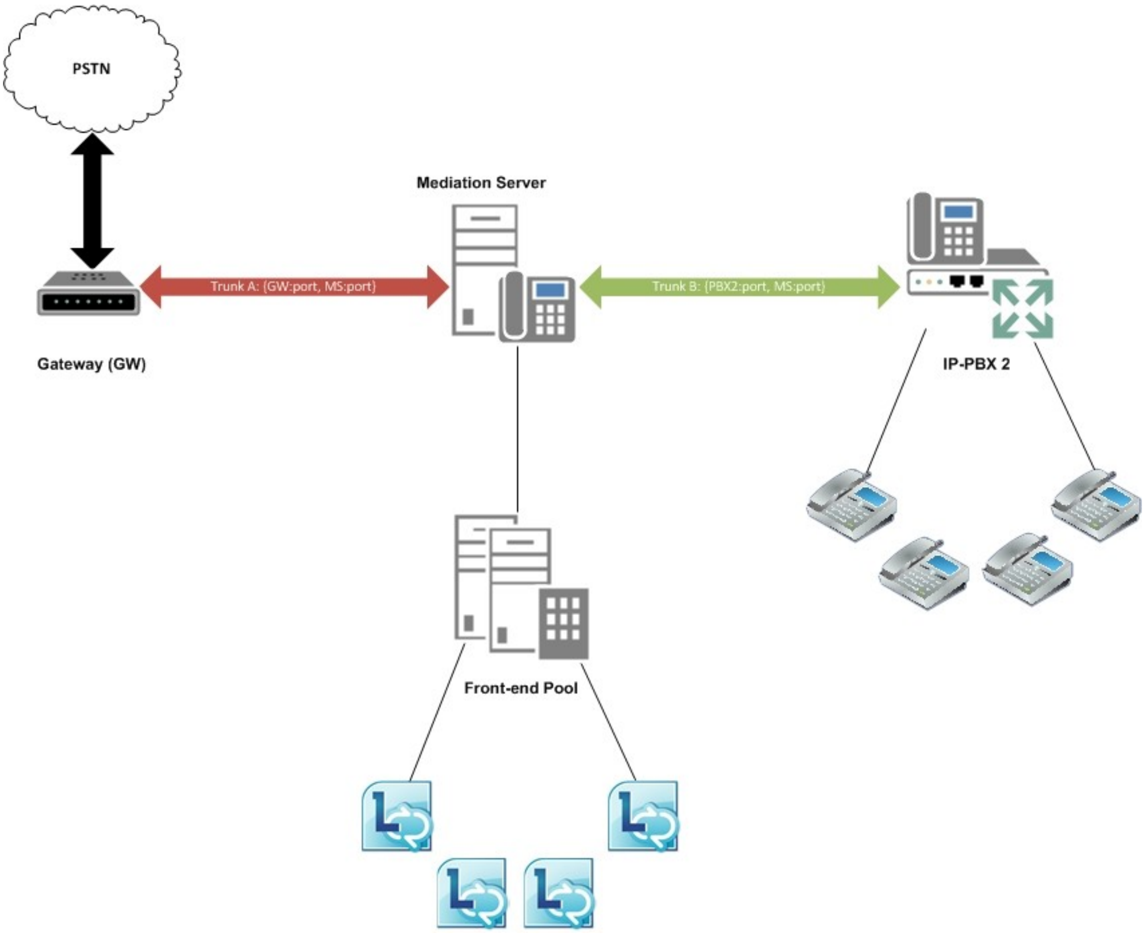
Inter-Trunk Routing

Planning > Planning for Enterprise Voice > Planning for PSTN Connectivity >

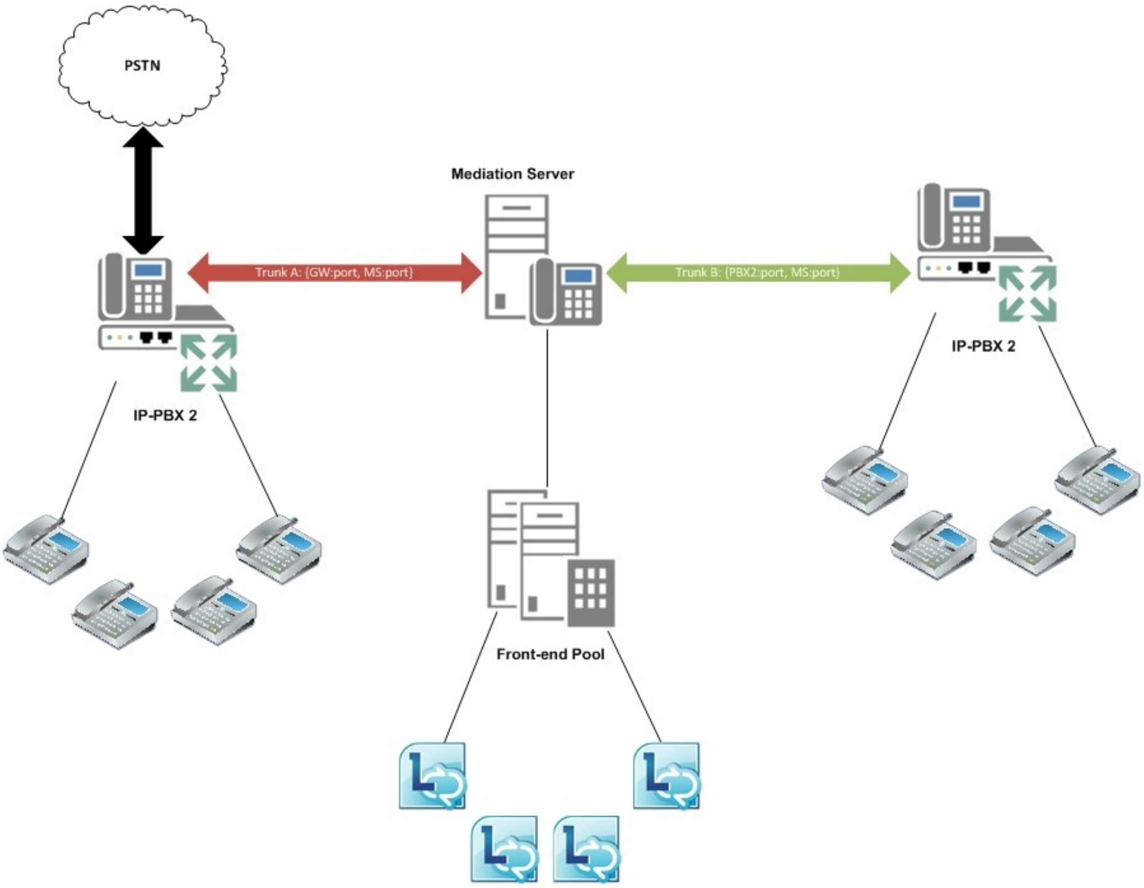
Topic Last Modified: *2012-10-08*

Lync Server 2013 provides basic session management through the support of intertrunk routing. This new capability enables Lync Server to provide call control functionalities to downstream telephony systems. Intertrunk routing can interconnect an IP-PBX to a public switched telephone network (PSTN) gateway so that calls from a private branch exchange (PBX) phone can be routed to the PSTN, and incoming PSTN calls can be routed to a PBX phone. Similarly, Lync Server can interconnect two or more IP-PBX systems so that calls can be placed and received between PBX phones from the different IP-PBX systems.

The following figure illustrates Lync Server 2013 providing interconnectivity between a PSTN gateway and an IP-PBX.



The next figure illustrates Lync Server 2013 connecting two IP-PBX systems.



1.4.3.4 Configuring Dial Plans

Configuring Dial Plans

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

***Topic Last Modified:** 2013-02-22*

A Lync Server 2013 dial plan is a named set of normalization rules that translate phone numbers for a named location, individual user, or contact object for purposes of phone authorization and call routing.

Note:
For details, see Dial Plans and Normalization Rules in the Planning documentation.

- View Dial Plan Information
- Create a Dial Plan
- Modify a Dial Plan

⊟See Also

Concepts

Dial Plans and Normalization Rules

1.4.3.4.1 View Dial Plan Information

View Dial Plan Information

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-11-01*

To view information for an existing dial plan, perform the steps in the following procedure. If you want to create a new dial plan, see Create a Dial Plan.

⊟To view information about a dial plan from Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, double-click a dial plan name.

> **Note:**
> You can view information for only one dial plan at a time.

⊟To view dial plans by using Windows PowerShell cmdlets

- Dial plans can be viewed by using the Windows PowerShell command-line interface and the **Get-CsDialPlan** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

  To view information about all your dial plans, type the following command in the Lync Server Management Shell, and then press ENTER:

  ```
  Get-CsDialPlan
  ```

  That command will return information similar to this:

  ```
  Identity                   : Global
  Description                :
  DialinConferencingRegion   :
  NormalizationRules         : {Description=;
                               Pattern=^(\d+)$;Translation=$1;Name=
                               KeepAll;IsInternalExtension=False}
  CountryCode                :
  State                      :
  City                       :
  ExternalAccessPrefix       :
  SimpleName                 : DefaultProfile
  OptimizeDeviceDialing      : False
  ```

Tasks

Create a Dial Plan
Modify a Dial Plan

1.4.3.4.2 Create a Dial Plan

Create a Dial Plan

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-10-06*

To create a new dial plan, perform the steps in the following procedure. If you want to edit a dial plan, see Modify a Dial Plan.

⊟To create a dial plan

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, click **New** and select a scope for the dial plan:
   - **Site dial plan** applies to an entire site, except any users or groups that are assigned to a user dial plan. If you select **Site** for a dial plan's scope, you must choose the site from the **Select a Site** dialog box. If a dial plan has already been created for a site, the site does not appear in the **Select a Site** dialog box.
   - **Pool dial plan** can apply to a public switched telephone network (PSTN) gateway or a Registrar. If you select **Pool** for a dial plan's scope, choose the PSTN gateway or Registrar from the **Select a Service** dialog box. If a dial plan has already been created for a service (PSTN gateway or Registrar), the service does not appear in the list.
   - **User dial plan** can be applied to specified users or groups.

Note:
After you select the dial plan scope, it cannot be changed.

5. If you are creating a user dial plan, enter a descriptive name in the **Name** field on the **New Dial Plan** dialog box. After this name is saved, it cannot be changed.

Note:
For site dial plans, the **Name** field is prepopulated with the site name and cannot be changed. For pool dial plans, the **Name** field is prepopulated with the PSTN gateway or Registrar name and cannot be changed.

6. The **Simple name** field is prepopulated with the same name that appears in the **Name** field. You can optionally edit this field to specify a more descriptive name that reflects the site, service, or user to which the dial plan applies.

Important:
The **Simple name** must be unique among all dial plans within the Lync Server deployment. It cannot exceed 256 Unicode characters, each of which can be an alphabetic or numeric character, a hyphen (-), a period (.), a plus sign (+), or an underscore (_). Spaces are not allowed in the **Simple name**.

7. (Optional) In the **Description** field, you can type additional descriptive information about the dial plan.
8. (Optional) If you want to use this dial plan as a region for dial-in access numbers, specify a **Dial-in conferencing region**. If you do not want to use this dial plan for dial-in access numbers, leave this field empty.

> **Note:**
> Dial-in conferencing regions are required to associate dial-in conferencing access numbers with one or more dial plans.

9. (Optional) In the **External access prefix** field, specify a value only if users need to dial one or more additional leading digits (for example, 9) to get an external line. You can type in a prefix value of up to four characters (#, *, and 0-9).

> **Note:**
> If you specify an external access prefix, you do not need to create a new normalization rule to accommodate the prefix.

10. Associate and configure normalization rules for the dial plan as follows:
    - To choose one or more rules from a list of all normalization rules available in your Enterprise Voice deployment, click **Select**. In **Select Normalization Rules**, highlight the rules you want to associate with the dial plan and then click **OK**.
    - To define a new normalization rule and associate it with the dial plan, click **New**. For details about defining a new rule, see Defining Normalization Rules.
    - To edit a normalization rule that is already associated with the dial plan, highlight the rule name and click **Show details**. For details about editing the rule, see Defining Normalization Rules.
    - To copy an existing normalization rule to use as a starting point for defining a new rule, highlight the rule name and click **Copy**, and then click **Paste**. For details about editing the copy, see Defining Normalization Rules.
    - To remove a normalization rule from the dial plan, highlight the rule name and click **Remove**.

> **Note:**
> Each dial plan must have at least one associated normalization rule. For information about how to determine all of the normalization rules a dial plan requires, see Dial Plans and Normalization Rules in the Planning documentation.

11. Verify that the dial plan’s normalization rules are arranged in the correct order. To change a rule’s position in the list, highlight the rule name and then click the up or down arrow.

> **Important:**
> Lync Server traverses the normalization rule list from the top down and uses the first rule that matches the dialed number. If you configure a dial plan so that a dialed number can match more than one normalization rule, make sure the more restrictive rules are sorted above the less restrictive ones.
> The default **Keep All** normalization rule **^(\d{11})$** matches any 11-digit number. For example, if you add a normalization rule that matches 11-digit numbers that start with 1425, make sure that **Keep All** is sorted below the more restrictive **^(1425\d{7})$** rule.

12. (Optional) Enter a number to test the dial plan and then click **Go**. The test results are displayed under **Enter a number to test**.

> **Note:**
> You can save a dial plan that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

13. Click **OK**.
14. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

> **Note:**
> Any time you create a dial plan, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Modify a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Defining Normalization Rules

1.4.3.4.3 Modify a Dial Plan

Modify a Dial Plan

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-11-01*

To modify an existing dial plan, perform the steps in the following procedure. If you want to create a new dial plan, see Create a Dial Plan.

⊟To modify a dial plan

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, double-click a dial plan name.

   Note:
   The dial plan scope and name were set when the dial plan was created. They cannot be changed.

5. (Optional) In **Edit Dial Plan**, edit the **Simple name** field, which is prepopulated with the same name that appears in the **Name** field to specify a more descriptive name that reflects the site, service, or user to which the dial plan applies.

   Important:
   The **Simple name** must be unique among all dial plans within the Lync Server 2013 deployment. It cannot exceed 256 Unicode characters, each of which can be an alphabetic or numeric character, a hyphen (-), a period (.), a plus sign (+), or an underscore (_).
   Spaces are not allowed in the **Simple name** field.

6. (Optional) In the **Description** field, type descriptive information about the dial plan.
7. (Optional) If you want to use this dial plan as a region for dial-in access numbers, specify a **Dial-in conferencing region**. If you do not want to use this dial plan for dial-in access numbers, leave this field empty.

   Note:
   Dial-in conferencing regions are required to associate dial-in conferencing access numbers with one or more dial plans.

8. (Optional) In the **External access prefix** field, specify a value only if users need to dial one or more additional leading digits to get an external line (for example, 9). You can type in a prefix value of up to four characters (that is, #, *, and 0-9).

   Note:
   If you specify an external access prefix, you do not need to create a new

normalization rule to accommodate the prefix.

9. Associate and configure normalization rules for the dial plan:
   - To choose one or more rules from a list of all normalization rules available in your Enterprise Voice deployment, click **Select**. In the **Select Normalization Rules** dialog box, highlight the rules that you want to associate with the dial plan and then click **OK**.
   - To define a new normalization rule and associate it with the dial plan, click **New**. For details about defining a new rule, see Defining Normalization Rules.
   - To edit a normalization rule that is already associated with the dial plan, highlight the rule name and click **Show details**. For details about editing the rule, see Defining Normalization Rules.
   - To copy an existing normalization rule to use as a starting point for defining a new rule, highlight the rule name and click **Copy**, and then click **Paste**. For details about editing the copy, see Defining Normalization Rules.
   - To remove a normalization rule from the dial plan, highlight the rule name and click **Remove**.

Note:

Each dial plan must have at least one associated normalization rule. For details about how to determine all of the normalization rules a dial plan requires, see Dial Plans and Normalization Rules in the Planning documentation.

10. Verify that the dial plan’s normalization rules are arranged in the correct order. To change a rule’s position in the list, highlight the rule name and then click the up or down arrow.

Important:

Lync Server traverses the normalization rule list from the top down and uses the first rule that matches the dialed number. If you configure a dial plan so that a dialed number can match more than one normalization rule, make sure the more restrictive rules are sorted above the less restrictive ones.

The default **Keep All** normalization rule **^(\d{11})$** matches any 11-digit number. If, for example, you add a normalization rule that matches 11-digit numbers that start with 1425, make sure that **Keep All** is sorted below the more restrictive **^(1425\d{7})$** rule.

11. (Optional) Enter a number to test the dial plan and then click **Go**. The test results are displayed under **Enter a number to test**.

Note:

You can save a dial plan that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

12. Click **OK**.
13. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

Note:

Any time you create or modify a dial plan, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create a Dial Plan

Publish Pending Changes to the Voice Routing Configuration

Other Resources

Defining Normalization Rules

1.4.3.4.4 Defining Normalization Rules

Defining Normalization Rules

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-09-23*

Lync Server 2013 normalization rules use .NET Framework regular expressions to translate dialed phone numbers to E.164 format. Each dial plan must be assigned one or more normalization rules.

For details about normalization rules, see Dial Plans and Normalization Rules in the Planning documentation.

For details about how to write regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.

You can use either of the following methods to define or edit a normalization rule:

- Use the **Build a Normalization Rule** tool to specify values for the starting digits, length, digits to remove and digits to add, and then let Lync Server Control Panel generate the corresponding matching pattern and translation rule for you.
- Write regular expressions manually to define the matching pattern and translation rule.
- Create or Modify a Normalization Rule by Using Build a Normalization Rule
- Create or Modify a Normalization Rule Manually

⊟See Also

Tasks

Create a Dial Plan
Modify a Dial Plan

1.4.3.4.4.1 Create or Modify a Normalization Rule by Using Build a Normalization Rule

Create or Modify a Normalization Rule by Using Build a Normalization Rule

See Also

Deploying Enterprise Voice > Configuring Dial Plans > Defining Normalization Rules >

Topic Last Modified: *2012-11-01*

Complete the following steps if you want to create or modify a normalization rule in Lync Server Control Panel. Alternatively, if you want to create or modify a normalization rule manually, see Create or Modify a Normalization Rule Manually.

⊟To define a rule by using Build a Normalization Rule

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. (Optional) Follow the steps in Create a Dial Plan through step 11 or Modify a Dial Plan through step 10.

4. In **New Normalization Rule** or **Edit Normalization Rule**, type a name that describes the number pattern being normalized in **Name** (for example, **5DigitExtension**).
5. (Optional) In **Description**, type a description of the normalization rule (for example, "Translates 5-digit extensions").
6. In **Build a Normalization Rule**, enter values in the following fields:
   - **Starting digits** (Optional) Specify the leading digits of dialed numbers you want the pattern to match. For example, type **425** if you want the pattern to match dialed numbers beginning with 425.
   - **Length** Specify the number of digits in the matching pattern and select whether you want the pattern to match this length exactly, match dialed numbers that are at least this length, or match dialed numbers of any length.
   - **Digits to remove** (Optional) Specify the number of starting digits to be removed from dialed numbers you want the pattern to match.
   - **Digits to add** (Optional) Specify digits to be added to dialed numbers you want the pattern to match.

   The values you enter in these fields are reflected in **Pattern to match** and **Translation rule**. For example, if you leave **Starting digits** empty, type **7** into the **Length** field and select **Exactly**, and specify **0** in **Digits to remove**, the resulting regular expression in the **Pattern to match** is:

   ^(\d{7})$
7. In **Translation rule**, specify a pattern for the format of translated E.164 phone numbers as follows:
   - A value that represents the number of digits specified in the matching pattern. For example, if the matching pattern is **^(\d{7})$** then **$1** in the translation rule represents 7-digit dialed numbers.
   - (Optional) Type a value into the **Digits to add** field to specify digits to be prepended to the translated number (for example, **+1425**).

   For example, if **Pattern to match** contains **^(\d{7})$** as the pattern for dialed numbers and **Translation rule** contains **+1425$1** as the pattern for E.164 phone numbers, the rule normalizes 5550100 to +14255550100.
8. (Optional) If the normalization rule results in a phone number that is internal to your organization, select **Internal extension**.
9. (Optional) Enter a number to test the normalization rule, and then click **Go**. The test results are displayed under **Enter a number to test**.

   Note:
   You can save a normalization rule that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.
10. Click **OK** to save the normalization rule.
11. Click **OK** to save the dial plan.
12. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

    Note:
    Whenever you create or change a normalization rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Normalization Rule Manually
Create a Dial Plan
Modify a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

1.4.3.4.4.2 Create or Modify a Normalization Rule Manually

Create or Modify a Normalization Rule Manually

See Also

Deploying Enterprise Voice > Configuring Dial Plans > Defining Normalization Rules >

Topic Last Modified: *2012-09-22*

Complete the following steps if you want to create or modify a normalization rule manually. If you want to create or modify a normalization rule by using Build a Normalization Rule in Lync Server Control Panel, see Create or Modify a Normalization Rule by Using Build a Normalization Rule.

⊟To define a normalization rule manually

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. (Optional) Follow the steps in Create a Dial Plan or Modify a Dial Plan.
4. In **New Normalization Rule** or **Edit Normalization Rule**, type a name that describes the number pattern being normalized in **Name** (for example, name the normalization rule **5DigitExtension**).
5. (Optional) In **Description** field, type a description of the normalization rule (for example, "Translates 5-digit extensions").
6. In **Build a Normalization Rule**, click **Edit**.
7. Enter the following in **Type a Regular Expression**:
   - In **Match this pattern**, specify the pattern that you want to use to match the dialed phone number.
   - In **Translation rule**, specify a pattern for the format of translated E.164 phone numbers.

   For example, if you enter **^(\d{7})$** in **Match this pattern** and **+1425$1** in **Translation rule**, the rule normalizes 5550100 to +14255550100.
8. (Optional) If the normalization rule results in a phone number that is internal to your organization, select **Internal extension**.
9. (Optional) Enter a number to test the normalization rule and then click **Go**. The test results are displayed under **Enter a number to test**.

   > **Note:**
   >
   > You can save a normalization rule that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.
10. Click **OK** to save the normalization rule.
11. Click **OK** to save the dial plan.
12. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

   > **Note:**
   >
   > Whenever you create or change a normalization rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Normalization Rule by Using Build a Normalization Rule
Create a Dial Plan
Modify a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

1.4.3.5 Configuring Voice Policies, PSTN Usage Records, and Voice Routes

Configuring Voice Policies, PSTN Usage Records, and Voice Routes

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-10-10*

Voice policies, PSTN usage records, and voice routes are integrally related. You configure voice policies by selecting a set of calling features and then assigning the policy a set of PSTN usage records, which specify what rights are authorized for the users or groups who are assigned the voice policy. Voice routes are also assigned PSTN usage records, which serve to match routes with the users who are authorized to use them. That is, users can only place calls that use the routes for which they have a matching PSTN usage record.

The recommended workflow for a new Enterprise Voice deployment is to start by configuring a voice policy that includes the appropriate PSTN usage records, and then associate the appropriate routes to each PSTN usage record.

Note:

You can also create voice policies with *user* scope and assign them to individual users or groups.

For the detailed steps to perform each of these tasks, see the procedures in this section.

- Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges
- View PSTN Usage Records
- Configuring Voice Routes for Outbound Calls
- Exporting and Importing Voice Routing Configuration
- Publish Pending Changes to the Voice Routing Configuration
- Test Voice Routing

1.4.3.5.1 Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges

Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges

Deployment > Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes >

Topic Last Modified: *2012-10-10*

A *voice policy* enables a set of calling features and associates one or more PSTN usage records to define the calling features and permissions of users who are assigned the policy.

Voice policy scope can be either *Site* (which defines the default features and permissions for a network site) or *User* (which defines the features and permissions to be assigned on a per-user or group basis). Users not assigned to a voice policy will automatically be assigned to the global policy, which is the default voice policy that is installed with the product.

Note:
For details, see Voice Policies in the Planning documentation.

- Create a Voice Policy and Configure PSTN Usage Records
- Modify a Voice Policy and Configure PSTN Usage Records
- Configuring Voice Mail Escape

1.4.3.5.1.1 Create a Voice Policy and Configure PSTN Usage Records

Create a Voice Policy and Configure PSTN Usage Records

See Also

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges >

Topic Last Modified: *2012-11-01*

Follow these steps if you want to create a new voice policy. If you want to edit a voice policy, see Modify a Voice Policy and Configure PSTN Usage Records for the procedure.

Note:
Each voice policy must have at least one associated public switched telephone network (PSTN) usage record. To see a listing of all PSTN usage records available in your Enterprise Voice deployment and view their properties, see View PSTN Usage Records.

⊟To create a voice policy

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Voice Policy**.
4. On the **Voice Policy** page, click **New** and then select a scope for the new policy:
   - **Site policy** applies to an entire site, except any users or groups that are assigned to a user policy. If you select Site for a policy scope, choose the site from the **Select a Site** dialog box. If a voice policy has already been created for a site, the site does not appear in the **Select a Site** dialog box.
   - **User policy** can be applied to specified users or groups.
5. If the voice policy scope is User, enter a descriptive name for the policy in the **Name** field.

   Note:
   If the voice policy scope is Site, the **Name** field in **New Voice Policy** is prepopulated with the site name and cannot be changed.
6. (Optional) Enter additional descriptive information for the voice policy.
7. Select or clear the following check boxes to enable or disable each of the **Calling features** for this voice policy:
   - **Voice mail escape** prevents calls from being immediately routed to the user's mobile phone voice mail system when simultaneous ringing is configured and the phone is turned off, out of battery, or out of range.

     Note:
     This feature is only configurable through the Lync Server

Management Shell

- **Call forwarding** enables users to forward calls to other phones and client devices. Lync Server 2013 provides a significantly wider range of configuration options for call forwarding. For example, if an organization does not want to allow incoming calls to be forwarded externally to the PSTN, an administrator can apply a special voice policy to deploy this restriction. Enabled by default.
- **Delegation** enables users to specify other users to send and receive calls on their behalf. In Lync Server 2013, a delegate can configure simultaneous ringing that enables incoming calls to his or her manager to ring all of the delegate's simultaneous ringing targets. This provides the delegate with greater flexibility in responding to calls directed to the manager. Enabled by default.
- **Call transfer** enables users to transfer calls to other users. Enabled by default.
- **Call park** enables users to park calls on hold and then pick up the call from a different phone or client. Disabled by default.
- **Simultaneous ringing** enables incoming calls to ring on additional phones (for example, a mobile phone) or other endpoint devices. Lync Server 2013 provides a significantly wider range of configuration options for simultaneous ringing. Enabled by default.
- **Team call** enables users on a defined team to answer calls for other members of the team. Enabled by default.
- **PSTN re-route** enables calls made by users who are assigned this policy to other enterprise users to be rerouted on the public switched telephone network (PSTN) if the WAN is congested or unavailable. Enabled by default.
- **Bandwidth policy override** enables administrators to override call admission control policy decisions for a particular user. Disabled by default.

Note:

The policy will be overridden only for incoming calls to the user and not for outgoing calls that are placed by the user. After the session is established, the bandwidth consumption will be accurately recorded. This setting should be used sparingly and should be reserved for appropriate call admission control decisions.

- **Malicious call tracing** enables users to report malicious calls (such as bomb threats) by using the client UI, which in turn flags the calls in the call detail records (CDRs). Disabled by default.

8.To associate and configure PSTN usage records for this voice policy, do any of the following:

- To choose one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records that you want to associate with this voice policy, and then click **OK**.
- To remove a PSTN usage record from this voice policy, highlight the record and click **Remove**.
- To define a new PSTN usage record and associate it with this voice policy, do the following:

  8..a.Click **New**.

  8..b.In the **Name** field, enter a unique descriptive name for the record. For example, you may want to create a PSTN usage record named **Redmond** for full-time employees located in Redmond, and another named **RedmondTemps** for temporary employees.

  Note:

  The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

  8..c.Use any of the following methods to associate and configure routes for this PSTN usage record:

- To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
- To remove a route from the PSTN usage record, highlight the route, and then click **Remove**.
- To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
- To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.

8..d.Click **OK**.

- To edit a PSTN usage record that is already associated with this voice policy, do the following:

  8..a.Highlight the PSTN usage record that you want to edit, and then click **Show details**.

  8..b.Use any of the following methods to associate and configure routes for this PSTN usage record:

  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from this PSTN usage record, highlight the route, and then click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route and lick **Show details**. For details, see Modify a Voice Route.

  8..c.Click **OK**.

9.Arrange the PSTN usage records for optimum performance. To change a record’s position in the list, highlight the record name and click the up or down arrow.

> **Important:**
>
> The order in which PSTN usage records are listed in the voice policy is significant. Lync Server traverses the list from the top down. We recommend that you organize the list by frequency of use, for example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup.

10.To associate and configure PSTN usage records for call forwarding and simultaneous ringing in this voice policy, do any of the following:

- To use the same PSTN usage records for call forwarding and simultaneous ringing as this voice policy, select the option **Route using the call PSTN usages** from the drop-down menu.
- To allow call forwarding and simultaneous ringing to internal Lync users only, select the option **Route to internal Lync users only** from the drop-down menu. Calls will not be forwarded to external PSTN numbers.
- To specify different PSTN usage records for call forwarding and simultaneous ringing than used for this voice policy, select the option **Route using custom PSTN usages** from the drop-down menu. This option displays a control to select existing PSTN usage records or create new PSTN usage records specifically for call forwarding and simultaneous ringing.

  10..a.To choose one or more records from a list of PSTN usage records for call forwarding and simultaneous ringing, click **Select**. Highlight the records that you want to associate with this call forwarding and simultaneous ringing policy, and then click **OK**.

  10..b.To remove a PSTN usage record from this call forwarding and simultaneous ringing policy, highlight the record and click **Remove**.

  10..c.To define a new PSTN usage record and associate it with this call forwarding and simultaneous ringing policy, do the following:

  - Click **New**.

- In the **Name** field, enter a unique descriptive name for the record.

> **Note:**
> The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

- Use any of the following methods to associate and configure routes for this PSTN usage record:
  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from the PSTN usage record, highlight the route and click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.
- Click **OK**.

10..d.To edit a PSTN usage record that is already associated with this voice policy, do the following:

- Highlight the PSTN usage record you want to edit and click **Show details**.
- Use any of the following methods to associate and configure routes for this PSTN usage record:
  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from this PSTN usage record, highlight the route and click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.
- Click **OK**.

11.(Optional) Enter a number to test the voice policy and click **Go**. The test results are displayed under **Translated number to test**.

> **Note:**
> You can save a voice policy that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

12.Click **OK**.

13.On the **Voice Policy** page, click **Commit**, and then click **Commit all**.

> **Note:**
> Any time you create or modify a voice policy, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

14.(Optional) Voicemail Escape detects that a call was immediately answered by the user’s mobile phone voice mail, and disconnects the call to the mobile phone voice mail. This allows the call to continue to ring on the user’s other endpoints giving the user the opportunity to answer the call. For details on how to configure a voice mail policy, see Configuring Voice Mail Escape.

Tasks

Modify a Voice Policy and Configure PSTN Usage Records
View PSTN Usage Records
Create a Voice Route
Modify a Voice Route
Publish Pending Changes to the Voice Routing Configuration
Configuring Voice Mail Escape

Other Resources

Test Voice Routing

1.4.3.5.1.2 Modify a Voice Policy and Configure PSTN Usage Records

Modify a Voice Policy and Configure PSTN Usage Records

See Also

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges >

Topic Last Modified: *2012-11-01*

Follow these steps if you want to modify a voice policy. If you want to create a new voice policy, see Create a Voice Policy and Configure PSTN Usage Records for the procedure.

Note:
If a user is assigned to a voice policy has no associated public switched telephone network (PSTN) usage records, the user cannot place outbound calls. For a listing of all PSTN usage records available in your Enterprise Voice deployment and view their properties, see View PSTN Usage Records.

⊟To modify a voice policy

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Voice Policy**.
4. On the **Voice Policy** page, double-click a voice policy name.

   Note:
   The scope and name were set when the voice policy was created. They cannot be changed.
5. (Optional) In **Edit Voice Policy**, enter additional descriptive information for the voice policy.
6. Select or clear the following check boxes to enable or disable each of the **Calling features**:
   - **Voice mail escape** prevents calls from being immediately routed to the user's mobile phone voice mail system when simultaneous ringing is configured and the phone is turned off, out of battery, or out of range.

     Note:
     This feature is only configurable through the Lync Server Management Shell
   - **Call forwarding** enables users to forward calls to other phones and client devices. Lync Server 2013 provides a significantly wider range of configuration options for call forwarding. For example, if an organization does not want to allow incoming calls to be forwarded externally to the PSTN, an administrator can apply a special voice policy to deploy this

restriction. Enabled by default.

- **Delegation** enables users to specify other users to send and receive calls on their behalf. In Lync Server 2013, a delegate can configure simultaneous ringing that enables incoming calls to his or her manager to ring all of the delegate's simultaneous ringing targets. This provides the delegate with greater flexibility in responding to calls directed to the manager. Enabled by default.
- **Call transfer** enables users to transfer calls to other users. Enabled by default.
- **Call park** enables users to park calls on hold, and then pick up the call from a different phone or client. Disabled by default.
- **Simultaneous ringing** enables incoming calls to ring on additional phones (for example, a mobile phone) or other endpoint devices. Lync Server 2013 provides a significantly wider range of configuration options for simultaneous ringing. Enabled by default.
- **Team call** enables users on a defined team to answer calls for other members of the team. Enabled by default.
- **PSTN re-route** enables calls made by users who are assigned this policy to other enterprise users to be rerouted on the public switched telephone network (PSTN) if the WAN is congested or unavailable. Enabled by default.
- **Bandwidth policy override** enables administrators to override call admission control (CAC) policy decisions for a particular user. Disabled by default.

> **Note:**
>
> The policy will be overridden only for incoming calls to the user and not for outgoing calls that are placed by the user. After the session is established, the bandwidth consumption will be accurately recorded. This setting should be used sparingly.

- **Malicious call tracing** enables users to report malicious calls (such as bomb threats) using the client UI, which in turn flags the calls in the call detail records (CDRs). Disabled by default.

7.To associate and configure PSTN usage records for this voice policy, do any of the following:

- To choose one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records that you want to associate with this voice policy, and then click **OK**.
- To remove a PSTN usage record from this voice policy, highlight the record and click **Remove**.
- To define a new PSTN usage record and associate it with this voice policy, do the following:

  7..a.Click **New**.

  7..b.In the **Name** field, enter a unique descriptive name for the record. For example, you may want to create a PSTN usage record named **Redmond** for full-time employees located in Redmond, and another record named **RedmondTemps** for temporary employees.

  > **Note:**
  >
  > The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

  7..c.Use any of the following methods to associate and configure routes for this PSTN usage record:

  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from the PSTN usage record, highlight the route and click **Remove**.
  - To define a new route and associate it with this PSTN usage record,

click **New**. For details, see Create a Voice Route.

- To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.

7..d.Click **OK**.

- To edit a PSTN usage record that is already associated with this voice policy, do the following:

7..a.Highlight the PSTN usage record that you want to edit and click **Show details**.

7..b.Use any of the following methods to associate and configure routes for this PSTN usage record:

- To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
- To remove a route from this PSTN usage record, highlight the route and click **Remove**.
- To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
- To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.

7..c.Click **OK**.

8.Arrange the PSTN usage records for optimum performance. To change a record’s position in the list, highlight the record name and click the up or down arrow.

Note:

The order in which PSTN usage records are listed in the voice policy is significant. Lync Server traverses the list from the top down. We recommend that you organize the list by frequency of use, for example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup.

9.To associate and configure PSTN usage records for call forwarding and simultaneous ringing in this voice policy, do any of the following:

- To use the same PSTN usage records for call forwarding and simultaneous ringing as this voice policy, select the option **Route using the call PSTN usages** from the drop-down menu.
- To allow call forwarding and simultaneous ringing to internal Lync users only, select **Route to internal Lync users only** from the drop-down menu. Calls will not be forwarded to external PSTN numbers.
- To specify different PSTN usage records for call forwarding and simultaneous ringing than those used for this voice policy, select the option **Route using custom PSTN usages** from the drop-down menu. This option displays a control to select existing PSTN usage records or to create new PSTN usage records, specifically for call forwarding and simultaneous ringing.

9..a.To choose one or more records from a list of PSTN usage records for call forwarding and simultaneous ringing, click **Select**. Highlight the records that you want to associate with this call forwarding and simultaneous ringing policy, and then click **OK**.

9..b.To remove a PSTN usage record from this call forwarding and simultaneous ringing policy, highlight the record and click **Remove**.

9..c.To define a new PSTN usage record and associate it with this call forwarding and simultaneous ringing policy, do the following:

- Click **New**.
- In the **Name** field, enter a unique descriptive name for the record.

Note:

The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

- Use any of the following methods to associate and configure routes for this PSTN usage record:
  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from the PSTN usage record, highlight the route and click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route, and then click **Show details**. For details, see Modify a Voice Route.
- Click **OK**.

9..d.To edit a PSTN usage record that is already associated with this voice policy, do the following:

- Highlight the PSTN usage record that you want to edit and click **Show details**.
- Use any of the following methods to associate and configure routes for this PSTN usage record:
  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from this PSTN usage record, highlight the route and click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.
- Click **OK**.

10.(Optional) Enter a number to test the voice policy and click **Go**. The test results are displayed under **Translated number to test**.

> **Note:**
>
> You can save a voice policy that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

11.Click **OK**.

12.On the **Voice Policy** page, click **Commit**, and then click **Commit all**.

> **Note:**
>
> Whenever you create or modify a voice policy, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

13.(Optional) Voicemail Escape detects that a call was immediately answered by the user's mobile phone voice mail, and disconnects the call to the mobile phone voice mail. This allows the call to continue to ring on the user's other endpoints giving the user the opportunity to answer the call. For details about how to configure a voice mail policy, see Configuring Voice Mail Escape.

Tasks

Create a Voice Policy and Configure PSTN Usage Records
View PSTN Usage Records
Create a Voice Route
Modify a Voice Route
Publish Pending Changes to the Voice Routing Configuration

Configuring Voice Mail Escape

Other Resources

Test Voice Routing

1.4.3.5.1.3 Configuring Voice Mail Escape

Configuring Voice Mail Escape

See Also Example

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges >

Topic Last Modified: *2013-02-22*

When a user configures simultaneous ringing to a mobile phone, a caller will typically be routed to the user’s personal voice mail if the mobile phone is turned off, out of battery power, or out of range. With Lync Server 2013, users can opt to have business-related calls routed to their corporate voice mail system. Specifically, a timer can be configured, and if the call is answered by the carrier’s voice mail within the range of time defined, Lync Server will disconnect from the carrier’s voice mail system (and the user’s personal voice mail), while the user’s remaining endpoints in the corporate system continue to ring. This way, the caller is automatically routed to the user’s corporate voice mail.

This configuration is performed using the Lync Server Management Shell cmdlet, **Set-CsVoicePolicy**, at the voice policy level, with the following parameters.

To configure voice mail escape

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Specify the following parameters to **Set-CsVoicePolicy**:
   - **EnableVoicemailEscapeTimer** - Enables or disables the escape timer.
   - **PSTNVoicemailEscapeTimer** - Specifies the timeout value in milliseconds. The default value is 1500 milliseconds, and the value can range from 0 milliseconds to 8000 milliseconds.

```
Set-CsVoicePolicy UserVoicePolicy -EnableVoiceMailEscapeTimer $true - PSTNVoicema
Set-CsVoicePolicy -Identity site:SitePolicy -EnableVoiceMailEscapeTimer $true -PS
```

See Also

Other Resources

Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges

1.4.3.5.2 View PSTN Usage Records

View PSTN Usage Records

See Also

Deployment > Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes >

Topic Last Modified: *2013-02-22*

A public switched telephone network (PSTN) usage record specifies a class of call (such as internal, local, or long distance) that can be made by various users or groups of users in an organization. For details, see PSTN Usage Records in the Planning documentation.

To view a PSTN usage record by using Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **PSTN Usage**.
4. On the **PSTN Usage** page, highlight the PSTN usage record you want to view, click **Edit** and then click **Show details**.

Note:
A read-only page of the selected PSTN usage record shows the associated routes and associated voice policies.

Viewing PSTN Usage Information by Using Windows PowerShell Cmdlets

You can also view PSTN usages by using Windows PowerShell and the **Get-CsPstnUsage** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view PSTN usage information by using Windows PowerShell cmdlets

- To view information about all of your PSTN usages, type the following command in the Lync Server Management Shell, and then press ENTER:

```
Get-CsPstnUsage
```

This command returns information similar to the following:

```
Identity : Global
Usage    : {Internal, Local, Long Distance}
```

For details, see Get-CsPstnUsage.

See Also

Tasks

Create a Voice Policy and Configure PSTN Usage Records
Modify a Voice Policy and Configure PSTN Usage Records

1.4.3.5.3 Configuring Voice Routes for Outbound Calls

Configuring Voice Routes for Outbound Calls

See Also

Deployment > Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes >

Topic Last Modified: *2012-11-01*

A Lync Server 2013 voice route associates destination phone numbers with one or more public switched telephone network (PSTN) gateways or SIP trunks and one or more PSTN usage records.

To view voice routes by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. Click **Voice Routing**.
3. Click **Route**.
4. Double-click a voice route to view additional properties from the list of voice routes, or select the route and click **Edit**. Then click **Show details**.

> **Note:**
> You can only view detailed information for a single route at a time.

To view voice routes by using Windows PowerShell

- Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**. Voice routes can be viewed by using Windows PowerShell and the **Get-CsVoiceRoute** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.
  To view information about all of your voice routes, type the following command in the Lync Server Management Shell, and then press ENTER:

```
Get-CsVoiceRoute
```

  That will return information similar to this:

```
Identity           : global
Priority           : -1
Description        :
NumberPattern      : ^(\+1[0-9]{10})$
PstnUsages         : {}
PstnGatewayList    : {}
Name               : global
SuppressCallerId   :
AlternateCallerId  :
```

> **Note:**
> For details, see Voice Routes in the Planning documentation.

- Create a Voice Route
- Modify a Voice Route

⊟See Also

Other Resources

Managing Voice Routing

1.4.3.5.3.1 Create a Voice Route

Create a Voice Route

See Also

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Routes for Outbound Calls >

Topic Last Modified: *2012-11-01*

The following procedure explains how to create a new voice route by using the Lync Server 2013 Control Panel. To edit an existing route, see Modify a Voice Route for the procedure.

⊟To create a voice route by using the Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **CsVoiceAdministrator**, **CsServerAdministrator**, or **CsAdministrator** administrative role.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.
4. Click **Route**.
5. Click **New** to display the **New Voice Route** dialog box.
6. In **Name**, type a descriptive name for the voice route.
7. (Optional) In **Description**, type additional descriptive information for the voice route.
8. To specify the patterns that you want this route to accommodate, you can either use the **Build a pattern to match** tool to generate a regular expression, or write the regular expression manually.
   - To use the **Build a pattern to match** tool to generate a regular expression, enter values as follows. You can specify two types of pattern matching:
     - **Starting digits for numbers that you want to allow:** Enter prefix values that this route must accommodate (including the leading + if needed). For example, type **+425**, and then click **Add**. Repeat this for each prefix value that you want to include in the route.
     - **Exceptions:** If you want to specify one or more exceptions for a prefix value, highlight the prefix and click **Exceptions**. Type in one or more values for the matching patterns that you do *not* want this route to accommodate. For example, to exclude numbers starting with +425237 from the route, enter a value of **+425237** in the **Exceptions** field, and then click **OK**.
   - To define the matching pattern manually, click **Edit** in the **Build a pattern to match** tool and then type in a .NET Framework regular expression to specify the matching pattern for destination phone numbers to which the route is applied. For details about how to write regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.
9. Select **Suppress caller ID** if you do not want the ID of the phone making the outbound call to appear to the call recipient. If you select this option, you must specify an **Alternate caller ID** that will appear on the recipient's caller ID display.
10. To associate one or more trunks with the voice route, click **Add** and then select a trunk from the list.

Note:
If your deployment includes any Microsoft Office Communications Server 2007 R2 Mediation Servers, they will also be available in the list.

11. To associate one or more public switched telephone network (PSTN) usages with the voice route, click **Select** and choose a record from the list of PSTN usage records that have been defined for your Enterprise Voice deployment.

Note:
To view the properties of each of the available PSTN usage records, see View PSTN Usage Records. To create or edit PSTN usage records, see Create a Voice Policy and Configure PSTN Usage Records or Modify a Voice Policy and Configure PSTN Usage Records.

12. Arrange the PSTN usage records for optimum performance. To change a record's position in the list, highlight the record name and click the up or down arrow.

Note:
In contrast to a voice policy, where the order in which PSTN usage records are listed is important, the order in which PSTN usage records are listed in the voice route is insignificant. However, we recommend that you organize the list by frequency of use. For example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup. (Lync Server traverses the list from the top down.)

13. (Optional) Type a value into the **Enter a translated number to test** field and click **Go**. The test results are displayed under the field.

Note:
You can save a voice route that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

14. Click **OK** to save the voice route.

Important:
Whenever you create a voice route, you must run the **Commit All** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration.

Tasks

Modify a Voice Route
View PSTN Usage Records
Create a Voice Policy and Configure PSTN Usage Records
Modify a Voice Policy and Configure PSTN Usage Records
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

1.4.3.5.3.2 Modify a Voice Route

Modify a Voice Route

See Also

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Routes for Outbound Calls >

Topic Last Modified: *2012-11-01*

This topic explains how to edit a voice route. To create a new route, see Create a Voice Route.

To modify a voice route

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Route**.
4. On the **Route** page, use either of the following methods to modify a voice route:
   - Click a voice route name, click **Edit**, and then click **Show details**.
   - Click a voice route name, click **Edit**, click **Copy**, and then click **Paste**. Click the new copy of the voice route that you just created, click **Edit**, and then click **Show details**.
5. In the **Name** field on the **Edit Voice Route** page, type a descriptive name for the voice route.
6. (Optional) In the **Description** field, type in additional descriptive information

for the voice route.

7. To specify the patterns you want this route to accommodate, you can either use the **Build a pattern to match** tool to generate a regular expression, or write the regular expression manually.
   - To use the **Build a pattern to match** tool to generate a regular expression, enter values as follows. You can specify two types of pattern matching:
     - **Starting digits for numbers that you want to allow:** Enter prefix values that this route must accommodate (including the leading + if needed). For example, type **+425** and then click **Add**. Repeat this for each prefix value that you want to include in the route.
     - **Exceptions:** If you want to specify one or more exceptions for a prefix value, highlight the prefix and click **Exceptions**. Type in one or more values for the matching patterns that you do *not* want this route to accommodate. For example, to exclude numbers starting with +425237 from the route, enter a value of **+425237** in the **Exceptions** field, and then click **OK**.
   - To define the matching pattern manually, click **Edit** in the **Build a pattern to match** tool and then type in a .NET Framework regular expression to specify the matching pattern for destination phone numbers to which the route is applied. For information about how to write regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.
8. Select **Suppress caller ID** if you do not want the ID of the phone that is making the outbound call to appear to the call recipient. If you select this option, you must specify an **Alternate caller ID** that will appear on the recipient’s caller ID display.
9. To associate one or more public switched telephone network (PSTN) trunks with the voice route, click **Add**, and then select a trunk from the list.

   > **Note:**
   >
   > If your deployment includes any Microsoft Office Communications Server 2007 R2 Mediation Servers, they will also be available in the list.

10. To associate one or more PSTN usages with the voice route, click **Select** and choose a record from the list of PSTN usage records that have been defined for your Enterprise Voice deployment.

    > **Note:**
    >
    > To view the properties of each of the available PSTN usage records, see View PSTN Usage Records.
    >
    > To create or edit PSTN usage records, see Create a Voice Policy and Configure PSTN Usage Records or Modify a Voice Policy and Configure PSTN Usage Records.

11. Arrange the PSTN usage records for optimum performance. To change a record’s position in the list, highlight the record name and click the up or down arrow.

    > **Note:**
    >
    > In contrast to a voice policy where the order in which PSTN usage records are listed is important, the order of PSTN usage records in a voice route is insignificant. However, we recommend that you organize the list by frequency of use, for example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup. (Lync Server traverses the list from the top down.)

12. (Optional) Type a value into the **Enter a translated number to test** field and click **Go**. The test results are displayed under the field.

    > **Note:**
    >
    > You can save a voice route that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

13. Click **OK**.

14.On the **Route** page, click **Commit**, and then click **Commit all**.

Note:
Whenever you create or modify a voice route, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create a Voice Route
View PSTN Usage Records
Create a Voice Policy and Configure PSTN Usage Records
Modify a Voice Policy and Configure PSTN Usage Records
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

1.4.3.6 Exporting and Importing Voice Routing Configuration

Exporting and Importing Voice Routing Configuration

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-11-01*

If you want to save your voice routing configuration without publishing it, follow these steps to use the Lync Server Control Panel configuration export and import commands to save and retrieve a snapshot of your voice routing configuration. When you import a voice routing configuration file (.vcfg), but changes have been made to the voice routing configuration on the server in the meantime, the pages in the **Voice Routing** group in Lync Server Control Panel will indicate that there are uncommitted changes to voice routing. Those uncommitted changes are the differences between the two configurations that require reconciliation.

Important:
If you have made any uncommitted changes to the settings on any page within the **Voice Routing** group, the changes are saved in the exported voice configuration file (.vcfg). This enables you to make voice routing configuration changes during multiple Lync Server Control Panel sessions before you publish the changes.

- Export a Voice Route Configuration File
- Import a Voice Route Configuration File

⊟Related Sections

1.4.3.6.1 Export a Voice Route Configuration File

Export a Voice Route Configuration File

See Also

Deployment > Deploying Enterprise Voice > Exporting and Importing Voice Routing Configuration >

Topic Last Modified: *2012-11-01*

If you want to save your voice routing configuration without publishing it, follow these steps to use the Lync Server Control Panel configuration export and import commands to save and retrieve a snapshot of your voice routing configuration. When you import a voice routing configuration file (.vcfg), but changes have been made to the voice routing configuration on the server in the meantime, the pages in the **Voice Routing** group in Lync Server Control Panel will indicate that there are uncommitted changes to voice routing. Those uncommitted changes are the differences between the two configurations that require reconciliation.

If you have made any uncommitted changes to the settings on any page within the group, the changes are saved in the exported voice configuration file (.vcfg). This enables you to make voice routing configuration changes during multiple sessions before you publish the changes.

⊟To export a voice routing configuration

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.
4. On the **Actions** menu, click **Export configuration**.
5. Specify a location and file name, and then click **Save**.

Tasks

Import a Voice Route Configuration File

1.4.3.6.2 Import a Voice Route Configuration File

Import a Voice Route Configuration File

See Also

Deployment > Deploying Enterprise Voice > Exporting and Importing Voice Routing Configuration >

Topic Last Modified: *2012-11-01*

If you want to save your voice routing configuration without publishing it, follow these steps to use the Lync Server Control Panel configuration export and import commands to save and retrieve a snapshot of your voice routing configuration. When you import a voice routing configuration file (.vcfg), but changes have been made to the voice routing configuration on the server in the meantime, the pages in the **Voice Routing** group in Lync Server Control Panel will indicate that there are uncommitted changes to voice routing. Those uncommitted changes are the differences between the two configurations that require reconciliation.

If you have made any uncommitted changes to the settings on any page within the group, the changes are saved in the exported voice configuration file (.vcfg). This enables you to make voice routing configuration changes during multiple sessions before you publish the changes.

⊟To import a voice routing configuration

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.

4. On the **Actions** menu, click **Import configuration**.
5. Find the configuration file you want to import and then click **Open**.
6. Click **Commit**, and then click **Commit all**.

Note:
Whenever you import a voice configuration file, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Export a Voice Route Configuration File
Publish Pending Changes to the Voice Routing Configuration

1.4.3.7 Test Voice Routing

Test Voice Routing

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2013-02-24*

You can use the Lync Server Control Panel **Test Voice Routing** tab to configure test case scenarios. To define a test case, you specify the dial plan, voice policy, PSTN usage, and voice route against which to test a specified phone number.

Before you actually deploy your voice routing configuration, we recommend that you test it on various phone numbers to make sure that the results are what you're expecting.

Tip:
You can use the **Export test cases** and **Import test cases** commands to save voice routing test cases and import them for use on another computer.

Caution:
If you delete any part of your voice routing configuration, such as a dial plan, voice policy, voice route, or phone usage, you should review and update your voice routing test cases. The Lync Server Control Panel will not alert you to test cases that are no longer valid due to changed configurations.

- Create a Voice Routing Test Case
- Export Voice Routing Test Cases
- Import Voice Routing Test Cases
- Running Voice Routing Tests

1.4.3.7.1 Create a Voice Routing Test Case

Create a Voice Routing Test Case

See Also

Deployment > Deploying Enterprise Voice > Test Voice Routing >

Topic Last Modified: *2012-10-10*

To create a test case

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to

start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Voice Routing** and then click **Test Voice Routing**.
4. On the **Test Voice Routing** page, click **New** to create a new test case.
5. In **Name**, type in a unique name for the test case.

   The name must be unique among all voice routing test cases in your Enterprise Voice deployment. It can be up to 32 characters in length and may contain any alphanumeric characters, in addition to the backslash (\), period (.), or underscore (_).
6. In **Dialed number to test**, type in the dialed number that you want to use to test the routing configuration that you specify for this test case. Based on the dial plan, route, and voice policy, this number will be normalized and displayed as output.
7. In the **Dial Plan** list, select the dial plan to use when running the test. Default is the Global dial plan.
8. In the **Voice Policy** list, select the voice policy to use when running the test. Default is the Global voice policy.
9. In **Expected translation**, type in the phone number in the format you expect to see it after translation. This is the value of the phone number that you are testing after it has been translated by the first normalization rule that matches in the selected dial plan. When you run the test case, if the number you are testing does not result in the value in **Expected translation**, the test fails.
10. (Optional) In the **Expected PSTN usage** list, you can select the public switched telephone network (PSTN) usage record that you expect to be used when you run the test case, based on the specified dial plan and voice policy. If a different PSTN usage record is used, the test fails.
11. (Optional) In the **Expected route** list, you can select the voice route that you expect to be used when you run the test case, based on the specified dial plan and voice policy. If a different voice route is used, the test fails.
12. (Optional) Click **Run** to run the test case. The results are shown in the right panel of the page.
13. Click **OK**.
14. Click **Commit**, and then click **Commit all**.

> **Note:**
>
> Whenever you create a voice routing test case, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Export Voice Routing Test Cases
Import Voice Routing Test Cases

Other Resources

Configuring Dial Plans
Configuring Voice Policies, PSTN Usage Records, and Voice Routes

1.4.3.7.2 Export Voice Routing Test Cases

Export Voice Routing Test Cases

See Also

Deployment > Deploying Enterprise Voice > Test Voice Routing >

Topic Last Modified: *2012-11-01*

Test cases provide a way for you to test voice routes in your organization: you define such things as the number to be dialed and the dial plan and voice policy to be employed, and Lync Server can then verify that that, given those conditions, the supplied number can successfully be routed to the PSTN network.

Test cases, which can be created by using Lync Server Control Panel, are typically saved only on the server where the case was originally created and run. However, these test cases can be exported as XML files (with the .vtest extension) and then imported on other servers. This enables you to run the same tests on different computers located at different points in your topology.

⊟To export a voice routing test case

1. In Lync Server Control Panel, click **Voice Routing** and then click **Test Voice Routing**.
2. On the **Test Voice Routing** tab, select the test case (or test cases) to be exported. To select multiple test cases, click the first case to be exported, then hold down the Ctrl key and select the additional cases to be exported.
3. Click **Action**, then click **Export test cases**.
4. In the **Save As** dialog box, select a folder to store the exported test cases and type a name for the resulting XML file in the **File name** box. Note that if you are exporting multiple tests cases all of these test cases will be saved to a single XML file.
5. To save the test cases, click **Save**.

Tasks

Import Voice Routing Test Cases

1.4.3.7.3 Import Voice Routing Test Cases

Import Voice Routing Test Cases

See Also

Deployment > Deploying Enterprise Voice > Test Voice Routing >

Topic Last Modified: *2013-02-21*

Test cases provide a way for you to test voice routes in your organization: you define such things as the number to be dialed and the dial plan and voice policy to be employed, and Lync Server 2013 can then verify that that, given those conditions, the supplied number can successfully be routed to the PSTN network.

Test cases, which can be created by using Lync Server Control Panel, are typically saved only on the server where the case was originally created and run. However, these test cases can be exported as XML files (with the .vtest extension) and then imported on other servers. This enables you to run the same tests on different computers located at different points in your topology.

⊟To import a voice routing test case

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.
4. On the **Actions** menu, click **Import test cases**.
5. Find the test case file (.vtest) that you want to import, and then click **Open**.
6. Click **Commit**, and then click **Commit all**.

Note:
Whenever you import a .vtest file, you must run the **Commit all** command to publish the test case. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Export Voice Routing Test Cases

1.4.3.7.4 Running Voice Routing Tests

Running Voice Routing Tests

Deployment > Deploying Enterprise Voice > Test Voice Routing >

Topic Last Modified: *2013-02-21*

Lync Server 2013 provides two different methods for testing voice routes: you can do informal, ad hoc testing against any phone number and any voice route; or you can do more formal testing using voice route test cases. With formal testing, you define such things as the number to be dialed and the dial plan and voice policy to be employed, and Lync Server can then verify that that, given those conditions, the supplied number can successfully be routed to the PSTN network. Both of these methods are described in subsequent sections of this documentation.

- Run Informal Voice Routing Tests
- Run Voice Routing Test Cases

1.4.3.7.4.1 Run Informal Voice Routing Tests

Run Informal Voice Routing Tests

See Also

Deploying Enterprise Voice > Test Voice Routing > Running Voice Routing Tests >

Topic Last Modified: *2012-08-07*

You can use the **Create voice routing test case information** dialog box to run informal tests before creating an actual test case. When you are satisfied with the outcome of a test, you have the option of saving it as a formal test case.

⊟To run an informal voice routing test

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Test Voice Routing**.
4. On the **Test Voice Routing** page, click **Create voice routing test case information**.
5. In the **Dialed number** field, type in the phone number you want to use for this test. This number will be normalized and displayed in the **Normalized number** field of the **Results** pane.
6. In the **Dial plan** list, select the dial plan to use for testing the dialed number. Default is the Global dial plan.

   When you run the test, the first normalization rule in this dial plan that matches the dialed number will be displayed in the **Normalization rule** field of the **Results** pane.

7.In the **Voice Policy** list, select the voice policy to use for testing the dialed number. Default is the Global voice policy.

When you run the test, the first matching PSTN usage record in this voice policy will be displayed in the **First PSTN usage** field of the **Results** pane. Also, the first matching voice route that is associated with this PSTN usage record will be displayed in the **First route** field.

8.(Optional) Select the **Populate from user** check box if you want to test the dialed number against the voice policy assigned to a particular user.

8.a.Click **Browse** to display the **Select Enterprise Voice Users** dialog box.

8.b.Click **Find** to display the list of users who are enabled for Enterprise Voice.

8.c.Double-click the user name whose assigned voice policy you want to use for this test. The **Policy** field is now populated with the voice policy assigned to the selected user.

When you run the test, the first matching public switched telephone network (PSTN) usage record in this voice policy will be displayed in the **First PSTN usage** field of the **Results** pane. Also, the first matching voice route that is associated with this PSTN usage record will be displayed in the **First route** field.

9.Click **Run** to run the test case. The results are shown in the right panel of the dialog box.

10.(Optional) Click **Save as** if you want to save this test configuration as a formal test case.

10.a.In the **Name** field of the **Save Voice Routing Test Case Information** dialog box, type a unique name for the test case.

The name must be unique among all voice routing test cases in your Enterprise Voice deployment. It can be up to 32 characters in length and may contain any alphanumeric characters, in addition to the backslash (\), period (.), or underscore (_).

10.b.Note that the remaining fields on the **Save Voice Routing Test Case Information** dialog box are read-only, and are prepopulated from the informal test configuration *and* results. Verify that this is the configuration that you want to save for the test case.

> **Note:**
>
> Values from the test results are used to prepopulate fields on the **Save Voice Routing Test Case Information** dialog box as follows:
>
> - **Expected translation** is prepopulated with the value in the **Normalized number** field.
> - **Expected route** is prepopulated with the value in the **First route** field.
> - **Expected PSTN usage record** is prepopulated with the value in the **First PSTN usage** field.
>
> If matches for any of these values were not found during the test run, the corresponding field is empty on the **Save Voice Routing Test Case Information** dialog box.

1.a.Click **Ok** to save the test case, or click **Cancel** to return to return to the **View voice routing test case information** dialog box to further develop the test before saving it.

2.Click **Commit**, and then click **Commit all**.

> **Note:**
>
> Whenever you create a voice routing test case, you must run the **Commit all** command to publish the test case. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create a Voice Routing Test Case
Run Voice Routing Test Cases
Export Voice Routing Test Cases
Import Voice Routing Test Cases

Other Resources

Configuring Dial Plans
Configuring Voice Policies, PSTN Usage Records, and Voice Routes

1.4.3.7.4.2 Run Voice Routing Test Cases

Run Voice Routing Test Cases

See Also

Deploying Enterprise Voice > Test Voice Routing > Running Voice Routing Tests >

Topic Last Modified: *2013-02-24*

You can run all of the test cases in your voice routing test case suite, or you can run one or more selected test cases.

⊟To run all voice routing test cases

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Test Voice Routing**.
4. On the **Test Voice Routing** page, click **Action** and then click **Run all**.

   The pass or fail status of each test case is shown in the **Pass/fail** column. If a test case has not yet been run, N/A is shown in the **Pass/fail** column.
5. (Optional) To see detailed results for each test case, double-click the test case name. Results are shown in the shaded area on the right side of the **Edit Test Case** page:

   5.a. **Test result:** Overall pass or fail status of the test case run.

   5.b. **Normalization rule:** The first normalization rule in the dial plan selected for this test case that matches the dialed number (the value in the **Number to test** field).

   5.c. **Normalized number:** The value of the dialed number after the normalization rule has translated it.

   5.d. **First PSTN usage:** The first public switched telephone network (PSTN) usage record in the voice policy selected for this test case that matches the dialed number.

   5.e. **First route:** The first voice route in the first PSTN usage record that matches the dialed number.

> **Note:**
> The **Expected PSTN usage record** and **Expected route** fields are optional in voice routing test case configuration. If the test case does not specify these values, the corresponding field in the test results will be empty.

⊟To run one or more selected voice routing test cases

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync

Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Voice Routing**, and then click **Test Voice Routing**.
4. On the **Test Voice Routing** page, click the names of the test cases that you want to run.
5. On the **Action** menu, click **Run selected**.

   The pass or fail status of each test case is shown in the **Pass/fail** column. If a test case has not yet been run, N/A is shown in the **Pass/fail** column.
6. (Optional) To see detailed results for each test case, double-click the test case name. Results are shown in the shaded area on the right side of the **Edit Test Case** page:
   - 6.a. **Test result:** Overall pass or fail status of the test case run.
   - 6.b. **Normalization rule:** The first normalization rule in the dial plan selected for this test case that matches the dialed number (the value in the **Number to test** field).
   - 6.c. **Normalized number:** The value of the dialed number after the normalization rule has translated it.
   - 6.d. **First PSTN usage:** The first PSTN usage record in the voice policy selected for this test case that matches the dialed number.
   - 6.e. **First route:** The first voice route in the first PSTN usage record that matches the dialed number.

> **Note:**
> The **Expected PSTN usage record** and **Expected route** fields are optional in voice routing test case configuration. If the test case does not specify these values, the corresponding field in the test results will be empty.

Other Resources

Test Voice Routing
Running Voice Routing Tests

1.4.3.8 Publish Pending Changes to the Voice Routing Configuration

Publish Pending Changes to the Voice Routing Configuration

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-08-07*

After you make changes to any of the configuration settings in pages in the **Voice Routing** group, perform this procedure to review, publish, or cancel the pending changes.

> **Important:**
> Be sure that only one user at a time modifies the Voice Routing configuration settings. All pending changes must be published at the same time by running the **Commit all** command. You cannot selectively publish pending changes. Before you publish pending changes, run the **Review uncommitted changes** command and cancel any configuration changes that you do not want to publish.
> If you navigate away from the pages in the **Voice Routing** group before committing pending changes, all pending changes will be lost. However, you can export the current configuration (including any pending changes) to a voice configuration file, and then import and publish the updated configuration. For details, see Export a Voice Route Configuration File.

⊟To review, publish, or cancel voice routing configuration changes

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator,

or CsAdministrator role. For details, see Delegate Setup Permissions.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.
4. Make the configuration changes you want to the settings on each page of the **Voice Routing** group.
5. To review pending changes without publishing them, select **Review uncommitted changes** from the **Commit** menu.
6. If you want to cancel any of the pending changes, do one of the following:
   - Select **Cancel all uncommitted changes** from the **Commit** menu.
   - Navigate to the tab of the **Voice Routing** page that has pending changes you want to cancel, select the item with the pending changes, click **Commit**, and then click **Cancel selected changes**.
7. After you have reviewed all pending changes and canceled any that you do not want to publish, click **Commit**, and then click **Commit all**.
8. In the **Uncommitted Voice Configuration Settings** dialog box, which displays a list of all of the pending changes, click **OK**.

   When Lync Server Control Panel has committed the changes, the **Successfully published voice routing configuration** message appears.

1.4.3.9 Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail

Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-09-26*

If you have deployed or plan to deploy Microsoft Exchange Server in your organization, you can use Exchange Unified Messaging (UM) features to provide voice mail to Enterprise Voice users.

In This Section

- Configuring Unified Messaging on Microsoft Exchange Server to Work with Lync Server 2013
- Configure Lync Server 2013 to Work with Unified Messaging on Microsoft Exchange Server

1.4.3.9.1 Configuring Unified Messaging on Microsoft Exchange Server to Work with Lync Server 2013

Configuring Unified Messaging on Microsoft Exchange Server to Work with Lync Server 2013

Deployment > Deploying Enterprise Voice > Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail >

Topic Last Modified: *2012-10-11*

Important:

If you want to use Exchange Unified Messaging (UM) to provide call answering, Outlook Voice Access, or auto-attendant services for Enterprise Voice users, read Planning for Exchange Unified Messaging Integration in the Planning documentation, and then follow the instructions in this section.

To configure Exchange Unified Messaging (UM) to work with Enterprise Voice, you'll need to perform the following tasks:

- Configure certificates on the server running Exchange Unified Messaging (UM) services

  > **Note:**
  > Add all Client Access and Mailbox servers to all UM SIP URI dial plans. If not, outbound call routing won't work as expected.

- Create one or more UM SIP URI dial plans, along with the subscriber access phone numbers, as needed, and then create corresponding Lync Server dial plans.
- Use the **exchucutil.ps1** script to:
  - Create UM IP gateways.
  - Create UM hunt groups.
  - Grant Lync Server 2013 permission to read UM Active Directory Domain Services (AD DS) objects.
- Create a UM auto-attendant object.
- Create a subscriber access object.
- Create a SIP URI for each user and associating users with a UM SIP URI dial plan.

Requirements and Recommendations

Before you begin, the documentation in this section assumes that you have deployed the following Exchange 2013 roles: Client Access and Mailbox. In Microsoft Exchange Server 2013, Exchange UM runs as a service on these servers.

For details about deploying Exchange 2013, see the Exchange 2013 TechNet Library at http://go.microsoft.com/fwlink/p/?LinkId=266637

Also note the following:

- If Exchange UM is installed in multiple forests, the Exchange Server integration steps must be performed for each UM forest. In addition, each UM forest must be configured to trust the forest in which Lync Server 2013 is deployed, and the forest in which Lync Server 2013 is deployed must be configured to trust each UM forest.
- Integration steps are performed on both the Exchange Server roles where Unified Messaging services are running, and on the server running Lync Server 2013. You should perform the Exchange Server Unified Messaging integration steps before you perform the Lync Server 2013 integration steps.

  > **Note:**
  > To see which integration steps are performed on which servers and by which administrator roles, see Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013.

The following tools must be available on each server running Exchange UM:

- Exchange Management Shell
- The script **exchucutil.ps1**, which performs the following tasks:
  - Creates a UM IP gateway for each Lync Server 2013.
  - Creates a hunt group for each gateway. The pilot identifier of each hunt group specifies the UM SIP URI dial plan used by the Front End pool or Standard Edition server that is associated with the gateway.
  - Grants Lync Server 2013 permission to read Exchange UM objects in Active Directory Domain Services (AD DS).

In This Section

1.4.3.9.1.1 Configure Certificates on the Server Running Microsoft Exchange Server Unified Messaging

Configure Certificates on the Server Running Microsoft Exchange Server Unified Messaging

Deploying Enterprise Voice > Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail > Configuring Unified Messaging on Microsoft Exchange Server to Work with Lync Server 2013 >

Topic Last Modified: *2012-09-26*

If you have deployed Exchange Unified Messaging (UM), as described in Planning for Exchange Unified Messaging Integration in the Planning documentation, and you want to provide Exchange UM features to Enterprise Voice users in your organization, you can use the following procedures to configure the certificate on the server running Exchange UM.

Important:
For internal certificates, both the servers running Lync Server 2013 and the servers running Microsoft Exchange must have trusted root authority certificates that are mutually trusted. The certification authority (CA) can either be the same, or a different certification authority, as long as the servers have the certification authority’s root certificate registered in their trusted root authority certificate store.

The Exchange Server must be configured with a server certificate in order to connect to Lync Server 2013:

1. Download the CA certificate for the Exchange Server.
2. Install the CA certificate for the Exchange Server.
3. Verify that the CA is in the list of trusted root CAs of the Exchange Server.
4. Create a certificate request for the Exchange Server and install the certificate.
5. Assign the certificate for the Exchange Server.

⊟To download the CA certificate

1. On the server running Exchange UM, click **Start**, click **Run**, type **http://<name of your Issuing CA Server>/certsrv**, and then click **OK**.
2. Under **Select a task**, click **Download a CA certificate, certificate chain, or CRL**.
3. Under **Download a CA Certificate, Certificate Chain, or CRL**, select **Encoding Method to Base 64**, and then click **Download CA certificate**.

Note:
You can also specify Distinguished Encoding Rules (DER) encoding at this step. If you select DER encoding, the file type in the next step of this procedure and in step 10 of **To Install the CA certificate** is .p7b rather than .cer.

4. In the **File Download** dialog box, click **Save**, and then save the file to the hard disk on the server. (The file will have either a .cer or a .p7b file extension, depending on the encoding that you selected in the previous step.)

⊟To install the CA certificate

1. On the server running Exchange UM, open Microsoft Management Console (MMC) by clicking **Start**, clicking **Run**, typing **mmc** in the **Open** box, and then clicking **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In the **Add Standalone Snap-ins** box, click **Certificates**, and then click **Add**.
4. In the **Certificate snap-in** dialog box, click **Computer account**, and then click **Next**.
5. In the **Select Computer** dialog box, verify that the **Local computer: (the computer this console is running on)** check box is selected, and then click **Finish**.
6. Click **Close**, and then click **OK**.
7. In the console tree, expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
8. Right-click **Certificates**, click **All Tasks**, and click **Import**.
9. Click **Next**.
10. Click **Browse** to locate the file, and then click **Next**. (The file will have either a .cer or a .p7b file extension, depending on the encoding that you selected in step 3 of **To download the CA certificate**.
11. Click **Place All Certificates in the following store**.
12. Click **Browse**, and then select **Trusted Root Certification Authorities**.
13. Click **Next** to verify the settings, and then click **Finish**.

⊟To verify that the CA is in the list of trusted root CAs

1. On the server running Exchange UM, in MMC expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
2. In the details pane, verify that your CA is on the list of trusted CAs.

⊟To configure Exchange Server 2013 UM with Lync Server

1. For details, see "Integrate Exchange 2013 UM with Lync Server" in the Exchange Server documentation at http://go.microsoft.com/fwlink/p/?LinkId=265372.

⊟To create a certificate request and install the certificate on Exchange Server 2007 (SP1)

1. On the server running Exchange UM, click **Start**, click **Run**, type **http://<***name of your Issuing CA Server***>/certsrv**, and then click **OK**.
2. Under **Select a task**, click **Request a Certificate**.
3. Under **Request a Certificate**, click **Advanced certificate request**.
4. Under **Advanced Certificate Request**, click **Create and submit a request to this CA**.
5. Under **Advanced Certificate Request**, select **Web server** or another server certificate template configured for server authentication.
6. Under **Identifying Information for Offline Template**, in the **Name** box, type the fully qualified domain name (FQDN) of the Exchange Server.

   Note:
   You must enter the FQDN of the Exchange Server for communications to work.

7. Under **Key Options**, click the **Store certificate in the local computer certificate store** check box.
8. Click the **Submit** button in the bottom of the webpage.
9. In the dialog box that opens asking for confirmation, click **Yes**.
10. On the Certificate Issued page, under **Certificate Issued**, click **Install this certificate**.
11. In the dialog box that opens asking for confirmation, click **Yes**.

12. Verify that the message "Your new certificate has been successfully installed" appears.

⊟To create a certificate on Exchange Server 2010

1. Log on to the server running Exchange UM with appropriate user rights. For details, see "Client Access Permissions" at http://go.microsoft.com/fwlink/p/?linkId=195499.
2. Refer to the following procedures to create the certificate:
   - 2.a. "Create a New Exchange Certificate" at http://go.microsoft.com/fwlink/p/?linkId=195494
   - 2.b. "Import an Exchange Certificate" at http://go.microsoft.com/fwlink/p/?linkId=195496

Note:
For the certificate **Subject Name**, you must enter the FQDN of the Exchange Server for communications to work.

⊟To assign the certificate on Exchange Server 2007 (SP1)

1. On the server running Exchange UM, open MMC.
2. In the console tree, expand **Personal** and then click **Certificates**.
3. In the details pane, verify that personal certificate is displayed.
4. Double-click the certificate to read its details and verify that it is valid.

Note:
It may take a few minutes before the certificate displays as valid.

5. Restart the Microsoft Exchange Unified Messaging service.

Note:
The server running Exchange Server 2007 SP1 Unified Messaging automatically retrieves the correct certificate.

6. Open Event Viewer and look for Event ID 1112, which specifies what certificate the server running Exchange Server 2007 SP1 Unified Messaging has retrieved.

⊟To assign the certificate on Exchange Server 2010

1. Log on to the server running Exchange UM with appropriate user rights. For details, see "Client Access Permissions" at http://go.microsoft.com/fwlink/p/?linkId=195499.
2. For the procedure to assign the certificate, see "Assign Services to a Certificate" at http://go.microsoft.com/fwlink/p/?linkId=195497.

1.4.3.9.1.2 Configure Unified Messaging on Microsoft Exchange

Configure Unified Messaging on Microsoft Exchange

Deploying Enterprise Voice > Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail > Configuring Unified Messaging on Microsoft Exchange Server to Work with Lync Server 2013 >

Topic Last Modified: *2013-02-24*

This topic describes how to configure Exchange Unified Messaging (UM) on a Microsoft Exchange Server for use with Enterprise Voice.

Note:
The cmdlet examples in this topic provide syntax for the Exchange 2007 version of Exchange Management Shell. If you are running Exchange 2010 or Exchange 2013, see the appropriate documentation as referenced.

To configure a server running Exchange Server UM

1. Create a UM Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) dial plan for each of your Enterprise Voice location profiles. If you choose to use the Exchange Management Console, create a new dial plan with the security setting **Secured (preferred)**.

   > **Warning:**
   > If you set your security setting value to **SIP Secured** to require encryption for SIP traffic only, as previously recommended, note that this security setting on a dial plan is insufficient if the Front End pool is configured to require encryption, which means the pool requires encryption for both SIP and RTP traffic. When the dial plan and pool security settings are not compatible, all calls to Exchange UM from the Front End pool will fail, resulting in an error indicating that you have an "Incompatible security setting."

   If you use the Exchange Management Shell, type:

   ```
   New-UMDialPlan -Name <dial plan name> -UriType "SipName" -VoipSecurity
   ```

   For details, see:

   - For Office Communications Server 2007, see "How to Create a Unified Messaging SIP URI Dial Plan" at http://go.microsoft.com/fwlink/p/?LinkId=268632 and "New-UMDialplan: Exchange 2007 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268666.
   - For Exchange 2010, see "Create a UM Dial Plan" at http://go.microsoft.com/fwlink/p/?LinkId=268674 and "New-UMDialplan: Exchange 2010 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268680.
   - For Exchange 2013, see "Unified Messaging" at http://go.microsoft.com/fwlink/p/?LinkID=266579.

   > **Note:**
   > Whether you select a security level of **SIPSecured** or **Secured** depends on whether secure real-time transport protocol (SRTP) is activated or deactivated for media encryption. For the Lync Server 2010 integration with Exchange UM, this should correspond to the encryption level in the Lync Server media configuration. The Lync Server media configuration can be viewed by running the **Get-CsMediaConfiguration** cmdlet. For details, see Get-CsMediaConfiguration in the Lync Server Management Shell documentation.
   > For details about selecting the appropriate VoIP Security setting, see Deployment Process for Integrating On-Premises Unified Messaging and Lync Server 2013.

2. Run the following cmdlet to obtain the fully qualified domain name (FQDN) for each UM dial plan:

   ```
   (Get-UMDialPlan <dialplanname>).PhoneContext
   ```

   For details, see:

   - For Exchange 2007, see "Get-UMDialplan: Exchange 2007 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268678.
   - For Exchange 2010, see "Get-UMDialplan: Exchange 2010 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268679.
   - For Exchange 2013, see "Unified Messaging" at http://go.microsoft.com/fwlink/p/?LinkID=266579.

3. Record the dial plan name of each UM dial plan. Depending on your version of Exchange Server, you may need to use the FQDN of each dial plan name later as the name of each UM dial plan’s corresponding Lync Server dial plan so that the dial plan names match.

   > **Note:**
   > Lync Server dial plan names must match UM dial plan names only if the UM

dial plan is running on a version of Exchange *earlier* than Exchange 2010 SP1.

4. Add the dial plan to the server running Exchange UM as follows:
   - If you choose to use the Exchange Management Console, you can add the dial plan from the property sheet for the server. For specific instructions, see the Exchange Server product documentation.

     For Exchange 2007, see "How to Add Unified Messaging Server to a Dial Plan" at http://go.microsoft.com/fwlink/p/?LinkId=268681.

     For Exchange 2010, see "View or Configure the Properties of a UM Server" at http://go.microsoft.com/fwlink/p/?LinkId=268682.

     For Exchange 2013, see "Unified Messaging" at http://go.microsoft.com/fwlink/p/?LinkID=266579.
   - If you use the Exchange Management Shell, run the following for each of your Exchange UM servers:

```
$ums=get-umserver;
$dp=get-umdialplan -id <name of dial-plan created in step 1>
$ums[0].DialPlans +=$dp.Identity;
set-umservice -instance $ums[0]
```

Note:

Before you perform the following step, make sure that all Enterprise Voice users have been configured with an Exchange Server mailbox.

For Exchange 2007, see the Exchange Server 2007 TechNet Library at http://go.microsoft.com/fwlink/p/?LinkId=268685.

For Exchange 2010, see the Exchange Server 2010 TechNet Library at http://go.microsoft.com/fwlink/p/?LinkId=268686.

When specifying a mailbox policy for each dial plan that you created in step 1, select either the default policy or one that you have created.

5. Navigate to <*Exchange installation directory*>\Scripts, and then if Exchange is deployed in a single forest, type:

```
exchucutil.ps1
```

Or, if Exchange is deployed in multiple forests, type:

```
exchucutil.ps1 -Forest:"<forest FQDN>"
```

where *forest FQDN* specifies the forest in which Lync Server is deployed.

If you have one or more UM dial plans that are associated with multiple IP gateways, continue to step 6. If your dial plans are each associated with only a single IP gateway, skip step 6.

Important:

Be sure to restart the **Lync Server Front-End** service (rtcsrv.exe) *after* you run exchucutil.ps1. Otherwise, Lync Server will not detect Unified Messaging in the topology.

6. Using either the Exchange Management Shell or Exchange Management Console, disable outbound calling for all but one of the IP gateways associated with each of your dial plans.

Note:

This step is necessary to make sure that outbound calls by the server running Exchange Server Unified Messaging to external users (for example, as is the case with play-on-phone scenarios) reliably traverse the corporate firewall.

Important:

When selecting the UM IP gateway through which to allow outgoing calls, choose the one that is likely to handle the most traffic. Do not allow outgoing traffic through an IP gateway that connects to a pool of Lync Server

Directors. Also avoid pools in another central site or a branch site. You can use either of the following methods to block outgoing calls from passing through an IP gateway:

- If you use the Exchange Management Shell, disable each IP gateway by running the following command:

  ```
  Set-UMIPGateway <gatewayname> -OutcallsAllowed $false
  ```

  For Exchange 2007, see "Set-UMIPGateway: Exchange 2007 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268687.
  For Exchange 2010, see "Set-UMIPGateway: Exchange 2010 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268688.
- If you use the Exchange Management Console, clear the **Allow outgoing calls through this IP gateway** check box.

Important:
If your UM SIP URI dial plan is associated with only a single IP gateway, do not disallow outgoing calls through this gateway.

7. Create a UM auto-attendant for each Lync Server dial plan.

Important:
Do not include any spaces in the name of the auto attendant.

```
New-umautoattendant -name <auto attendant name> -umdialplan < name of
```

For details, see:

- For Exchange 2007, see "New-UMAutoAttendant: Exchange 2007 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268689.
- For Exchange 2010, see "New-UMAutoAttendant: Exchange 2010 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268690.

The following step should be performed for each user after you have enabled Lync Server users for Enterprise Voice and know their SIP URIs.

8. Associate Exchange UM users (each of whom should be configured with an Exchange mail box) with the UM dial plan and create a SIP URI for each user.

Note:
The **SIPResourceIdentifier** in the following sample must be the SIP address of the Lync Server user.

```
enable-ummailbox -id <user name> -ummailboxpolicy <name of the mailbox
```

For details, see:

- For Exchange 2007, see "Enable-UMMailbox: Exchange 2007 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268691.
- For Exchange 2010, see "Enable-UMMailbox: Exchange 2010 Help" at http://go.microsoft.com/fwlink/p/?LinkId=268692.

1.4.3.9.2 Configure Lync Server 2013 to Work with Unified Messaging on Microsoft Exchange Server

Configure Lync Server 2013 to Work with Unified Messaging on Microsoft Exchange Server

Deployment > Deploying Enterprise Voice > Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail >

Topic Last Modified: *2012-09-26*

This step requires the Exchange UM Integration Utility (OcsUmUtil.exe). This tool is located on the Lync Server 2013 in the %CommonProgramFiles%\Microsoft Lync Server 2013 \Support folder.

Running the Exchange UM Integration Utility

The Exchange UM Integration Utility must be run from a user account with the following characteristics:

- Membership in the RTCUniversalServerAdmins and RtcUniversalUserAdmins groups (which includes permission to read Exchange Server Unified Messaging settings).
- User rights within the domain to create contact objects in the specified organizational unit (OU) container.

When you run the Exchange UM Integration Utility, it performs the following tasks:

- Creates contact objects for each auto-attendant and subscriber access number to be used by Enterprise Voice users.
- Verifies that the name of each Enterprise Voice dial plan matches its corresponding unified messaging (UM) dial plan phone context. This matching is necessary only if the UM dial plan is running on a version of Exchange *earlier* than Exchange 2010 Service Pack 1 (SP1).

> **Important:**
>
> Before running the Exchange UM Integration Utility, be sure that you have done the following:
>
> - Create one or more Exchange UM dial plans, as described in the Exchange product documentation.
>   For Microsoft Exchange Server 2010, see "Create a UM Dial Plan" at http://go.microsoft.com/fwlink/p/?linkId=186177.
>   For Microsoft Exchange Server 2007 Service Pack 1 (SP1), see "How to Create a Unified Messaging SIP URI Dial Plan" at http://go.microsoft.com/fwlink/p/?linkId=185771.
> - Create one or more corresponding Lync Server dial plans, as described in Create a Dial Plan.
>
>   > **Important:**
>   >
>   > If you are using a version of Exchange that is earlier than Microsoft Exchange Server 2010 SP1, you must enter the fully qualified domain name (FQDN) of the corresponding Exchange Unified Messaging (UM) SIP dial plan in the Lync Server 2013 dial plan **Simple name** field. If you are using Microsoft Exchange Server 2010 SP1 or latest service pack, this dial plan name matching is not necessary.
>
> - Create an auto-attendant and make sure that both the subscriber access number and auto-attendant number are in E.164 format.

To run the Exchange UM Integration Utility

1. On a Front End Server, open a command prompt and type **cd %CommonProgramFiles%\Microsoft Lync Server 2013\Support**, and then press ENTER.
2. Type **OcsUmUtil.exe**, and then press ENTER.
3. Click **Load Data** to find all trusted Exchange forests.
4. In the **SIP Dial Plans** list, select a UM SIP dial plan for which you want to create contact objects, and then click **Add**.
5. In the **Contact** box, accept the default organizational unit, or click **Browse** to start the **OU Picker**. In the **OU Picker** box, you can select an OU and click **OK**, or you can click **Make New OU** to create a new organizational unit under the root or any other OU in the domain (for example, "OU=RTC Special Accounts,DC=fourthcoffee,DC=com"), and then click **OK**.

   > **Note:**

The distinguished name (DN) of the OU that you have selected or created is now displayed in the **Organizational Unit** box.

6. In the **Name** box, either accept the default dial plan name or type a new display name for the contact object that you are creating.

   Note:
   For example, if you are creating a subscriber access contact object, you might simply name it Subscriber Access.

7. In the **SIP Address** box, either accept the default SIP address or type a new SIP address.

   Note:
   If you type a new SIP address, it must begin with **SIP:** (that is, "SIP:" including the colon).

8. In the **Server or Pool** list, select the Standard Edition server or Front End pool in which the contact object is to be enabled.

   Note:
   Preferably, the pool you select is the same one pool where users enabled for Enterprise Voice and Exchange UM are deployed.

9. In the **Phone Number** list, select either **Enter phone number** or **Use this pilot number from Exchange UM** and then enter a phone number.
10. In the **Contact Type** list, select the contact type that you want to create, and then click **OK**.
11. Repeat steps 1 through 10 for additional contact objects that you want to create.

   Note:
   You should create at least one contact for each auto attendant. If you want external access, you also need a Subscriber Access contact and to specify Direct Inward Dial (DID) numbers.

To verify that the contact objects have been created, open Active Directory Users and Computers and select the OU in which the objects were created. The contact objects should appear in the details pane.

1.4.3.10 Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM

Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-09-24*

This section guides you through the process of providing users in an on-premises Lync Server 2013 deployment with voice mail on a hosted Exchange Unified Messaging (UM) service.

- Create a DNS SRV Record for Integration with Hosted Exchange UM
- Configure the Edge Server for Integration with Hosted Exchange UM
- Manage Hosted Voice Mail Policies
- Enable Users for Hosted Voice Mail
- Create Contact Objects for Hosted Exchange UM

Create a DNS SRV Record for Integration with Hosted Exchange UM

See Also

Deployment > Deploying Enterprise Voice > Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM >

Topic Last Modified: *2013-02-20*

This topic describes how to configure the Domain Name System (DNS) SRV record that is required for a Lync Server 2013 Edge Server to route to a hosted Exchange service such as Microsoft Exchange Online.

⊟To create an external DNS SRV record for the hosted Exchange service

1. Log on to the external DNS server as a member of the DnsAdmins group.
2. Click **Start**, click **Administrative Tools**, and then click **DNS**.
3. In the console tree for your SIP domain, expand **Forward Lookup Zones**, and select the SIP domain in which Lync Server 2013 will be installed.

   Important:

   You must create the DNS SRV record in the SIP domain in which Lync Server is or will be installed. When you create the SRV record, the FQDN used for the Host offering this service field must be the external FQDN of the Edge pool. For example, if the external FQDN of your Edge pool is edge01.contoso.net, enter that value. This must also be in the same domain as the DNS Hosts (A) record.

4. Right-click the selected domain, and then click **Other New Records**.
5. In **Resource Record Type**, click **Service Location (SRV)**, and then click **Create Record**.
6. In **New Resource Record**, click **Service**, and then type **_sipfederationtls**.
7. Click **Protocol**, and then type **_tcp**.
8. Click **Port Number**, and then type **5061**.
9. Click **Host offering this service**, and then type the fully qualified domain name (FQDN) of the Lync Server 2013 Edge pool that provides access to your Lync Server 2013 system for trusted external clients.

   Note:

   The domain must also be set up as an authoritative, accepted domain in your Exchange Online settings. For details, see Create Accepted Domains at http://go.microsoft.com/fwlink/p/?linkId=229762.

10. Click **OK**, and then click **Done**.

⊟To verify that the DNS SRV record was created successfully

1. Log on to a client computer in the domain.
2. Click **Start**, and then click **Run**.
3. At the command prompt, run the following command:

   ```
   nslookup <FQDN Lync Edge Pool>
   ```

4. Verify that you receive a reply that resolves to the appropriate IP address for the FQDN.

Concepts

Create DNS Records for Reverse Proxy Servers

1.4.3.10.2 Configure the Edge Server for Integration with Hosted Exchange UM

Configure the Edge Server for Integration with Hosted Exchange UM

See Also

Deployment > Deploying Enterprise Voice > Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM >

Topic Last Modified: *2012-10-10*

To provide your Lync Server 2013 users with voice mail capabilities on hosted Exchange Unified Messaging (UM), you must perform the following configuration tasks on the Edge Server:

- Configure the Edge Server for federation.
- Replicate Central Management store data to the Edge Server and verify the replication.
- Create a hosting provider on the Edge Server.

For details, see the Lync Server Management Shell documentation for the following cmdlets:

- Set-CsAccessEdgeConfiguration
- New-CsHostingProvider

Important:

You must create an external DNS SRV record for the hosting Exchange service before you perform these steps. For details, see Create a DNS SRV Record for Integration with Hosted Exchange UM.

To configure the Edge Server for federation

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsAccessEdgeConfiguration cmdlet to configure the server for federation. For example, run:

   ```
   Set-CsAccessEdgeConfiguration -UseDnsSrvRouting -AllowFederatedUsers 1
   ```

   The preceding example sets the following parameters:

   - **UseDnsSrvRouting** specifies that Edge Servers will rely on DNS SRV records when sending and receiving federation requests.
   - **AllowFederatedUsers** specifies whether internal users are allowed to communicate with users from federated domains. This property also determines whether internal users can communicate with users in a split domain scenario.
   - **EnablePartnerDiscovery** specifies whether Lync Server will use DNS records to try to discover partner domains not listed in the Active Directory allowed domains list. If False, Lync Server 2013 will only federate with domains found on the allowed domains list. This parameter is required if you use DNS service routing. In most deployments, the value is set to false to avoid opening up federation to all partners.

To replicate data to the Edge Server and verify the replication

- Verify that the replication to the Edge Server is complete. For the procedure, see Verify Connectivity Between Internal Servers and Edge Servers.

To create a hosting provider on the Edge Server

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click

Microsoft Lync Server 2013, and then click **Lync Server Management Shell**.

2. Run the **New-CsHostingProvider** cmdlet to configure the hosting provider. For example, run:

```
New-CsHostingProvider -Identity Fabrikam.com -Enabled $True -EnabledSh
```

The preceding example sets the following parameters:

- **Identity** specifies a unique string value identifier for the hosting provider you are creating, in this example, **Fabrikam.com**. Note that the command will fail if an existing provider has already been configured with that Identity.
- **Enabled** indicates whether the network connection between your domain and the hosting provider is enabled. Messages cannot be exchanged between the two organizations until this value is set to **True**.
- **EnabledSharedAddressSpace** indicates whether the hosting provider is being used in a shared SIP address space (split domain) scenario.
- **HostsOCSUsers** indicates whether the hosting provider is used to host Lync Server 2013 accounts. If **False**, the provider hosts other account types, such as Microsoft Exchange accounts.
- **ProxyFQDN** specifies the fully qualified domain name (FQDN) for the proxy server used by the hosting provider, in this example, **proxyserver.fabrikam.com**. This value cannot be modified. If the hosting provider changes its proxy server you will need to delete and then recreate the entry for that provider.
- **IsLocal** indicates whether the proxy server used by the hosting provider is contained within your Lync Server 2013 topology.
- **VerficationLevel** indicates the allowed verification level for messages sent to and from the hosted provider. Specify **UseSourceVerification**, which relies on the verification level included in messages sent from the hosting provider. If this level is not specified, then the message will be rejected as being unverifiable.

Tasks

Export Your Topology and Copy It to External Media for Edge Installation

Concepts

Verify Connectivity Between Internal Servers and Edge Servers

Other Resources

New-CsHostingProvider

1.4.3.10.3 Manage Hosted Voice Mail Policies

Manage Hosted Voice Mail Policies

Deployment > Deploying Enterprise Voice > Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM >

Topic Last Modified: *2012-09-20*

A *hosted voice mail policy* provides information to the Lync Server 2013 ExUM Routing application about where to route calls for users whose mailboxes are located on a hosted Exchange service.

Note:

Typically, only one hosted voice mail policy is required. In many cases, you can modify the global policy to meet all your needs. If you create a policy with site scope, it is assigned automatically to all users homed at the specified site. If you create a policy with per-user scope, you must explicitly assign it to users, groups, and contact objects. It is possible to deploy multiple hosted voice mail policies, but in that case the policies must be assigned on a per-user basis.

For details about planning hosted voice mail policies, see Hosted Voice Mail Policies in the Planning documentation.

- Modify the Global Hosted Voice Mail Policy
- Create a Site-Level Hosted Voice Mail Policy
- Create a Per-User Hosted Voice Mail Policy
- Assign a Per-User Hosted Voice Mail Policy

1.4.3.10.3.1 Modify the Global Hosted Voice Mail Policy

Modify the Global Hosted Voice Mail Policy

Deploying Enterprise Voice > Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM > Manage Hosted Voice Mail Policies >

***Topic Last Modified:** 2012-09-24*

The *global* hosted voice mail policy is installed with Lync Server 2013. You can modify it to meet your needs, but you cannot rename or delete it. To modify the global policy, you use the Set-CsHostedVoicemailPolicy cmdlet to set the parameters to appropriate values for your specific deployment.

For details about the Set-CsHostedVoicemailPolicy cmdlet, see the Lync Server Management Shell documentation.

To modify the global hosted voice mail policy

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsHostedVoicemailPolicy cmdlet to set the global policy parameters for your environment. For example, run:

```
Set-CsHostedVoicemailPolicy -Destination ExUM.fabrikam.com -Organizati
```

Because this command does not specify the policy’s Identity parameter, Windows PowerShell command-line interface sets the following values on the global hosted voice mail policy:

- **Destination** specifies the fully qualified domain name (FQDN) of the hosted Exchange UM service. This parameter is optional, but if you attempt to enable a user for hosted voice mail and the user’s assigned policy does not have a Destination value, the enable will fail.
- **Organization** specifies a comma-separated list of the Exchange tenants that home Lync Server users. Each tenant must be specified as the FQDN of that tenant on the hosted Exchange UM service.

Note:

In the previous example cmdlet, the value “corp1.litwareinc.com” replaces any value that might already be present in the Organization parameter. For example, if the policy already contains a comma-separated list of organizations, the full list would be replaced. If you want to add an organization to the list rather than replace the entire list, run a command similar to the following.

```
$a = Get-CsHostedVoicemailPolicy
$a.Organization += ",corp3.litwareinc.com"
Set-CsHostedVoicemailPolicy -Organization $a.Organization
```

1.4.3.10.3.2 Create a Site-Level Hosted Voice Mail Policy

Create a Site-Level Hosted Voice Mail Policy

Deploying Enterprise Voice > Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM > Manage Hosted Voice Mail Policies >

***Topic Last Modified:** 2012-09-24*

A *site* policy can impact all users that are homed on the site for which the policy is defined. If a user is configured for hosted Exchange UM access and has not been assigned a Per-user policy, the site policy applies. If you have not deployed a site policy, the global policy applies.

For details about configuring site policies, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsHostedVoicemailPolicy
- Set-CsHostedVoicemailPolicy
- Get-CsHostedVoicemailPolicy

To create a site hosted voice mail policy

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the New-CsHostedVoicemailPolicy cmdlet to create the policy. For example, run:

```
New-CsHostedVoicemailPolicy -Identity site:Redmond -Destination ExUM.f
```

   This example creates a hosted voice mail policy with site scope, and sets the following parameters:

   - **Identity** specifies a unique identifier for the policy, which includes the scope. For a policy with site scope, the Identity parameter value must be specified in the format `site:`<*name*>, for example, `site:Redmond`.
   - **Destination** specifies the fully qualified domain name (FQDN) of the hosted Exchange UM service. This parameter is optional, but if you attempt to enable a user for hosted voice mail and the user’s assigned policy does not have a Destination value, the enable will fail.
   - **Description** provides optional descriptive information about the policy.
   - **Organization** specifies a comma-separated list of the Exchange tenants that home Lync Server 2013 users. Each tenant must be specified as the FQDN of that tenant on the hosted Exchange UM service.

1.4.3.10.3.3 Create a Per-User Hosted Voice Mail Policy

Create a Per-User Hosted Voice Mail Policy

See Also

Deploying Enterprise Voice > Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM > Manage Hosted Voice Mail Policies >

***Topic Last Modified:** 2012-09-24*

A *per-user* policy can only impact individual users, groups, and contact objects. To deploy a per-user policy, you must explicitly assign the policy to one or more users, groups, or contact objects. For details, see Assign a Per-User Hosted Voice Mail Policy.

For details about working with per-user hosted voice mail policies, see the Lync Server

Management Shell documentation for the following cmdlets:

- New-CsHostedVoicemailPolicy
- Set-CsHostedVoicemailPolicy
- Get-CsHostedVoicemailPolicy

To create a per-user hosted voice mail policy

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the New-CsHostedVoicemailPolicy cmdlet to create the policy. For example, run:

```
New-CsHostedVoicemailPolicy -Identity ExRedmond -Destination ExUM.fabr
```

The previous example creates a hosted voice mail policy with per-user scope, and sets the following parameters:

- **Identity** specifies a unique identifier for the policy, which includes the scope. For a policy with per-user scope, this parameter value is specified as a simple string, for example, ExRedmond.
- **Destination** specifies the fully qualified domain name (FQDN) of the hosted Exchange UM service. This parameter is optional, but if you attempt to enable a user for hosted voice mail and the user’s assigned policy does not have a Destination value, the enable will fail.
- **Description** provides optional descriptive information about the policy.
- **Organization** specifies a comma-separated list of the Exchange tenants that home Lync Server 2013 users. Each tenant must be specified as the FQDN of that tenant on the hosted Exchange UM service.

Tasks

Assign a Per-User Hosted Voice Mail Policy

1.4.3.10.3.4 Assign a Per-User Hosted Voice Mail Policy

Assign a Per-User Hosted Voice Mail Policy

Deploying Enterprise Voice > Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM > Manage Hosted Voice Mail Policies >

***Topic Last Modified:** 2010-11-07*

Deploying one or more per-user hosted voice mail policies is optional. If you do deploy per-user policies, you must explicitly assign them to users, groups, or contact objects.

For details about assigning or removing the assignment of per-user hosted voice mail policies, see the Lync Server Management Shell documentation for the following cmdlets:

- Grant-CsHostedVoicemailPolicy
- Remove-CsHostedVoicemailPolicy

To assign a per-user hosted voice mail policy

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Grant-CsHostedVoicemailPolicy cmdlet to assign the per-user hosted voice mail policy to individual users, groups, and contact objects. For example, run:

```
Grant-CsHostedVoicemailPolicy -Identity "Ken Myer" -PolicyName ExRedmo
```

This example assigned the ExRedmond hosted voice mail policy to user Ken

Myer.

Identity specifies the user account to be modified. The Identity value can be specified using any of the following formats:

- The user's SIP address
- The user's Active Directory User-Principal-Name
- The user's domain\logon name (for example, contoso\kenmyer)
- The user's Active Directory Domain Services Display-Name (for example, Ken Myer). If using the Display-Name as the Identity value, you can use the asterisk (*) wildcard character. For example, the Identity "* Smith" returns all the users who have a Display-Name that ends with the string value "Smith".

Note:

The user’s Active Directory SAM-Account-Name cannot be used as the Identity value because the SAM-Account-Name is not necessarily unique in the forest.

1.4.3.10.4 Enable Users for Hosted Voice Mail

Enable Users for Hosted Voice Mail

Deployment > Deploying Enterprise Voice > Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM >

Topic Last Modified: *2012-09-24*

Follow the procedure to enable Lync Server 2013 users for voice mail on a hosted Exchange Unified Messaging (UM) service.

For details, see Hosted Exchange User Management in the Planning documentation.

For details about the Set-CsUser cmdlet, see the Lync Server Management Shell documentation.

Important:

Before a Lync Server 2013 user can be enabled for hosted voice mail, a hosted voice mail policy that applies to their user account must be deployed. For details, see Hosted Voice Mail Policies.

⊟To enable users for hosted voice mail

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsUser cmdlet to configure the user account for hosted voice mail. For example, run:

```
Set-CsUser -HostedVoiceMail $True -Identity "contoso\kenmyer"
```

The preceding example sets the following parameters:

- **HostedVoiceMail** enables a user’s voice mail calls to be routed to hosted Exchange UM. It also signals Microsoft Lync 2013 to light up the “call voice mail” indicator.
- **Identity** specifies the user account to be modified. The Identity value can be specified using any of the following formats:
    - The user's SIP address
    - The user's Active Directory User-Principal-Name
    - The user's domain\logon name (for example, contoso\kenmyer)
    - The user's Active Directory Domain Services Display-Name (for example, Ken Myer). If using the Display-Name as the Identity value, you can use

the asterisk (*) wildcard character. For example, the Identity "* Smith" returns all the users who have a Display-Name that ends with the string value "Smith".

> **Note:**
> The user’s Active Directory SAM-Account-Name cannot be used as the Identity value because the SAM-Account-Name is not necessarily unique in the forest.

1.4.3.10.5 Create Contact Objects for Hosted Exchange UM

Create Contact Objects for Hosted Exchange UM

Deployment > Deploying Enterprise Voice > Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM >

Topic Last Modified: *2012-09-24*

The following procedure explains how to create Auto Attendant (AA) or Subscriber Access (SA) contact objects for hosted Exchange Unified Messaging (UM).

For details, see Hosted Exchange Contact Object Management in the Planning documentation.

For details about configuring contact objects, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsExUmContact
- Set-CsExUmContact

> **Important:**
> Before Lync Server 2013 contact objects can be enabled for hosted Exchange UM, a hosted voice mail policy that applies to them must be deployed. For details, see Hosted Voice Mail Policies.

To create AA or SA contact objects for hosted Exchange UM

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the New-CsExUmContact cmdlet to create any contact objects required for your deployment. For example, run the following to create an AA and an SA contact object:

```
New-CsExUmContact -SipAddress "sip:exumaa1@fabrikam.com" -RegistrarPoo
```

```
New-CsExUmContact -SipAddress "sip:exumsa1@fabrikam.com" -RegistrarPoo
```

These examples set the following parameters:

- **SipAddress** specifies the SIP address of the contact object. This must be an address that has not already been used to configure a user or contact object in Active Directory Domain Services. This value must be in the format “sip:<*SIP address*>“ as shown in the previous examples.
- **RegistrarPool** specifies the fully qualified domain name (FQDN) of the pool on which the Registrar service is running.

> **Note:**
> Exchange UM contact objects cannot be moved to pools that are part of Lync Server 2013 deployments prior to Lync Server 2013.

- **OU** specifies the Active Directory organizational unit where this contact object will be located.

- **DisplayNumber** specifies the telephone number of the contact object. The phone number for each contact object must be unique.
- **AutoAttendant** specifies whether the Contact object is an Auto Attendant. Auto Attendant provides a set of voice prompts that allow callers to navigate the phone system and reach the party that they want to contact. A value of **False** (the default) for this parameter indicates a Subscriber Access contact object.

1.4.3.11 Configuring On-premises Lync Server 2013 Integration with Exchange Online

Configuring On-premises Lync Server 2013 Integration with Exchange Online

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-10-21*

Customers who are using on-premises Lync Server 2013 deployments can configure interoperability with Microsoft Outlook Web App in Microsoft Exchange Online in a hybrid deployment mode. Interoperability features include single sign on and instant messaging (IM) and presence integration with the Outlook Web App interface. To enable this integration, you must configure the Edge Server in your on-premises Lync Server deployment by completing the following tasks:

- Configure a shared SIP address space
- Configure a hosting provider on the Edge Server
- Verify replication of the updated Central Management store

Configure a Shared SIP Address Space

To integrate on-premises Lync Server 2013 with Exchange Online, you must configure a shared SIP address space. The same SIP domain address space is supported by both Lync Server and the Exchange Online service.

Using the Lync Server Management Shell, configure the Edge Server for federation by running the **Set-CSAccessEdgeConfiguration** cmdlet, using the parameters displayed in the following example:

```
Set-CsAccessEdgeConfiguration -AllowFederatedUsers $True
```

- **AllowFederatedUsers** parameter specifies whether internal users are allowed to communicate with users from federated domains. This property also determines whether internal users can communicate with users in a shared SIP address space scenario with Lync Server and Exchange Online.

For details about using the Lync Server Management Shell, see Lync Server Management Shell.

Configure a Hosting Provider on the Edge Server

Using the Lync Server Management Shell, configure a hosting provider on the Edge Server by running the **New-CsHostingProvider** cmdlet, using the parameters in the following example:

```
New-CsHostingProvider -Identity "Exchange Online" -Enabled $True -EnabledSharedAd
```

- **Identity** specifies a unique string value identifier for the hosting provider that you are creating (for example, "Exchange Online"). Values that contain spaces must be in double quotes.

- **Enabled** indicates whether the network connection between your domain and the hosting provider is enabled. This must be set to True.
- **EnabledSharedAddressSpace** indicates whether the hosting provider will be used in a shared SIP address space scenario. This must be set to True.
- **HostsOCSUsers** indicates whether the hosting provider is used to host Office Communications Server or Lync Server. This must be set to False.
- **ProxyFQDN** specifies the fully qualified domain name (FQDN) for the proxy server used by the hosting provider. For Exchange Online, the FQDN is exap.um.outlook.com.
- **IsLocal** indicates whether the proxy server used by the hosting provider is contained within your Lync Server topology. This must be set to False.
- **VerificationLevel** Indicates the verification level allowed for messages that are sent to and from the hosted provider. Specify **UseSourceVerification**, which relies on the verification level included in messages sent from the hosting provider. If this level is not specified, the message will be rejected as being unverifiable.

Verify Replication of the Updated Central Management Store

The changes you made by using the cmdlets in the preceding sections are automatically applied to the Edge Server, and generally take less than a minute to replicate. You can validate replication status, and then confirm that the changes were applied to your Edge Server by using the following cmdlets.

To verify replication updates, on a server internal in your Lync Server deployment, run the following cmdlet:

```
Get-CsManagementStoreReplicationStatus
```

To confirm that the changes were applied, on the Edge Server, run the following cmdlet:

```
Get-CsHostingProvider -LocalStore
```

See Also

Other Resources

Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM
Hosted Exchange Unified Messaging Integration

1.4.3.12 Deploying Advanced Enterprise Voice Features

Deploying Advanced Enterprise Voice Features

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-09-22*

After you have configured basic Enterprise Voice functionality for your organization, you can optionally deploy one or more advanced Enterprise Voice features by following the procedures in this section.

For details about the advanced Enterprise Voice features, see the following sections of the Planning documentation:

- Planning for Call Admission Control
- Planning for Emergency Services (E9-1-1)

- Planning for Media Bypass
- About Network Regions, Sites, and Subnets
- Create or Modify a Network Region
- Create or Modify a Network Site
- Associate a Subnet with a Network Site
- Configure Call Admission Control
- Configure Enhanced 9-1-1
- Configure Media Bypass

1.4.3.12.1 About Network Regions, Sites, and Subnets

About Network Regions, Sites, and Subnets

Deployment > Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features >

***Topic Last Modified:** 2013-02-24*

The advanced Enterprise Voice features described in this section share certain configuration requirements for network regions, network sites, and subnets. For example, all three advanced features require that each subnet in your topology be associated with a specific *network site*, and each network site must be associated with a *network region*.

> ◆**Important:**
>
> Before you begin network configuration for call admission control, E9-1-1, or media bypass, make sure that you reviewed additional information about network settings in the Network Settings for the Advanced Enterprise Voice Features topic in the Planning documentation. For details about network configuration primarily about call admission control, also see Defining Your Organization's Requirements for Call Admission Control in the Planning documentation.

Call admission control and E9-1-1 have additional configuration requirements for network sites:

- Call admission control requires that a *bandwidth policy profile* be specified for each site that is constrained by WAN bandwidth limitations. If you plan to deploy call admission control, you must Create Bandwidth Policy Profiles before you configure your network sites.
- E9-1-1 requires that a *location policy* be specified for each site. If you plan to deploy E9-1-1, you must Create Location Policies before you configure your network sites.

Create or Modify Network Regions, Network Sites, and Subnets

The following topics provide steps to create or modify network regions and network sites, and to associate subnets with network sites. These topics are not specific to any particular advanced Enterprise Voice feature.

- Create or Modify a Network Region
- Create or Modify a Network Site
- Associate a Subnet with a Network Site

1.4.3.12.2 Create or Modify a Network Region

Create or Modify a Network Region

Deployment > Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features >

Topic Last Modified: *2012-10-19*

Network regions are the network hubs or backbones used in the configuration of call admission control, E9-1-1, and media bypass. Use the following procedures to create or modify network regions. For example, if you have already created network regions for one Voice feature, you do not need to create new network regions; other advanced Enterprise Voice features will use those same network regions. You may, however, need to modify an existing network region definition to apply feature-specific settings. For example, if you have created network regions for E9-1-1 (which do not require an associated central site) and you then deploy call admission control, you need to modify the network region definitions to specify a central site. For details, see Configure Network Regions for CAC.

Note:

Any feature-specific requirements for network region definitions are documented in the Deployment topics for the feature.

For details about working with network regions, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsNetworkRegion
- Get-CsNetworkRegion
- Set-CsNetworkRegion
- Remove-CsNetworkRegion

Create a Network Region

Create a network region that can be used by call admission control, E9-1-1, or media bypass.

To create a network region using Lync Server Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the New-CsNetworkRegion cmdlet to create network regions:

   ```
   New-CsNetworkRegion -Identity <String> -CentralSite <String>
   ```

   For example:

   ```
   New-CsNetworkRegion -Identity NorthAmerica -CentralSite CHICAGO -Descr
   ```

   In this example, you created a network region called “NorthAmerica” that is associated with a central site with site ID CHICAGO.
3. To finish creating network regions for your topology, repeat step 2 with settings for each network region.

To create a network region using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Click **Region**.
4. Click **New**.
5. On the **New Region** page, click **Name** and then type a name for the network region.
6. Click **Central site**, and then click a central site in the list.
7. Optionally, click **Description**, and then type additional information to describe this network site.
8. Click **Commit**.
9. To finish creating network regions for your topology, repeat steps 4 through

8 with settings for other regions.

Modify a Network Region

Modify settings for an existing network region to accommodate changes to the basic region information or changes required by a new feature.

⊟To modify a network region using Lync Server Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsNetworkRegion cmdlet to modify an existing network region:

   ```
   Set-CsNetworkRegion -Identity <String> -CentralSite <String>
   ```

   For example:

   ```
   Set-CsNetworkRegion -Identity NorthAmerica -CentralSite CHICAGO -Descr
   ```

   In this example, you modified an existing network region called “NorthAmerica” (created using the procedures earlier in this topic) by changing the description. If a description existed for the “NorthAmerica” region, this command overwrites it with this value; if no description had been set, then this command sets it.
3. To modify other network regions, repeat step 2 with settings for other regions.

⊟To modify a network region using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Region** navigation button.
4. In the table, click the network region that you want to modify.
5. Click **Edit**, and then click **Show details...**.
6. On the **Edit Region** page, change the values for this network region’s settings as appropriate.
7. Click **Commit**.
8. To finish modify network regions, repeat steps 4 through 7 with settings for other regions.

1.4.3.12.3 Create or Modify a Network Site

Create or Modify a Network Site

Deployment > Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features >

Topic Last Modified: *2013-02-24*

Call admission control (CAC), E9-1-1, and media bypass deployments rely on the configuration of *network sites* which are defined within and always associated with a network region. A network site represents a branch office location, a set of buildings, or a campus. Network sites represent collections of subnets with similar bandwidth.

Use the following procedures to create or modify network sites. For example, if you have already created network sites for one Voice feature, you do not need to create new network sites; other Voice features will use those same sites. You may, however, need to modify an existing network site definition to apply feature-specific settings. For example, if you created a network site for E9-1-1, you need to modify the network site during deployment of call admission control to apply a bandwidth policy profile.

Note:

Where they exist, you can find specific examples and requirements for network sites as they pertain to an advanced Voice feature in the Deployment documentation for each feature:

- Configure Network Sites for CAC

For details about working with network sites, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsNetworkSite
- Get-CsNetworkSite
- Set-CsNetworkSite
- Remove-CsNetworkSite

Create a Network Site

Create a network region that can be used by call admission control, E9-1-1, or media bypass.

To create a network site by using Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the New-CsNetworkSite cmdlet to create network sites:

   ```
   New-CsNetworkSite -NetworkSiteID <string>
   ```

   For example:

   ```
   New-CsNetworkSite -NetworkSiteID Chicago -Description "Corporate headq
   ```

   In this example, you created a network site called “Chicago” that is in the “NorthAmerica” network region.

   Note:

   The NorthAmerica network region must already exist for this command to run successfully.
3. To finish creating network sites for your topology, repeat step 2 with settings for other sites.

To create a network site by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Site** navigation button.
4. Click **New**.
5. On the **New Site** page, click **Name** and then type a name for the network site.
6. Click **Region**, and then click a region in the list.
7. Optionally, click **Bandwidth policy**, and then click a bandwidth policy in the list.

   Note:

   Bandwidth policy is required only if you deploy call admission control at the site.
8. Optionally, click **Location policy**, and then click a location policy in the list.

   Note:

   Location policy is required only if you deploy E9-1-1 at the site.
9. Optionally, click **Description**, and then type additional information to describe

this network site.

10. Click **Commit**.
11. To finish creating network sites for your topology, repeat steps 4 through 10 with settings for other sites.

Modify a Network Site

Modify a network region that can be used by call admission control, E9-1-1, or media bypass.

⊟To modify a network site

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsNetworkSite cmdlet to modify network sites:

```
Set-CsNetworkSite -Identity <string>
```

For example:

```
Set-CsNetworkSite -Identity Albuquerque -NetworkRegionID NorthAmerica
```

In this example, the site called “Albuquerque” is moved to the “NorthAmerica” network region. To modify the network site configuration to deploy call admission control, E9-1-1, or media bypass, modify the network site settings by running the Set-CsNetworkSite cmdlet with the BWPolicyProfileID or LocationPolicy parameter, respectively.

> **Note:**
> Although the BypassID parameter exists for media bypass, we strongly recommend that you do not override automatically generated bypass IDs. You do not need to specify additional parameters to configure a network site for media bypass.

3. To finish modifying network sites for your topology, repeat step 2 with settings for other sites.

⊟To modify a network site by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Site** navigation button.
4. In the table, click the network site that you want to modify.
5. Click **Edit**, and then click **Show details...**.
6. On the **Edit Site** page, change the values for this network site’s settings as appropriate.
7. Click **Commit**.
8. To finish modify network sites, repeat steps 4 through 7 with settings for other sites.

1.4.3.12.4 Associate a Subnet with a Network Site

Associate a Subnet with a Network Site

Deployment > Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features >

Topic Last Modified: *2012-10-19*

Every subnet in your network must be associated with a specific network site, because subnet information is used to determine the network site on which an endpoint is located while a new session is initiated. When the location of each party in a session is known, advanced Enterprise Voice features can apply that information to determine how to handle the call setup or routing.

Important:

All configured public IP addresses of the Audio/Video Edge Servers in your deployment must be added to your network configuration settings. These IP addresses are added as subnets with a mask of 32. The associated network site should correspond to the appropriate configured network site. For example, the public IP address that corresponds to the A/V Edge Server in central site Chicago would be NetworkSiteID Chicago. For details about public IP addresses, see Determine External A/V Firewall and Port Requirements in the Planning documentation.

Note:

A Key Health Indicator (KHI) alert is raised, specifying a list of IP addresses that are present in your network but are either not associated with a subnet, or the subnet that includes the IP addresses is not associated with a network site. This alert will not be raised more than once within an 8-hour period. The relevant alert information and an example are as follows:

Source: CS Bandwidth Policy Service (Core)
Event number: 36034
Level: 2
Description: The subnets for the following IP addresses: <List of IP Addresses> are either not configured or the subnets are not associated to a Network Site.
Cause: The subnets for the corresponding IP addresses are missing from the network configuration settings or the subnets are not associated to a network site.
Resolution: Add subnets corresponding to the list of IP addresses into the network configuration settings and associate every subnet to a network site.

For example, if the IP address list in the alert specifies 10.121.248.226 and 10.121.249.20, either these IP addresses are not associated with a subnet or the subnet they are associated with does not belong to a network site. If 10.121.248.0/24 and 10.121.249.0/24 are the corresponding subnets for these addresses, you can resolve this issue as follows:

1. Be sure that IP address 10.121.248.226 is associated with the 10.121.248.0/24 subnet and IP address 10.121.249.20 is associated with the 10.121.249.0/24 subnet.
2. Be sure that the 10.121.248.0/24 and 10.121.249.0/24 subnets are each associated with a network site.

For details about working with network subnets, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsNetworkSubnet
- Get-CsNetworkSubnet
- Set-CsNetworkSubnet
- Remove-CsNetworkSubnet

Tip:

If you are working with a large number of subnets, we recommend using a comma-separated values (CSV) file to associate the subnets to sites. The CSV file must have the following four columns: **IPAddress**, **mask**, **description**, **NetworkSiteID**.

To associate a subnet with a network site by using Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the **New-CsNetworkSubnet** cmdlet to associate a subnet with a network site:

```
New-CsNetworkSubnet -SubnetID <String> -MaskBits <Int32> -NetworkSiteI
```

For example:

```
New-CsNetworkSubnet -SubnetID 172.11.12.13 - MaskBits 20 -NetworkSiteI
```

In this example, you created an association between the subnet 172.11.12.13 and the network site “Chicago”.

3. Repeat step 2 for all subnets in your topology.

⊟To associate subnets with network sites by importing a CSV file

1. Create a CSV file that includes all of the subnets you want to add. For example, create a file named **subnet.csv** with the following content:
```
IPAddress, mask, description, NetworkSiteID
172.11.12.0, 24, "NA:Subnet in Portland", Portland
172.11.13.0, 24, "NA:Subnet in Reno", Reno
172.11.14.0, 25, "EMEA:Subnet in Warsaw", Warsaw
172.11.15.0, 31, "EMEA:Subnet in Paris", Paris
```
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run the following cmdlet to import **subnet.csv**, and then store its contents in the Lync Server management store:
```
import-csv subnet.csv | foreach {New-CSNCSSubnet  _.IPAddress -MaskBit
```

⊟To associate a subnet with a network site by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Subnet** navigation button.
4. Click **New**.
5. On the **New Subnet** page, click **Subnet ID**, and then type the first address in the IP address range defined by the subnet you want to associate with a network site.
6. Click **Mask**, and then type the bitmask to apply to the subnet.
7. Click **Network site ID**, and then select the site ID of the site to which you are adding this subnet.

> **Note:**
> If you have not yet created network sites, this list will be empty. For details about the procedure, see Create or Modify a Network Site. You can also retrieve site IDs for your deployment by running the **Get-CsNetworkSite** cmdlet. For details, see the Lync Server Management Shell documentation.

8. Optionally, click **Description**, and then type additional information to describe this subnet.
9. Click **Commit**.

Repeat these steps to add other subnets to a network site.

1.4.3.12.5 Configure Call Admission Control

Configure Call Admission Control

Deployment > Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features >

Topic Last Modified: *2012-09-21*

Call admission control (CAC) is a solution that determines whether a real-time session can be established based on the available bandwidth to help prevent poor audio/video quality for users on congested networks. CAC controls real-time traffic only for audio and video, and does not affect data traffic. CAC may route the call through an Internet path when the default WAN path does not have the required bandwidth. For details, see Planning for Call Admission Control in the Planning documentation.

This section provides a set of example procedures that illustrate how to deploy and manage CAC in your network.

Important:

Before you deploy CAC, you must gather all of the required information for your enterprise network topology, as described in Example: Gathering Your Organization's Requirements for Call Admission Control in the Planning documentation. Also be sure that CAC components have been installed and activated, as described in Define and Configure a Front End Pool or Standard Edition Server in the Deployment documentation.

Note:

All CAC deployment and management examples in this section are performed by using the Lync Server Management Shell. As an alternative, you can also use the **Network Configuration** section of Lync Server Control Panel to manage CAC.

- Configure Network Regions for CAC
- Create Bandwidth Policy Profiles
- Configure Network Sites for CAC
- Associate Subnets with Network Sites for CAC
- Create Network Region Links
- Create Network Interregion Routes
- Create Network Intersite Policies
- Enable Call Admission Control
- Call Admission Control Deployment Checklist

1.4.3.12.5.1 Configure Network Regions for CAC

Configure Network Regions for CAC

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Call Admission Control >

Topic Last Modified: *2012-09-21*

Important:

If you have already created network regions for E9-1-1 or media bypass, you can modify the existing network regions by adding settings specific to call admission control (CAC) by using the **Set-CsNetworkRegion** cmdlet. For an example of how to modify a network region, see Create or Modify a Network Region.

Network regions are the network hubs or backbones that are used in configuring CAC, E9-1-1, and media bypass. Use the following procedure to create network regions that align to network regions in the example network topology for CAC. To view the example network topology, see Example: Gathering Your Organization's Requirements for Call Admission Control in the Planning documentation.

The example network topology for CAC has three regions: North America, EMEA, and APAC. Each region has a specified central site. For the North America region, the designated central site is named CHICAGO. The following procedure shows an example of how you can use the **New-CsNetworkRegion** cmdlet to create the North America region.

Note:

In the following procedure, Lync Server Management Shell is used to create a network region. For details about using Lync Server Control Panel to create a network region, see Create or Modify a Network Region.

To create a network region for call admission control

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. For each region that you need to create, run the **New-CsNetworkRegion** cmdlet. For example, to create the North America region, run:

   ```
   New-CsNetworkRegion -Identity NorthAmerica -CentralSite CHICAGO -Descr
   ```

3. Repeat step 2 to create the network regions, EMEA and APAC.

1.4.3.12.5.2 Create Bandwidth Policy Profiles

Create Bandwidth Policy Profiles

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Call Admission Control >

***Topic Last Modified:** 2012-10-19*

Bandwidth policies define limitations on bandwidth usage for real-time audio and video modalities. Bandwidth policies are applied to *bandwidth policy profiles*, which can be applied to multiple network sites for call admission control.

For guidelines about what bandwidth limits you should set in your CAC deployment, see Defining Your Organization's Requirements for Call Admission Control in the Planning documentation.

For details about working with bandwidth policies and policy profiles, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsNetworkBandwidthPolicyProfile
- Get-CsNetworkBandwidthPolicyProfile
- Set-CsNetworkBandwidthPolicyProfile
- Remove-CsNetworkBandwidthPolicyProfile

The example policies created in the following procedure set limits for overall audio traffic, individual audio sessions, overall video traffic, and individual video sessions. For example, the 5Mb_Link bandwidth policy profile sets the following limits:

- Audio Limit: 2,000 kbps
- Audio Session Limit: 200 kbps
- Video Limit: 1,400 kbps
- Video Session Limit: 700 kbps

Note:

The minimum Audio Session Limit value is 40 kbps. The minimum Video Session Limit value is 100 kbps.

To create bandwidth policy profiles by using Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. For each bandwidth policy profile that you want to create, run the New-CsNetworkBandwidthPolicyProfile cmdlet. For example, run:

```
New-CsNetworkBandwidthPolicyProfile -Identity 5Mb_Link -Description "B
```

```
New-CsNetworkBandwidthPolicyProfile -Identity 10Mb_Link -Description "
```

```
New-CsNetworkBandwidthPolicyProfile -Identity 50Mb_Link -Description "
```

```
New-CsNetworkBandwidthPolicyProfile -Identity 25Mb_Link -Description "
```

To create bandwidth policy profiles by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Policy Profile** navigation button.
4. Click **New**.
5. On the **New Policy Profile** page, click **Name** and then type a name for the bandwidth policy profile.
6. Click **Audio limit**, and then type in the maximum number of kbps to allow for all audio sessions combined.
7. Click **Audio session limit**, and then type in the maximum number of kbps to allow for each individual audio session.
8. Click **Video limit**, and then type in the maximum number of kbps to allow for all video sessions combined.
9. Click **Video session limit**, and then type in the maximum number of kbps to allow for each individual video session.
10. Optionally, click **Description**, and then type additional information to describe this bandwidth policy profile.
11. Click **Commit**.
12. To finish creating bandwidth policy profiles for your topology, repeat steps 4 through 11 with settings for other bandwidth policy profiles.

1.4.3.12.5.3 Configure Network Sites for CAC

Configure Network Sites for CAC

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Call Admission Control >

Topic Last Modified: *2012-09-05*

Important:

If you have already created network sites for E9-1-1 or media bypass, you can modify the existing network sites to apply a bandwidth policy profile by using the **Set-CsNetworkSite** cmdlet. For an example of how to modify a network site, see Create or Modify a Network Site.

Network sites are the offices or locations within each network region of call admission control (CAC), E9-1-1, and media bypass deployments. Use the following procedures to create network sites that align to network sites in the example network topology for CAC. These procedures show how to create and configure network sites that are constrained by WAN bandwidth and therefore require bandwidth policies that limit real-time audio or video traffic flow.

In the example CAC deployment, the North America region has six sites. Three of these sites are constrained by WAN bandwidth: Reno, Portland, and Albuquerque. The other three sites, which are *not* constrained by WAN bandwidth: New York, Chicago, and Detroit. For an example of how to create or modify those other network sites, see Create or Modify a Network Site.

To view the example network topology, see Example: Gathering Your Organization's Requirements for Call Admission Control in the Planning documentation.

Note:
In the following procedure, Lync Server Management Shell is used to create a network site. For details about using Lync Server Control Panel to create a network site, see Create or Modify a Network Site.

To create network sites for call admission control

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the **New-CsNetworkSite** cmdlet to create network sites and apply an appropriate bandwidth policy profile to each site. For example, run:

   ```
   New-CsNetworkSite -NetworkSiteID Reno -Description "NA:Branch office f
   ```

   ```
   New-CsNetworkSite -NetworkSiteID Portland -Description "NA:Branch offi
   ```

   ```
   New-CsNetworkSite -NetworkSiteID Albuquerque -Description "NA:Branch o
   ```

3. To finish creating network sites for the entire example topology, repeat step 2 for the bandwidth-constrained network sites in the EMEA and APAC regions.

1.4.3.12.5.4 Associate Subnets with Network Sites for CAC

Associate Subnets with Network Sites for CAC

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Call Admission Control >

Topic Last Modified: *2012-10-20*

Every subnet in your network must be associated with a specific network site. This is because subnet information is used to determine the network site on which an endpoint is located. When the locations of both parties in a session are known, call admission control (CAC) can determine if there is sufficient bandwidth to establish a call.

Call admission control does not have any special requirements for associating subnets with network sites. To create an association between the subnets and network sites in your topology, follow the procedures in Associate a Subnet with a Network Site. To view the network sites (and their respective subnets) in the example network topology for call admission control, see Example: Gathering Your Organization's Requirements for Call Admission Control in the Planning documentation.

1.4.3.12.5.5 Create Network Region Links

Create Network Region Links

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Call Admission Control >

Topic Last Modified: *2012-10-19*

Regions within a network are linked through physical WAN connectivity. A *network region link* creates a link between two regions configured for call admission control (CAC) and sets the bandwidth limitations on audio and video traffic between these regions.

For details about working with network region links, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsNetworkRegionLink
- Get-CsNetworkRegionLink
- Set-CsNetworkRegionLink
- Remove-CsNetworkRegionLink

The example topology has a link between the North America and APAC regions, and a link between the EMEA and APAC regions. Each of these region links is constrained by WAN bandwidth, as described in Region Link Bandwidth Information table in the Example: Gathering Your Organization's Requirements for Call Admission Control section of the Planning documentation.

To create network region links by using Lync Server Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the New-CsNetworkRegionLink cmdlet to create the region links and apply appropriate bandwidth policy profiles. For example, run:

```
New-CsNetworkRegionLink -NetworkRegionLinkID NA-EMEA-LINK -NetworkRegi
```

```
New-CsNetworkRegionLink -NetworkRegionLinkID EMEA-APAC-LINK -NetworkRe
```

To create network region links by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Region Link** navigation button.
4. Click **New**.
5. On the **New Region Link** page, click **Name** and then type a name for the network region link.
6. Click **Network Region #1**, and then click the network region in the list that you want to link to Network Region #2.
7. Click **Network Region #2**, and then click a network region in the list that you want to link to Network Region #1.
8. Optionally, click **Bandwidth policy**, and then select the bandwidth policy profile that you want to apply to the network region link.

> **Note:**
> Apply a bandwidth policy only if the network region link is bandwidth-constrained and you want to use CAC to control media traffic on that link.

9. Click **Commit**.
10. To finish creating network region links for your topology, repeat steps 4 through 9 with settings for other regions.

1.4.3.12.5.6 Create Network Interregion Routes

Create Network Interregion Routes

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Call Admission Control >

Topic Last Modified: *2012-10-20*

A *network interregion route* defines the route between a pair of network regions. Each pair of network regions in your call admission control deployment requires a network interregion route. This enables every network region within the deployment to access every other region.

While region links set bandwidth limitations on the connections between regions, an interregion route determines which linked path the connection will traverse from one region to another.

For details about working with network interregion routes, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsNetworkInterRegionRoute
- Get-CsNetworkInterRegionRoute
- Set-CsNetworkInterRegionRoute
- Remove-CsNetworkInterRegionRoute

In the example topology, network interregion routes must be defined for each of the three region pairs: North America/EMEA, EMEA/APAC, and North America/APAC.

⊟To create network interregion routes by using Lync Server Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the **New-CsNetworkInterRegionRoute** cmdlet to define the required routes. For example, run:

```
New-CsNetworkInterRegionRoute -Identity NorthAmerica_EMEA_Route -Netwo
```

```
New-CsNetworkInterRegionRoute -Identity NorthAmerica_APAC_Route -Netwo
```

```
New-CsNetworkInterRegionRoute -Identity EMEA_APAC_Route -NetworkRegion
```

Note:

The North America/APAC network interregion route requires two network region links because there is no direct network region link between them.

⊟To create network interregion routes by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Region Route** navigation button.
4. Click **New**.
5. On the **New Region Route** page, click **Name** and then type a name for the network interregion route.
6. Click **Network Region #1**, and then click a network region in the list that you want to route to Network Region #2.
7. Click **Network Region #2**, and then click a network region in the list that you want to route to Network Region #1.
8. Click **Add** beside the **Network Region Links** field, and then add a network region link that will be used in the network interregion route.

Note:

If you are creating a route for two network regions that do not have a direct network region link between them, you must add all the necessary links to complete the route. For example, the North America/APAC network interregion route requires two network region links because there is no direct network region link between them.

9. Click **Commit**.
10. To finish creating network interregion routes for your topology, repeat steps

4 through 9 with settings for other network interregion routes.

1.4.3.12.5.7 Create Network Intersite Policies

Create Network Intersite Policies

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Call Admission Control >

Topic Last Modified: *2012-10-19*

A *network intersite policy* defines bandwidth limitations between sites that have direct WAN links between them.

For details, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsNetworkInterSitePolicy
- Get-CsNetworkInterSitePolicy
- Set-CsNetworkInterSitePolicy
- Remove-CsNetworkInterSitePolicy

Important:

A network intersite policy is required *only* if there is a direct cross link between two network sites.

In the example topology North America region, there is a direct link between the Reno and Albuquerque sites. These two sites require an intersite policy that applies an appropriate bandwidth policy profile. The following example applies the 20Mb_Link profile.

To create a network intersite policy

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the New-CsNetworkInterSitePolicy cmdlet to create network intersite policies and apply an appropriate bandwidth policy profile for two sites that have a direct cross link. For example, run:

```
New-CsNetworkInterSitePolicy -InterNetworkSitePolicyID Reno_Albuquerqu
```

3. Repeat step 2 as needed to create network intersite policies for all network sites pairs that have a direct cross link.

1.4.3.12.5.8 Enable Call Admission Control

Enable Call Admission Control

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Call Admission Control >

Topic Last Modified: *2012-10-19*

After you have configured your network settings for call admission control deployment, you must enable CAC to put your bandwidth policies into effect.

For details, see the Lync Server Management Shell documentation for the following cmdlets:

- Get-CsNetworkConfiguration
- Set-CsNetworkConfiguration
- Remove-CsNetworkConfiguration

To enable call admission control by using Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the Set-CsNetworkConfiguration cmdlet to enable CAC in your network. For example, run:

   ```
   Set-CsNetworkConfiguration -EnableBandwidthPolicyCheck 1
   ```

   If you want to disable CAC in your network, run the following:

   ```
   Set-CsNetworkConfiguration -EnableBandwidthPolicyCheck 0
   ```

To enable call admission control by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Click the **Global** navigation button.
4. Click **Global** in the list, and then select **Show Details** on the **Edit** menu.
5. On the **Edit Global Settings** page, select the **Enable call admission control** check box.

   Note:
   If you want to disable call admission control throughout your deployment, clear this check box.

6. Click **Commit**.

1.4.3.12.5.9 Call Admission Control Deployment Checklist

Call Admission Control Deployment Checklist

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Call Admission Control >

Topic Last Modified: *2012-10-22*

Use the following checklist to verify that you have completed all the necessary configuration tasks to deploy call admission control (CAC).

- If one or more Edge Servers are deployed, each external interface IP address must be added to the subnet list in the network configuration settings, with a bit mask of 32. You should also associate this subnet (IP address) with the network site ID for the geographic location where the A/V Edge service is deployed.

  Note:
  Edge servers are not required to implement CAC.

- Make sure that CAC is enabled, either through Lync Server Control Panel or by running the cmdlet as specified in Enable Call Admission Control.
- Make sure that CAC is enabled in all central sites. This can be done through the Topology Builder. If a warning is generated when you publish, *do not* ignore it.
- Make sure that all the subnets that are managed in the enterprise network are configured in the network configuration settings. It is also essential that every subnet be associated to a network site, as explained in Associate a Subnet with a Network Site.

- Make sure that the subnet or IP addresses of all Front End Servers, Survivable Branch Appliances (SBAs), Audio/Video Conferencing Servers (if in a separate pool), and Mediation Servers are configured in the network configuration settings.

1.4.3.12.6 Configure Enhanced 9-1-1

Configure Enhanced 9-1-1

Deployment > Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features >

Topic Last Modified: *2013-02-24*

Enhanced 9-1-1 (E9-1-1) is an emergency notification feature that associates the calling party's telephone number with a civic or a street address. Using this information, the Public Safety Answering Point (PSAP) can immediately dispatch emergency services to the caller in distress.

To support E9-1-1, Lync Server 2013 must be able to correctly associate a location with a client and to make sure that this information is used to route the emergency call to the nearest PSAP.

For details about planning for an E9-1-1 deployment, see Planning for Emergency Services (E9-1-1).

◆Important:

Lync Server 2013 only supports E9-1-1 within the United States. To deploy E9-1-1, you need to configure a SIP connection to a qualified E9-1-1 service provider, or deploy an emergency location identification number (ELIN) gateway to a public switched telephone (PSTN)-based E9-1-1 service provider. For details, see Enhanced 9-1-1 (E9-1-1) and Mediation Server. For details about configuring trunk connections, see Configure a Trunk with Media Bypass.

- Configure an E9-1-1 Voice Route
- Create Location Policies
- Configure Site Information for E9-1-1
- Configure the Location Database
- Configure Advanced E9-1-1 Features

1.4.3.12.6.1 Configure an E9-1-1 Voice Route

Configure an E9-1-1 Voice Route

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 >

Topic Last Modified: *2012-09-17*

To deploy E9-1-1, you first need to configure an emergency call voice route. For details about creating voice routes, see Create a Voice Route. You may define more than one route if, for example, your deployment includes a primary SIP trunk and a secondary SIP trunk.

Note:

To include location information in an E9-1-1 INVITE, you need to configure the SIP trunk that connects to the E9-1-1 service provider to route emergency calls through the gateway. To do this, set the EnablePIDFLOSupport flag on the **Set-CsTrunkConfiguration** cmdlet to True. The default value for EnablePIDFLOSupport is False. For example: `Set-CsTrunkConfiguration`

```
Service:PstnGateway:192.168.0.241 -EnablePIDFLOSupport $true.
```

It is not necessary to enable receiving locations for fallback public switched telephone network (PSTN) gateways and Emergency Location Identification Number (ELIN) gateways.

For details about working with voice routes, see the Lync Server Management Shell documentation for the following cmdlets:

- **Set-CsPstnUsage**
- **Get-CsPstnUsage**
- **New-CsVoiceRoute**
- **Get-CsVoiceRoute**
- **Set-CsVoiceRoute**
- **Remove-CsVoiceRoute**

To configure an E9-1-1 voice route

1. Log on to the computer with an account that is a member of the RTCUniversalServerAdmins groups, or a member of the CsVoiceAdministrator administrative role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run the following cmdlet to create a new PSTN usage record.

   This must be the same name that you will use for the **PSTN** setting in the location policy. Although your deployment will have multiple phone usage records, the following example adds "Emergency Usage" to the current list of available PSTN usages. For details, see Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges.

   ```
   Set-CsPstnUsage -Usage @{add='EmergencyUsage'}
   ```

4. Run the following cmdlet to create a new voice route by using the PSTN usage record that you created in the previous step.

   The number pattern must be the same number pattern that is used in the **Emergency Dial String** setting in the location policy. A "+" sign is needed because Lync adds "+" to emergency calls. "Co1-pstngateway-1" is the SIP trunk service ID for the E9-1-1 service provider or for the ELIN gateway service ID. The following example uses "EmergencyRoute" as the name of the voice route.

   ```
   New-CsVoiceRoute -Name "EmergencyRoute" -NumberPattern "^\+911$" -Pstn
   ```

5. Optionally, for SIP trunk connections, we recommend that you run the following cmdlet to create a local route for calls that are not handled by the E9-1-1 service provider's SIP trunk. This route will be used if the connection to the E9-1-1 service provider is not available.

   The following example assumes that user has "Local" usage in their voice policy.

   ```
   New-CsVoiceRoute -Name "LocalEmergencyRoute" -NumberPattern "^\+911$"
   ```

1.4.3.12.6.2 Create Location Policies

Create Location Policies

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 >

Topic Last Modified: *2012-09-11*

Lync Server uses a location policy to enable Lync clients for E9-1-1 during client registration. A location policy contains the settings that define how E9-1-1 will be implemented.

You can edit the global location policy and create new tagged location policies. A client obtains a global policy when it is not located within a subnet with an associated location policy, or when the client has not been directly assigned a location policy. Tagged policies are assigned to subnets or users.

To create a location policy, you must use an account that is a member of the RTCUniversalServerAdmins group, or is a member of the CsVoiceAdministrator administrative role, or has equivalent administrator rights and permissions.

For a complete description of Location policies, see Defining the Location Policy. Cmdlets in this procedure use a location policy defined using the following values:

Element	Value
EnhancedEmergencyServicesEnabled	**True**
LocationRequired	**Disclaimer**
EnhancedEmergencyServiceDisclaimer	Your company policy requires you to set a location. If you do not set a location, emergency services will not be able to locate you in an emergency. Please set a location.
UseLocationForE911Only	**False**
PstnUsage	**EmergencyUsage**
EmergencyDialString	**911**
EmergencyDialMask	**112**
NotificationUri	**sip:security@litwareinc.com**
ConferenceUri	**sip:+14255550123@litwareinc.com**
ConferenceMode	**twoway**
LocationRefreshInterval	**2**

For details about working with location policies, see the Lync Server Management Shell documentation for the following cmdlets:

- New-CsLocationPolicy
- Get-CsLocationPolicy
- Set-CsLocationPolicy
- Remove-CsLocationPolicy
- Grant-CsLocationPolicy

To create location policies

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

Note:
CsLocationPolicy will fail if the setting for **PstnUsage** is not already in the Global list of PstnUsages.

2. Optionally, run the following cmdlet to edit the global Location Policy:

   ```
   Set-CsLocationPolicy -Identity Global -EnhancedEmergencyServicesEnable
   ```

3. Run the following to create a tagged Location Policy.

   ```
   New-CsLocationPolicy -Identity Tag:Redmond - EnhancedEmergencyServices
   ```

4. Run the following cmdlet to apply the tagged Location Policy created in step 3 to a user policy.

   ```
   (Get-CsUser | where { $_.Name -match "UserName" }) | Grant-CsLocationP
   ```

1.4.3.12.6.3 Configure Site Information for E9-1-1

Configure Site Information for E9-1-1

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 >

Topic Last Modified: *2012-10-03*

To define a location policy for subnets, you must do the following, in any order:

- Apply a location policy to the network site.
- Add the subnets to the network site.

For details about network sites, see Sites.

Note:
If you create network sites for another voice feature and you want to configure E9-1-1 by using the same sites, then you can modify the sites to be used for E9-1-1.

- Add a Location Policy to a Network Site
- Associate a Subnet with a Network Site

Add a Location Policy to a Network Site

Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 > Configure Site Information for E9-1-1 >

Topic Last Modified: *2013-02-24*

The following examples show how to add the **Redmond** location policy defined in Create Location Policies to an existing network site and how to create a new network site that uses the **Redmond** location policy.

For details about working with network sites, see the Lync Server Management Shell documentation for the following cmdlets:

- **New-CsNetworkSite**
- **Get-CsNetworkSite**
- **Set-CsNetworkSite**
- **Remove-CsNetworkSite**

To assign a location policy to an existing network site

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the following cmdlets to modify an existing network site.

   Assign the **Redmond** tagged Location policy to an existing network site named **Redmond**.

   ```
   Set-CsNetworkSite -Identity "Redmond" -NetworkRegionID "NorthAmerica"
   ```

To assign a location policy to a new network site

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the following cmdlet to create a new network site.

   Create a new network site in the network region and assign the **Redmond** tagged Location policy.

   ```
   New-CsNetworkSite -Identity "Redmond" -NetworkRegionID "NorthAmerica"
   ```

Associate Subnets with Network Sites for E9-1-1

Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 > Configure Site Information for E9-1-1 >

Topic Last Modified: *2012-10-02*

Every subnet in your network that you want to enable for E9-1-1 must be associated with a specific network site. This is because subnet information is used to determine the network site on which an endpoint is located.

E9-1-1 does not have any special requirements for associating subnets with network sites. To create an association between the subnets and network sites in your topology, follow the procedures in Associate a Subnet with a Network Site.

1.4.3.12.6.4 Configure the Location Database

Configure the Location Database

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 >

Topic Last Modified: *2012-09-17*

To enable clients to automatically detect their location within a network, you first need to configure the location database. If you do not configure a location database, and **Location Required** in the location policy is set to **Yes** or **Disclaimer**, the user will be prompted to manually enter a location.

To configure the location database, you will perform the following tasks:

1. Populate the database with a mapping of network elements to locations. If you use an Emergency Location Identification Number (ELIN) gateway, you need to include the ELIN in the <CompanyName> field.
2. Validate the addresses against the master street address guide (MSAG) that is maintained by the E9-1-1 service provider.
3. Publish the updated database.

> **Note:**
>
> Alternately, you can define a secondary location source database that can be used in placed of the location database. For details, see Configure a Secondary Location Information Service.

- Populate the Location Database
- Validate Addresses
- Publish the Location Database

Populate the Location Database

Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 > Configure the Location Database >

Topic Last Modified: *2012-09-17*

To automatically locate clients within a network, you first need to populate the location database with a network *wiremap*, which maps network elements to civic (that is, street) addresses. You can use subnets, wireless access points, switches, and ports to define the wiremap.

You can add addresses to the location database individually, or in bulk by using a CSV file that contains the column formats described in the following table.

If you use an Emergency Location Identification Number (ELIN) gateway, include the ELIN in the **CompanyName** field for each location. You can include multiple ELINs for each location, each separated by a semicolon.

Network Element	Required Columns
Wireless access point	<BSSID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,… …<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
Subnet	<Subnet>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,… …<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
Port	<ChassisID>,<PortIDSubType>,<PortID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,… …<PreDirectional>,<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
Switch	<ChassisID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,… …<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>

If you do not populate the location database, and the **Location Required** in the Location Policy is set to **Yes** or **Disclaimer**, the client will prompt the user to enter a location manually.

For details about populating the location database, see the Lync Server Management Shell documentation for the following cmdlets:

- **Get-CsLisSubnet**
- **Set-CsLisSubnet**
- Remove-CsLisSubnet
- **Get-CsLisWirelessAccessPoint**
- **Set-CsLisWirelessAccessPoint**
- **Remove-CsLisWirelessAccessPoint**
- **Get-CsLisSwitch**
- **Set-CsLisSwitch**
- **Remove-CsLisSwitch**
- **Get-CsLisPort**
- **Set-CsLisPort**
- **Remove-CsLisPort**

To add network elements to the location database

1. Run the following cmdlet to add a subnet location to the location database.

   ```
   Set-CsLisSubnet -Subnet 157.56.66.0 -Description "Subnet 1" -Location
   ```

   For ELIN gateways, put the ELIN in the CompanyName field. You can include more than one ELIN. For example:

   ```
   Set-CsLisSubnet -Subnet 157.56.66.0 -Description "Subnet 1" -Location
   ```

   Alternately, you can run the following cmdlets and use a file named "subnets.csv" to bulk update subnet locations.

   ```
   $g = Import-Csv subnets.csv
   $g | Set-CsLisSubnet
   ```

2. Run the following cmdlet to add wireless locations to the location database.

   ```
   Set-CsLisWirelessAccessPoint -BSSID 0A-23-CD-16-AA-2E -Description "Wi
   ```

   Alternately, you can run the following cmdlets and use a file named "waps.csv" to bulk update wireless locations.

   ```
   $g = Import-Csv waps.csv
   $g | Set-CsLisWirelessAccessPoint
   ```

3. Run the following cmdlet to add switch locations to the location database.

   ```
   Set-CsLisSwitch-ChassisID 0B-23-CD-16-AA-BB -Description "Switch1" -Lo
   ```

   Alternately, you can run the following cmdlets and use a file named "switches.csv" to bulk update switch locations.

   ```
   $g = Import-Csv switches.csv
   $g | Set-CsLisSwitch
   ```

4. Run the following cmdlet to add port locations to the location database

   ```
   Set-CsLisPort -ChassisID 0C-23-CD-16-AA-CC -PortID 0A-abcd -Descriptio
   ```

   The default for PortIDSubType is LocallyAssigned. You can also set it to InterfaceAlias or InterfaceName

   Alternately, you can run the following cmdlets and use a file named "ports.csv" to bulk update port locations.

   ```
   $g = Import-Csv ports.csv

   $g | Set-CsLisPort
   ```

Validate Addresses

Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 > Configure the Location Database >

Topic Last Modified: *2012-09-17*

Before publishing the location database, you must validate new locations against the Master Street Address Guide (MSAG) that is maintained by your SIP trunk or public switched telephone network (PSTN) E9-1-1 service provider.

For details about SIP trunk E9-1-1 service providers, see Choosing an E9-1-1 Service Provider.

For details about validating addresses, see the Lync Server Management Shell documentation for the following cmdlets:

- **Get-CsLisServiceProvider**
- **Set-CsLisServiceProvider**
- **Remove-CsLisServiceProvider**
- **Get-CsLisCivicAddress**
- **Test-CsLisCivicAddress**

To validate addresses located in the location database

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the following cmdlets to configure the emergency service provider connection.

```
$pwd = Read-Host -AsSecureString <password>
Set-CsLisServiceProvider -ServiceProviderName Provider1 -ValidationSer
```

3. Run the following cmdlet to validate the addresses in the location database.

```
Get-CsLisCivicAddress | Test-CsLisCivicAddress -UpdateValidationStatus
```

You can also use the **Test-CsLisCivicAddress** cmdlet to validate individual addresses.

Publish the Location Database

Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 > Configure the Location Database >

Topic Last Modified: *2012-10-30*

The new locations that you added to the location database will not be made available to the client until they have been published.

For details, see the Lync Server Management Shell documentation for the following cmdlet:

- **Publish-CsLisConfiguration**

If you use Emergency Location Identification Number (ELIN) gateways, you also need to upload the ELINs to your public switched telephone network (PSTN) carrier's Automatic Location Identification (ALI) database. Your PSTN carrier may require you to use a specific format for the ELIN records. Contact your PSTN carrier for details. You can export the records from the Location Information service database and format them as required.

To publish the location database

- Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
- Run the following cmdlet to publish the location database.

```
Publish-CsLisConfiguration
```

Configure Advanced E9-1-1 Features

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 >

Topic Last Modified: *2012-06-06*

Lync Server 2013 includes the following features that you can use to customize your E9-1-1 deployment:

- A web service interface to connect the Location Information Server to an SNMP application.
- A web service interface to connect to a Secondary Location Source database.
- Configure an SNMP Application
- Configure a Secondary Location Information Service

Configure an SNMP Application

Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 > Configure Advanced E9-1-1 Features >

Topic Last Modified: *2012-10-03*

Lync Server 2013 includes a standard web service interface that you can use to connect the Location Information service to Simple Network Management Protocol (SNMP) applications that match MAC addresses with port and switch information.

If an SNMP application is installed and the Location Information service fails to find a match in the location database, the Location Information service automatically queries the application by using the MAC address provided by the client. The Location Information service then uses the port and switch information returned by the SNMP application to query the location database again.

For details, see Set-CsWebServiceConfiguration.

Note:

MAC addresses are not available on computers running Windows 8.

⊟To configure the SNMP application URL

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the following cmdlet to configure the URL for the SNMP application.

```
Set-CsWebServiceConfiguration -MACResolverUrl "<SNMP application url>"
```

Configure a Secondary Location Information Service

Deploying Advanced Enterprise Voice Features > Configure Enhanced 9-1-1 > Configure Advanced E9-1-1 Features >

Topic Last Modified: *2012-10-30*

Lync Server 2013 provides a web service interface that you can use to point the Location Information service to a Secondary Location Source (SLS) database. The web service interface that connects to the SLS database must conform to Location Information service

WSDL. If both a location database and secondary location database are configured, the Location Information service first queries the location database, and if no match is found, sends the location request from the client to the SLS database. If the location exists in the SLS, the Location Information service then sends the location back to the client.

For details, see the Lync Server Management Shell documentation for the following cmdlet:

- **Set-CsWebServiceConfiguration**

To configure Secondary Location database

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the following cmdlet to configure the URL for the location of the secondary location database.

```
Set-CsWebServiceConfiguration -SecondaryLocationSourceURL "<web servic
```

1.4.3.12.7 Configure Media Bypass

Configure Media Bypass

See Also

Deployment > Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features >

Topic Last Modified: *2013-02-24*

This section assumes that you have already published and configured either at least one or more Mediation Servers (as described in Define a Mediation Server in Topology Builder and Publish the Topology, or in Define and Configure a Front End Pool or Standard Edition Server and Publish the Topology, respectively, all in the Deployment documentation).

This section also assumes that you have defined at least one gateway peer to provide PSTN connectivity, as described in Define a Gateway in Topology Builder. If the peer you connect to is the SBC of a SIP trunking provider, make sure that the provider is a qualified provider and that the provider supports media bypass. For example, many SIP trunking providers will only allow their SBC to receive traffic from the Mediation Server. If so, then bypass must not be enabled for the trunk in question. Also, you cannot enable media bypass unless your organization reveals its internal network IP addresses to the SIP trunking provider.

Note:

Media bypass will not interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed on Unified Communications Open Interoperability Program – Lync Server at http://go.microsoft.com/fwlink/p/?linkId=214406.

This section describes how to enable media bypass to reduce the processing required of the Mediation Server. Before you enable media bypass, make sure that your environment meets the conditions required to support media bypass, as described in Planning for Media Bypass in the Planning documentation. Also make sure that you used the information in Planning for Media Bypass to decide whether to enable media bypass global settings to always bypass the Mediation Server or to use site and region information when determining whether to bypass the Mediation Server.

If you have already optionally configured call admission control (CAC), another advanced Enterprise Voice feature, note that the bandwidth reservation performed by call admission control does not apply to any calls for which media bypass is employed. The verification of whether to employ media bypass is performed first, and if media bypass is employed, call admission control is not used for the call; only if the media bypass check fails is the check performed for call admission control. The two features are thus mutually exclusive for any particular call that is routed to the PSTN. This is the logic because media bypass assumes that bandwidth constraints do not exist between the media endpoints on a call; media bypass cannot be performed on links with restricted bandwidth. As a result, one of the following will apply to a PSTN call: a) media bypasses the Mediation Server, and call admission control does not reserve bandwidth for the call; or b) call admission control applies bandwidth reservation to the call, and media is processed by the Mediation Server involved in the call.

Next Steps: Enable Media Bypass on the Trunk Connection

After configuring initial settings for PSTN connectivity (dial plans, voice policies, PSTN usage records, outbound call routes, and translation rules), begin the process of enabling media bypass by using the steps in Configure a Trunk with Media Bypass.

⊟See Also

Tasks

Configure a Trunk with Media Bypass
Configure Media Bypass to Always Bypass the Mediation Server
Configure Media Bypass Global Settings to Use Site and Region Information

Concepts

Global Media Bypass Options

Other Resources

Planning for Media Bypass

1.4.3.12.7.1 Configure a Trunk with Media Bypass

Configure a Trunk with Media Bypass

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2013-02-24*

Follow these steps to configure a trunk with media bypass enabled. To configure a trunk with media bypass disabled, see Configure a Trunk without Media Bypass.

We strongly recommend that you enable media bypass. However, before you enable media bypass on a SIP trunk, confirm that your qualified SIP trunk provider supports media bypass and is able to accommodate the requirements for successfully enabling the scenario. Specifically, the provider must have the IP addresses of servers in your organization’s internal network. If the provider cannot support this scenario, media bypass will not succeed. For details, see Planning for Media Bypass in the Planning documentation.

> **Note:**
> Media bypass will not interoperate with every public switched telephone network (PSTN) gateway, IP-PBX, and Session Border Controller (SBC). Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions that are listed on

Unified Communications Open Interoperability Program – Lync Server at http://go.microsoft.com/fwlink/p/?linkId=214406.

A trunk configuration as described below groups a set of parameters that are applied to trunks assigned this trunk configuration. A particular trunk configuration can be scoped globally (to all trunks that do not have more specific site or pool configuration), or to a site, or to a pool. The pool-level trunk configuration is used to scope a specific trunk configuration to a single trunk.

⊟To configure a trunk with media bypass

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
4. On the **Trunk Configuration** page, use one of the following methods to configure a trunk:
   - Double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
   - Click **New**, and then select a scope for the new trunk configuration:
     - **Site trunk:** Choose the site for this trunk configuration from **Select a Site**, and then click **OK**. Note that if a trunk configuration has already been created for a site, the site does not appear in **Select a Site**. This trunk configuration will be applied to all trunks in the site.
     - **Pool trunk:** Choose the name of the trunk that this trunk configuration applies to. This trunk can be the root trunk or any additional trunks defined in Topology Builder. From **Select a Service**, click **OK**. Note that if a trunk configuration has already been created for a specific trunk, the trunk does not appear in **Select a Service**.

   Note:
   After you select the scope of the trunk configuration, it cannot be changed. The **Name** field is prepopulated with the name of the trunk configuration's associated site or service and cannot be changed.

5. Specify a value in **Maximum early dialogs supported**. This is the maximum number of forked responses a public switched telephone network (PSTN) gateway, IP-PBX, or ITSP Session Border Controller (SBC) can receive to an INVITE that it sent to the Mediation Server. The default value is 20.

   Note:
   Before you change this value, consult your service provider or equipment manufacturer for details about the capabilities of your system.

6. Select one of the following **Encryption support level** options:
   - **Required:** Secure real-time transport protocol (SRTP) encryption must be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
   - **Optional:** SRTP encryption will be used if the service provider or equipment manufacturer supports it.
   - **Not Supported:** SRTP encryption is not supported by the service provider or equipment manufacturer and therefore will not be used.
7. Select the **Enable media bypass** check box if you want media to bypass the Mediation Server for processing by the trunk peer.

   Important:
   For media bypass to work successfully, the PSTN gateway, IP-PBX, or ITSP

> Session Border Controller must support certain capabilities. For details, see Planning for Media Bypass in the Planning documentation.

8. Select the **Centralized media processing** check box if there is a well-known media termination point (for example, a PSTN gateway where the media termination has the same IP as the signaling termination). Clear this check box if the trunk does not have a well-known media termination point.
9. If the trunk peer supports receiving SIP REFER requests from the Mediation Server, select the **Enable sending refer to the gateway** check box.

> **Note:**
>
> If you disable this option while the **Enable media bypass** option is selected, additional settings are required. If the trunk peer does not support receiving SIP REFER requests from the Mediation Server and media bypass is enabled, you must also run the **Set-CsTrunkConfiguration** cmdlet to disable RTCP for active and held calls in order to support proper conditions for media bypass. For details, see the Lync Server Management Shell documentation. Alternatively, you can select **Enable refer using third-party-call control** if you want transferred calls to be media bypassed, and the gateway does not support SIP REFER requests.

10. (Optional) To enable inter-trunk routing, associate and configure PSTN usage records to this trunk configuration. The PSTN usages associated to this trunk configuration will be applied for all incoming calls through the trunk that is not originating from a Lync endpoint. To manage PSTN usage records associated to a trunk configuration, use one of the following methods:
    - To select one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records you want to associate with this trunk configuration and then click **OK**.
    - To remove a PSTN usage record from this trunk configuration, select the record and click **Remove**.
    - To define a new PSTN usage record and associate it with this trunk configuration, do the following:
        - Click **New**.
        - In the **Name** field, specify a descriptive name for the record that is unique.

        > **Note:**
        >
        > The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

        - Use one of the following methods to associate and configure routes for this PSTN usage record:
            - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
            - To remove a route from the PSTN usage record, select the route, and click **Remove**.
            - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
            - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
        - Click **OK**.
    - To edit a PSTN usage record that is already associated with this trunk configuration, do the following:
        - Select the PSTN usage record you want to edit, and click **Show details**.
        - Use one of the following methods to associate and configure routes for this PSTN usage record:
            - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.

  - To remove a route from the PSTN usage record, select the route, and click **Remove**.
  - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
- Click **OK**.

> **◆Important:**
> It important to associate PSTN usage records according to the Mediation Server peer that is associated to the trunk being configured. If the Mediation Server peer is a PSTN gateway or a Session Border Controller (SBC), it is strongly recommended that the trunk configuration is not associated to a PSTN usage record that routes to a PSTN destination or any other downstream systems connected via Lync Server.

11.Arrange the PSTN usage records for optimum performance. To change a record's position in the list, select the PSTN usage record, and click the up or down arrows.

> **◆Important:**
> The order in which PSTN usage records are listed in the trunk configuration is significant. Lync Server traverses the list from top to down.

12.**Enable RTP Latching** should be selected to enable bypass media for clients behind a network address translation (NAT) or firewall and an SBC that supports latching.

13.**Enable forward call history** should be selected to enable sending of call history information to the gateway peer of the Mediation Server.

14.**Enable forward P-Asserted-Identity data** should be selected to enable the P-Asserted-Identity (PAI) call originator information to be forwarded between the Mediation Server side and gateway side (and vice versa), when present.

15.**Enable outbound routing failover timer** should be selected to enable fast failover. The gateway associated with this trunk can give notification within 10 seconds that it is processing an outbound call. Rerouting to another trunk will occur if this notification is not received by the Mediation Server. On networks where latency may delay the response time or the gateway takes longer than 10 seconds to respond, the fast failover should be disabled.

16.(Optional) Associate and configure **calling number translation rules** for the trunk. These translation rules apply to the calling number for outbound calls

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

> **⚠Warning:**
> Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

17.(Optional) Associate and configure **called number translation rules** for the trunk. The translation rules apply to the called number in an outbound call.

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

⚠**Warning:**

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

18.Make sure that the trunk’s translation rules are arranged in the correct order. To change a rule’s position in the list, highlight the rule name and then click the up or down arrow.

Important:

Lync Server 2013 traverses the translation rule list from the top down and uses the first rule that matches the dialed number. If you configure a trunk so that a dialed number can match more than one translation rule, be sure that the more restrictive rules are sorted above the less restrictive rules. For example, if you have included a translation rule that matches any 11-digit number and a translation rule that matches only 11-digit numbers that start with +1425, be sure that the rule that matches any 11-digit number is sorted *below* the more restrictive rule.

19.When you are finished configuring the trunk, click **OK**.

20.On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

Note:

Whenever you create or modify a trunk configuration, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

After you have configured the trunk, continue configuring media bypass by choosing between global media bypass options, as described in Global Media Bypass Options in the Deployment documentation.

Tasks

Configure a Trunk without Media Bypass

Concepts

Configure Media Bypass
Global Media Bypass Options

Other Resources

Defining Translation Rules

Defining Translation Rules

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2013-02-22*

Lync Server 2013 Enterprise Voice routes calls based on phone numbers normalized to E.164 format. This means that all dialed strings must be normalized to E.164 format for the purpose of performing reverse number lookup (RNL) so they can be translated to their matching SIP URI. Lync Server 2013 provides the ability to manipulate the called ID and the caller ID presentation.

This section discusses how to manipulate the called ID and caller ID.

- Caller ID Presentation
- Called ID Presentation

⊟See Also

Other Resources

Defining Normalization Rules

Create or Modify a Translation Rule by Using the Build a Translation Rule Tool

See Also

Configuring Trunks > Defining Translation Rules > Called ID Presentation >

Topic Last Modified: *2012-10-05*

Follow these steps if you want to define a translation rule by entering a set of values in the **Build a Translation Rule** tool and enabling Lync Server Control Panel to generate the corresponding matching pattern and translation rule for you. Alternatively, you can a write regular expression manually to define the matching pattern and translation rule. For details, see Create or Modify a Translation Rule Manually.

⊟To define a rule by using the Build a Translation Rule tool

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. To begin defining a translation rule, follow the steps in Configure a Trunk with Media Bypass through step 10 or Configure a Trunk without Media Bypass through step 9.
4. Under **Name** on the **New Translation Rule** or **Edit Translation Rule** page, type a name that describes the number pattern being translated.
5. (Optional) Under **Description**, type a description of the translation rule, for example **US International long-distance dialing**.
6. In the **Build a Translation Rule** section of the dialog box, enter values in the following fields:
   - **Starting digits**: (Optional) Specify the leading digits of numbers you want the pattern to match. For example, enter **+** in this field to match numbers in E.164 format (which begin with +).
   - **Length**: Specify the number of digits in the matching pattern and select whether you want the pattern to match numbers that are this length exactly, at least this length, or any length. For example, enter **11** and select **At least** in the drop-down list to match numbers that are at least 11 digits in length.
   - **Digits to remove**: (Optional) Specify the number of starting digits to be removed. For example, enter **1** to strip out the **+** from the beginning of the

number.

- **Digits to add**: (Optional) Specify digits to be prepended to the translated numbers. For example, enter **011** if you want 011 to be prepended to the translated numbers when the rule is applied.

The values you enter in these fields are reflected in the **Pattern to match** and **Translation rule** fields. For example, if you specify the preceding example values, the resulting regular expression in the **Pattern to match** field is:

^\+(\d{9}\d+)$

The **Translation rule** field specifies a pattern for the format of translated numbers. This pattern has two parts:

- A value (for example, **$1**) that represents the number of digits in the matching pattern
- (Optional) A value that you can prepend by entering it in the **Digits to add** field

Using the preceding example values, **011$1** appears in the **Translation rule** field.

When this translation rule is applied, +441235551010 becomes 011441235551010.

7. Click **OK** to save the translation rule.
8. Click **OK** to save the trunk configuration.
9. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

Note:

Whenever you create or modify a translation rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Translation Rule Manually
Configure a Trunk with Media Bypass
Configure a Trunk without Media Bypass
Publish Pending Changes to the Voice Routing Configuration

Concepts

Global Media Bypass Options

Create or Modify a Translation Rule Manually

See Also

Configuring Trunks > Defining Translation Rules > Called ID Presentation >

Topic Last Modified: *2012-08-06*

Follow these steps if you want to define a translation rule by writing a regular expression for the matching pattern and translation rule. Alternatively, you can enter a set of values in the **Build a Translation Rule** tool and enable Lync Server Control Panel to generate the corresponding matching pattern and translation rule for you. For details, see Create or Modify a Translation Rule by Using the Build a Translation Rule Tool.

⊟To define a translation rule manually

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. To begin defining a translation rule, follow the steps in Configure a Trunk with

Media Bypass through step 10 or Configure a Trunk without Media Bypass through step 9.

4. In the **Name** field on the **New Translation Rule** or **Edit Translation Rule** page, type a name that describes the number pattern being translated.
5. (Optional) In **Description**, type a description of the translation rule, for example **US International long-distance dialing**.
6. Click **Edit** at the bottom of the **Build a Translation Rule** section.
7. Enter the following in **Type a Regular Expression**:
   - In **Match this pattern**, specify the pattern that will be used to match the numbers to be translated.
   - In **Translation rule**, specify a pattern for the format of translated numbers.

   For example, if you enter **^\+(\d{9}\d+)$** in **Match this pattern** and **011$1** in **Translation rule**, the rule will translate +441235551010 to 011441235551010.
8. Click **OK** to save the translation rule.
9. Click **OK** to save the trunk configuration.
10. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

> **Note:**
> Whenever you create or modify a translation rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Translation Rule by Using the Build a Translation Rule Tool
Configure a Trunk with Media Bypass
Configure a Trunk without Media Bypass
Publish Pending Changes to the Voice Routing Configuration

Concepts

Global Media Bypass Options

1.4.3.12.7.2 Global Media Bypass Options

Global Media Bypass Options

See Also

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configure Media Bypass >

Topic Last Modified: *2012-10-04*

> **Note:**
> This topic assumes that you have already configured media bypass for any trunks to a peer (a public switched telephone network (PSTN) gateway, an IP-PBX, or a Session Border Controller (SBC) at an Internet Telephony Service Provider) for a specific site or service for which you want media to bypass the Mediation Server.

In addition to enabling media bypass for individual trunk connections associated with a peer, you must also enable media bypass globally. Global media bypass settings can either specify that media bypass is always attempted for calls to the PSTN, or that media bypass is employed by using the mapping of subnets to network sites and network regions—similar to what is done by call admission control, another advanced voice feature. When media bypass and call admission control are both enabled, then the network region, network site, and subnet information that is specified for call admission control is automatically used when determining whether to employ media bypass. This means that you cannot specify that media bypass is always attempted for calls to the PSTN when call admission control is enabled.

This topic describes how to use Lync Server Control Panel and Lync Server Management Shell together to configure global media bypass settings.

Note:

When you use these steps to configure media bypass, the assumption is that you have good connectivity between clients and the Mediation Server peer (for example, a PSTN gateway, an IP-PBX, or an SBC at a SIP trunking provider). If there are any bandwidth limitations on the link, media bypass cannot be applied to the call. Media bypass will not interoperate with every PSTN gateway, IP-PBX, and SBC. Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions listed on Unified Communications Open Interoperability Program – Lync Server at http://go.microsoft.com/fwlink/p/?linkId=214406.

Next Steps: Choose Global Media Bypass Settings

After you have enabled media bypass on any trunk connections to a peer for specific sites or services, use the following content to either:

- Enable media bypass always, as described in Configure Media Bypass to Always Bypass the Mediation Server.
- Or, configure media bypass to use site and region information, as described in Configure Media Bypass Global Settings to Use Site and Region Information.

See Also

Tasks

Configure a Trunk with Media Bypass
Associate a Subnet with a Network Site

Concepts

Configure Media Bypass
Media Bypass and Mediation Server

Configure Media Bypass to Always Bypass the Mediation Server

See Also

Deploying Advanced Enterprise Voice Features > Configure Media Bypass > Global Media Bypass Options >

***Topic Last Modified:** 2013-02-25*

Note:

This topic assumes that you have already configured media bypass for any trunk connections to a peer (a public switched telephone network (PSTN) gateway, an IP-PBX, or a Session Border Controller (SBC) at an Internet Telephony Service Provider (ITSP)) for a specific site or service for which you want media to bypass the Mediation Server.
You cannot configure media to always bypass the Mediation Server while also enabling call admission control. These settings are incompatible and are therefore mutually exclusive settings in the Lync Server Control Panel user interface.

In addition to enabling media bypass for individual trunk connections associated with a peer to the Mediation Server, you must also configure global settings for media bypass. If you use the steps in this topic to configure global settings for media bypass, the assumption is that you have good connectivity between Lync endpoints and any peer for which you configured media bypass on the trunk connection.

If you do not have good connectivity between Lync Server endpoints and all peers to the Mediation Server whose respective trunk connections have been enabled for media bypass, you must configure global media bypass settings to use site and region information when employing media bypass. This allows for more control in determining when media bypasses the Mediation Server. To do this, use the steps in Configure Media Bypass Global Settings to Use Site and Region Information and Associate a Subnet with a Network Site instead.

⊟To Enable Media Bypass Globally to Always Bypass the Mediation Server

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Double-click the **Global** configuration in the list.
4. On the **Edit Global Setting** page, select the **Enable media bypass** check box.
5. Click **Always bypass**.
6. Click **Commit**.

Concepts

Configure Media Bypass
Global Media Bypass Options
Media Bypass and Mediation Server

Other Resources

Planning for Media Bypass

Configure Media Bypass Global Settings to Use Site and Region Information

See Also

Deploying Advanced Enterprise Voice Features > Configure Media Bypass > Global Media Bypass Options >

Topic Last Modified: *2012-09-21*

Note:

This topic assumes that you have already configured media bypass for any trunk connections from the Mediation Server to a peer (a public switched telephone network (PSTN) gateway, an IP-PBX, or a Session Border Controller (SBC) at an Internet Telephony Service Provider (ITSP) for a specific site or service for which you want media to bypass the Mediation Server.
This topic also assumes that you have defined all central sites and branch sites in Topology Builder in a way that matches the network region, network site, and subnet configuration that you performed according to the steps in Create or Modify a Network Region, Create or Modify a Network Site, and Associate a Subnet with a Network Site. If they do not match, then media bypass will not succeed.

In addition to enabling media bypass for individual trunk connections associated with a peer, you must also configure global settings. If you use the steps in this topic to configure global settings for media bypass, the assumption is that one or both of the following situations affects your configuration:

- You *do not* have good connectivity between Lync Server endpoints and any peers for which you configured media bypass on the trunk connection.
- Call admission control (CAC) for bandwidth management is enabled.

Note:

For details about the considerations for both call admission control and media bypass, see the "Call Admission Control of PSTN Connections" section in

Media Bypass and Mediation Server in the Planning documentation.

Network region and network site information is shared between call admission control and media bypass advanced Enterprise Voice features when both are enabled. Therefore, if you have already configured call admission control, you are not required to use the following procedure to edit the site and region information specifically for media bypass. Follow the steps in this procedure if you have not yet configured network regions and sites for call admission control, and you want to change media bypass settings.

Or, follow these steps if you want to use site and region information in making the bypass decision, but have no intention of enabling call admission control. In such a case, bandwidth restricted links will still need to be represented through network intersite policies, as described in Create Network Intersite Policies. The actual bandwidth constraints are not as important in this case, because call admission control has not been enabled. Instead, these links are used to partition subnets to specify those that have no bandwidth limits and can, therefore, employ media bypass. Note that this is also true when call admission control and media bypass are both enabled.

Furthermore, for bypass to work properly there must be consistency between a site as defined in Topology Builder and as it is defined when you configure network regions and network sites. For example, if you have a branch site that you defined in Topology Builder as having only a PSTN gateway deployed, then that branch site must be configured with an Enterprise Voice policy that enables branch site users to have their PSTN calls routed through the PSTN gateway at the branch site.

⊟To Configure Site and Region Information for Media Bypass

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Network Configuration**.
3. Double-click the **Global** configuration in the table.
4. On the **Edit Global Setting** page, select the **Enable media bypass** check box.
5. Click **Use sites and region configuration**.
6. If necessary, select the **Enable bypass for non-mapped sites** check box.

   Note:

   Select this check box only if you have one or more large sites associated with the same region that do not have bandwidth constraints (for example, a large central site), but you also have some branch sites associated with the same region that do have bandwidth constraints. When you enable bypass for non-mapped sites, configuration is streamlined in that you specify only the subnets associated with the branch sites, rather than needing to specify all subnets associated with all sites. We recommend that you do not select this check box if call admission control is enabled.

7. Click **Commit**.

Next, add subnets to the network site, as described in Associate Subnets with Network Sites for Media Bypass. (The actual procedures for associating subnets with network sites are described in Associate a Subnet with a Network Site.) After you associate all subnets with network sites, media bypass deployment is complete.

Important:

If you have not already created network regions and network sites, you must first create those before you can proceed with media bypass deployment. For details, see Create or Modify a Network Region and Create or Modify a Network Site.

Concepts

Associate Subnets with Network Sites for Media Bypass

Associate Subnets with Network Sites for Media Bypass

Configure Media Bypass > Global Media Bypass Options > Configure Media Bypass Global Settings to Use Site and Region Information >

Topic Last Modified: *2012-09-12*

Note:

This topic assumes that you have configured media bypass global settings and that you have configured network region and network sites for media bypass.

Every subnet in your network must be associated with a specific network site. This is because subnet information is used to determine the network site on which an endpoint is located. When the locations of both parties in a session are known, media bypass can determine where to send media for processing.

Media bypass does not have any special requirements for associating subnets with network sites. To create an association between the subnets and network sites in your topology, follow the procedures in Associate a Subnet with a Network Site.

Next Steps: Create Bandwidth Policy Profiles

After you associate subnets with network sites for media bypass, you must create one or more bandwidth policy profiles that will partition subnets into those with good connectivity and those without, for the purposes of media bypass. All subnets within a network region with network sites that do not have bandwidth constraints have good connectivity, and, therefore, those subnets can use media bypass.

For procedures to configure bandwidth policy profiles, see Create Bandwidth Policy Profiles.

1.4.3.12.8 Configuring Location-Based Routing

Configuring Location-Based Routing

See Also

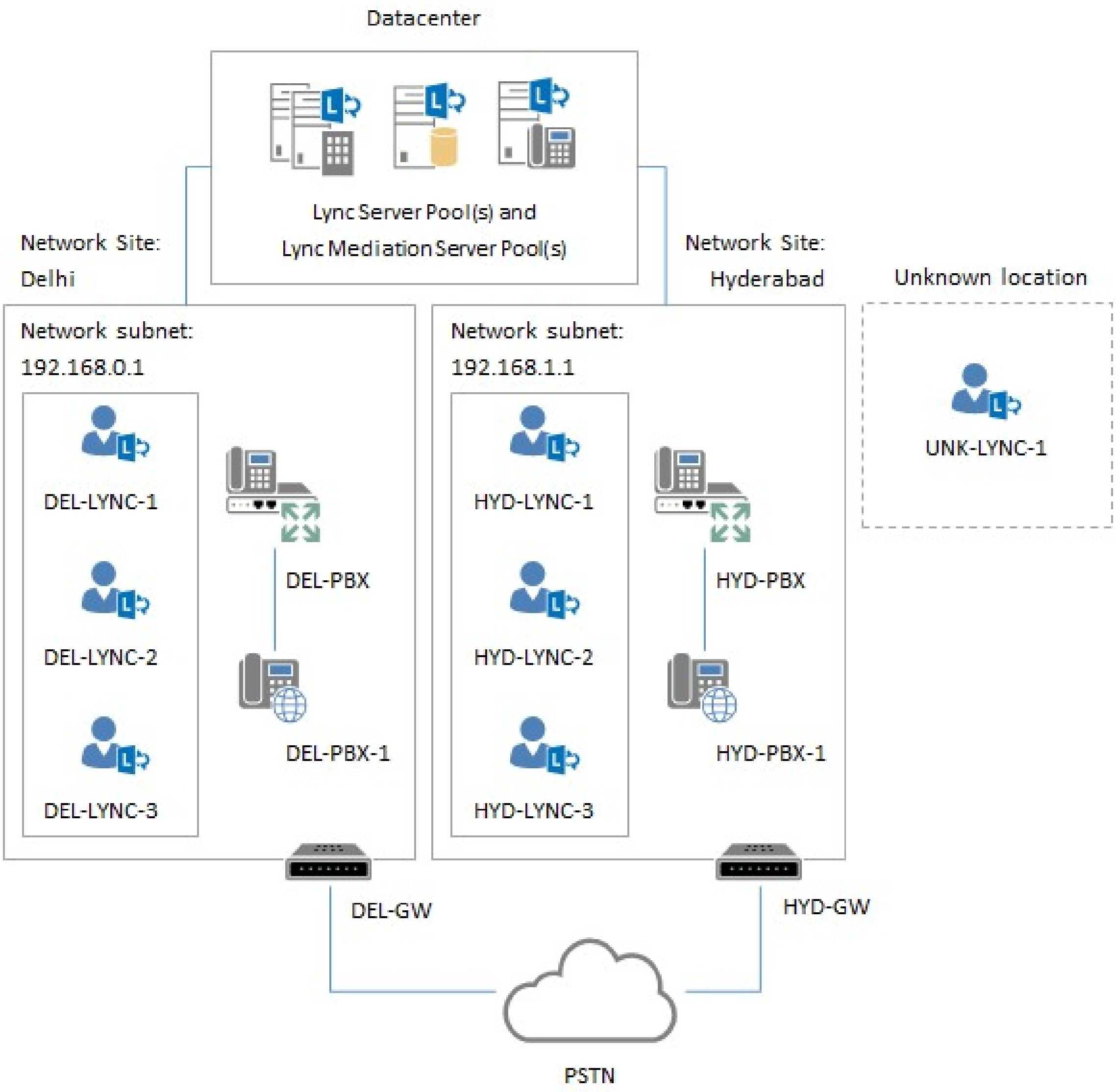
Deployment > Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features >

Topic Last Modified: *2013-03-12*

Lync Server 2013 CU1, Location-Based Routing is a feature of Enterprise Voice. Location-Based Routing is a call management feature that controls how calls are routed by Lync Server 2013 CU1. It enforces restrictions on whether calls can be routed to PBX or PSTN destinations based on the Lync caller's location. Location-Based Routing applies call authorization rules to PSTN calls based on the caller's network location. The caller's location is determined based on the network site associated with the network subnet the caller is connected on. Configuring Location-Based Routing requires first deploying Enterprise Voice, then configuring network regions, sites and subnets. This sets up the foundation for enabling Location-Based Routing.

Before deploying Location-Based Routing, you must first deploy Enterprise Voice, and configure network regions, sites, and associate network subnets to your network sites. Once completed, you can configure Location-Based Routing. For steps on how to configure network regions, sites and subnets, see Deploying Advanced Enterprise Voice Features

This section guides you through the configuration of Location-Based Routing using the following example as illustration.



The following table represents the users defined in this example.

Endpoint type	Location	Users
Lync	Delhi corporate office	DEL-LYNC-1,DEL-LYNC-2,DEL-LYNC-3
Lync	Hyderabad corporate office	HYD-LYNC-1, HYD-LYNC-2, HYD-LYNC-3
Lync	Unknown (i.e. hotel)	UNK-LYNC-1
PBX	Delhi corporate office	DEL-PBX-1, DEL-PBX-2
PBX	Hyderabad corporate office	HYD-PBX-1, HYD-PBX-2

PSTN	Unknown	PSTN-1, PSTN-2, PSTN-3

The following table represents the systems illustrated in this example environment.

System	Location	Name
Lync Server 2013 CU1 pool	any	LS-PL1
Lync Server 2013 CU1, Mediation Server	any	MS-PL1
PSTN gateway 1	Delhi	DEL-GW
PSTN gateway 2	Hyderabad	HYD-GW
PBX 1	Delhi	DEL-PBX
PBX 2	Hyderabad	RED-PBX

- Configuring Enterprise Voice
- Deploying network regions, sites and subnets
- Enabling Location-Based Routing

⊟See Also

Other Resources

Deploying Advanced Enterprise Voice Features

1.4.3.12.8.1 Configuring Enterprise Voice

Configuring Enterprise Voice

See Also

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configuring Location-Based Routing >

Topic Last Modified: *2013-03-12*

To deploy Enterprise Voice, you'll need to configure the following:

- Create a Trunk
- Define a Voice Policy
- Define a Voice Route
- Enable Users for Enterprise Voice

Create a Trunk

You must define trunks in your Enterprise Voice deployment. For Location-Based Routing, you must create a trunk configuration per trunk. Use the Lync Server Topology Builder to define your trunks, and use the Lync Server Windows PowerShell command, New-CsTrunkConfiguration, or the Lync Server Control Panel to define the corresponding trunk configurations. More information on how to enable Location-Based Routing on trunk configurations can be found in the section, Enable Location-Based Routing to Trunks, in the topic, Enabling Location-Based Routing. For this example, the following table illustrates the trunks used in this scenario.

For more information, see Define additional Trunks in Topology Builder.

Trunk name	System type	Name	Location	Mediation Server

Trunk 1 DEL-GW	PSTN gateway	DEL-GW	Delhi	MS1
Trunk 2 HYD-GW	PSTN gateway	HYD-GW	Hyderabad	MS1
Trunk 3 DEL-PBX	PBX	DEL-PBX	Delhi	MS1
Trunk 4 HYD-PBX	PBX	HYD-PBX	Hyderabad	MS1

⊟

Defines Voice Policies

You must define voice policies for your Enterprise Voice deployment. Define a Voice Policy to enforce Location-Based Routing restrictions to a subset of users if only a subset of them is required to use Location-Based Routing. For this example, the following table illustrates the voice policies used in this scenario. Only settings that are specific to Location-Based Routing are included in the table for illustration purposes.

For more information, see Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges.

	Voice policy 1	**Voice policy 2**
Voice policy ID	Delhi voice policy	Hyderabad voice policy
PSTN usages	Delhi usage, PBX Del usage, PBX Hyd usage	Hyderabad usage, PBX Hyd usage, PBX Del usage
PreventPSTNTollBypass	False	False

⊟

Define Voice Routes

You must define voice routes for your Enterprise Voice deployment. For this example, the following table illustrates the voice routes used in this scenario. Only settings that are specific to Location-Based Routing are included in the table for illustration purposes.

For more information, see Configuring Voice Routes for Outbound Calls.

	Voice route 1	**Voice route 2**	**Voice route 3**	**Voice route 4**
Name	Delhi route	Hyderabad route	PBX Del route	PBX Hyd route
PSTN usages	Delhi usage	Hyderabad usage	PBX Del usage	PBX Hyd usage
Trunk	Trunk 1 DEL-GW	Trunk 2 HYD-GW	Trunk 3 DEL-PBX	Trunk 4 HYD-PBX

⊟

Enable Users for Enterprise Voice

Enable users for Enterprise Voice and assign them a voice policy you’ve previously defined. For this example, the following table illustrates the assignment used in this scenario. Only settings that are specific to Location-Based Routing are included in the table for illustration purposes.

For more information, see Enable Users for Enterprise Voice.

	Users located in Delhi	Users located in Hyderabad
Associated voice policy	Delhi voice policy	Hyderabad voice policy
Sample users	DEL-LYNC-1,DEL-LYNC-2,DEL-LYNC-3	HYD-LYNC-1, HYD-LYNC-2, HYD-LYNC-3

See Also

Other Resources

Configuring Location-Based Routing

1.4.3.12.8.2 Deploying network regions, sites and subnets

Deploying network regions, sites and subnets

See Also

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configuring Location-Based Routing >

Topic Last Modified: *2013-03-12*

Once Enterprise Voice is deployed, you need to configure:

- Network regions
- Network sites
- Network subnets

Define Network Regions

Use the Lync Server Windows PowerShell command, New-CsNetworkRegion, or Lync Server Control Panel to define network regions.

```
New-CsNetworkRegion -NetworkRegionID <region ID> -CentralSite <site ID>
```

For more information, see New-CsNetworkRegion.

For this example, the following Windows PowerShell command illustrates the network region, region 1 (India), defined in this scenario.

```
New-CsNetworkRegion -NetworkRegionID "India" -CentralSite "India Central Site"
```

Define Network Sites

Use the Lync Server Windows PowerShell command, New-CsNetworkSite, or the Lync Server Control Panel to define network sites.

```
New-CsNetworkSite -NetworkSiteID <site ID> -NetworkRegionID <region ID>
```

For more information, see New-CsNetworkSite.

For this example, the following table and Lync Server Windows PowerShell command illustrate the network sites defined in this scenario. Only settings that are specific to Location-Based Routing are included in the table for illustration purposes.

```
New-CsNetworkSite -NetworkSiteID "Delhi" -NetworkRegionID "India"
```

```
New-CsNetworkSite -NetworkSiteID "Hyderabad" -NetworkRegionID "India"
```

	Site 1 (Delhi)	Site 2 (Hyderabad)
Site ID	Site 1 (Delhi)	Site 2 (Hyderabad)
Region ID	Region 1 (India)	Region 1 (India)

Define Network Subnets

Use the Lync Server Windows PowerShell command, New-CsNetworkSubnet, or the Lync Server Control Panel to define network subnets and assign them to network sites.

```
New-CsNetworkSubnet -SubnetID <Subnet IP address> -MaskBits <Subnet bitmask> -Net
```

For more information, see New-CsNetworkSubnet.

For this example, the following table and Windows PowerShell commands illustrate the assignment of network subnets to the network sites, Delhi and Hyderabad, defined in this scenario. Only settings that are specific to Location-Based Routing are included in the table for illustration purposes.

```
New-CsNetworkSubnet -SubnetID "192.168.0.0" -MaskBits "24" -NetworkSiteID "Delhi"
New-CsNetworkSubnet -SubnetID "192.168.1.0" -MaskBits "24" -NetworkSiteID "Hydera
```

	Site 1 (Delhi)	Site 2 (Hyderabad)
Subnet ID	192.168.0.0	192.168.1.0
Mask	24	24
Site ID	Site 1 (Delhi)	Site 2 (Hyderabad)

See Also

Other Resources

Configuring Location-Based Routing

1.4.3.12.8.3 Enabling Location-Based Routing

Enabling Location-Based Routing

See Also

Deploying Enterprise Voice > Deploying Advanced Enterprise Voice Features > Configuring Location-Based Routing >

Topic Last Modified: *2013-03-12*

Once Enterprise Voice is deployed and network regions, sites and subnets are defined, you can enable Location-Based Routing. Location-Based Routing must be enabled for the following Enterprise Voice elements:

- Network sites
- Trunk configurations
- Voice policies
- Routing configuration

Enable Location-Based Routing to Network Sites

After you have deployed Enterprise Voice, and configured network sites, you are ready to configure Location-Based Routing. First, you create a voice routing policy to associate the network site with the appropriate PSTN usages. When assigning PSTN usages to a voice routing policy, make sure to only use PSTN usages that are associated to voice routes that use a PSTN gateway local to the site or a PSTN gateway that is located in a region where Location-Based Routing restrictions are not needed.Use the Lync Server Windows PowerShell command, New-CsVoiceRoutingPolicy, or Lync Server Control Panel to create voice routing policies.

```
New-CsVoiceRoutingPolicy -Identity <voice routing policy ID> -Name <voice routing
```

For more information, see New-CsVoiceRoutingPolicy.

For this example, the following table and Windows PowerShell commands illustrate two voice routing policies and their associated PSTN usages defined in this scenario. Only settings that are specific to Location-Based Routing are included in the table for illustration purposes.

```
New-CsVoiceRoutingPolicy -Identity "DelhiVoiceRoutingPolicy" -Name "Delhi voice r
New-CsVoiceRoutingPolicy -Identity "HyderabadVoiceRoutingPolicy" -Name " Hyderaba
```

	Voice routing policy 1	**Voice routing policy 2**
Voice policy ID	Delhi voice routing policy	Hyderabad voice routing policy
PSTN usages	Delhi usage, PBX Del usage, PBX Hyd usage	Hyderabad usage, PBX Hyd usage, PBX Del usage

Next, configure Location-Based Routing for the applicable network sites and associate your voice routing policies to them. Use the Lync Server Windows PowerShell command, New-CsNetworkSite, to enable Location-Based Routing and associate voice routing policies to your network sites that must enforce routing restrictions.

```
Set-CsNetworkSite -Identity <site ID> -EnableLocationBasedRouting <$true|$false>
```

In this example, the following table illustrates Location-Based Routing for two different network sites, Delhi and Hyderabad, defined in this scenario using the Lync Server Windows PowerShell. Only settings that are specific to Location-Based Routing are included in the table for illustration purposes.

```
Set-CsNetworkSite -Identity "Delhi" -EnableLocationBasedRouting $true -VoiceRouti
Set-CsNetworkSite -Identity "Hyderabad" -EnableLocationBasedRouting $true -VoiceR
```

	Site 1 (Delhi)	**Site 2 (Hyderabad)**
Site Name	Site 1 (Delhi)	Site 2 (Hyderabad)
EnableLocationBasedRouting	True	True
Voice routing policy	Delhi voice routing policy	Hyderabad voice routing policy
Subnets	Subnet 1 (Delhi)	Subnet 2 (Hyderabad)

⊟

Enable Location-Based Routing to Trunks

Before a trunk configuration can be enabled for Location-Based Routing, you need to create a trunk configuration for each trunk or each network site. Use the Lync Server Windows PowerShell command, New-CsTrunkConfiguration, to create a trunk configuration. If multiple trunks are associated with a given system (i.e. Gateway or PBX), each trunk configuration must be modified to enable Location-Based Routing restrictions.

```
New-CsTrunkConfiguration -Identity < trunk configuration ID>
```

For more information, see New-CsTrunkConfiguration.

For this example, the following Windows PowerShell commands illustrate creating one trunk configuration for each trunk in the deployment defined in this scenario.

```
New-CsTrunkConfiguration -Identity Service:PstnGateway:"<Trunk 1 DEL-GW>"
New-CsTrunkConfiguration -Identity Service:PstnGateway:"<Trunk 2 HYD-GW>"
New-CsTrunkConfiguration -Identity Service:PstnGateway:"<Trunk 3 DEL-PBX>"
New-CsTrunkConfiguration -Identity Service:PstnGateway:"<Trunk 4 HYD-PBX>"
```

Once a trunk configuration is configured per trunk, you can use the the Lync Server Windows PowerShell command, Set-CsTrunkConfiguration, to enable Location-Based Routing to your trunks that must enforce routing restrictions. Enable Location-Based Routing to trunks that route calls to PSTN gateways that route calls to the PSTN, and associate the network site where the gateway is located.

```
Set-CsTrunkConfiguration -Identity <trunk configuration ID> -EnableLocationRestri
```

For more information, see New-CsTrunkConfiguration.

In this example, Location-Based Routing is enabled for each trunk that is associated to PSTN gateways in Delhi and Hyderabad:

```
Set-CsTrunkConfiguration -Identity Service:PstnGateway:Trunk 1 DEL-GW -EnableLoca
Set-CsTrunkConfiguration -Identity Service:PstnGateway:Trunk 2 HYD-GW -EnableLoca
```

Do not enable Location-Based Routing for trunks that do not route calls to the PSTN; however, you must still associate the trunk to the network site where the system is located as Location-Based Routing restrictions need to be enforced for PSTN calls reaching endpoints connected via this trunk. For this example, Location-Based Routing is not enabled for each trunk that is associated to PBX systems in Delhi and Hyderabad:

```
Set-CsTrunkConfiguration -Identity Service:PstnGateway:Trunk 3 DEL-PBX -EnableLoc
Set-CsTrunkConfiguration -Identity Service:PstnGateway:Trunk 4 HYD-PBX -EnableLoc
```

Endpoints that are connected to systems that do not route calls to the PSTN (i.e. a PBX) will have similar restrictions as Lync endpoints of users enabled for Location-Based Routing. This means that these users will be able to place and receive calls to and from Lync user regardless of the user's location. They will also be able to place an receive calls to and from other systems that do not route calls to the PSTN network (i.e. an endpoint connected to a different PBX) regardless of the network site to which the system is associated. All inbound calls, outbound calls, call transfers and call forwarding involving PSTN endpoints will be subject to Location-Based Routing enforcements. Such calls must use only PSTN gateways that are defined as local to such systems.

Name	EnableLocationRestriction	NetworkSiteID
PstnGateway:Trunk 1 DEL-	True	Site 1 (Delhi)

GW		
PstnGateway:Trunk 2 HYD-GW	True	Site 2 (Hyderabad)
PstnGateway:Trunk 3 DEL-PBX	False	Site 1 (Delhi)
PstnGateway:Trunk 4 HYD-PBX	False	Site 2 (Hyderabad)

Enable Location-Based Routing to Voice Policies

To enforce Location-Based Routing to specific users, configure those users' voice policy to prevent PSTN toll bypass. Use the Lync Server Windows PowerShell command, New-CsVoicePolicy, to create a new voice policy or Set-CsVoicePolicy, if using an existing policy, to enable Location-Based Routing by preventing PSTN toll bypass.

```
Set-CsVoicePolicy -Identity <voice policy ID> -PreventPSTNTollBypass <$true|$fals
```

For more information, see New-CsVoicePolicy.

For this example, the following table and Windows PowerShell commands illustrate enabling the prevention of PSTN toll bypass to the Delhi and Hyderabad voice policies defined in this scenario. Only settings that are specific to Location-Based Routing are included in the table for illustration purposes.

```
Set-CsVoicePolicy -Identity "Delhi voice policy" -PreventPSTNTollBypass $true
Set-CsVoicePolicy -Identity "Hyderabad voice policy" -PreventPSTNTollBypass $true
```

	Voice policy 1	**Voice policy 2**
Voice policy ID	Delhi voice policy	Hyderabad voice policy
PSTN usages	Delhi usage, PBX Del usage, PBX Hyd usage	Hyderabad usage, PBX Hyd usage, PBX Del usage
PreventPSTNTollBypass	True	True

Enable Location-Based Routing in the routing configuration

Finally, globally enable Location-Based Routing to your routing configuration. Use the Lync Server Windows PowerShell command, New-CsRoutingConfiguration, to enable Location-Based Routing.

```
Set-CsRoutingConfiguration -EnableLocationBasedRouting $true
```

For more information, see Set-CsRoutingConfiguration.

Note:

while Location-Based Routing must be enabled via a global configuration, the set of rules to be applied will only be enforced for the sites, users and trunks for which it has been configured as specified in this documentation.

⊟

⊟See Also

Other Resources

Configuring Location-Based Routing

1.4.3.13 Deploying Call Management Features

Deploying Call Management Features

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-12-18*

Enterprise Voice call management features control how incoming calls are routed and answered. Lync Server 2013 provides the following call management features:

- **Call Park:** Enables voice users to temporarily park a call and then pick it up from the same phone or another phone.
- **Group Pickup:** Enables users to answer calls made to another user who is assigned to a pickup group by dialing the call pickup group number.
- **Response Group:** Routes incoming calls to groups of agents by using hunt groups or interactive voice response (IVR) questions and answers.
- **Announcement:** Plays a message for calls made to an unassigned number, or routes the call elsewhere, or both.

This section describes how to configure these call management features during an Enterprise Voice deployment.

- Configuring Call Park
- Configuring Group Call Pickup
- Configuring Response Group
- Configuring Announcements for Unassigned Numbers

1.4.3.13.1 Configuring Call Park

Configuring Call Park

Deployment > Deploying Enterprise Voice > Deploying Call Management Features >

Topic Last Modified: *2012-10-30*

Call Park enables an Enterprise Voice user to put a call on hold from one telephone and then retrieve the call later by dialing an internal number (known as a Call Park *orbit*) from any telephone.

The components that Call Park uses are automatically installed and enabled on the Front End Server or Standard Edition server when you deploy Enterprise Voice. However, you must configure Call Park before it is available to users.

This section guides you through the configuration of Call Park.

- Call Park Configuration Prerequisites and User Rights
- Deployment Process for Call Park
- Configure the Call Park Orbit Table
- Configure Call Park Settings
- Customize Call Park Music on Hold
- Enable Call Park for Users
- Verify Normalization Rules for Call Park

- (Optional) Verify Call Park Deployment

1.4.3.13.1.1 Call Park Configuration Prerequisites and User Rights

Call Park Configuration Prerequisites and User Rights

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Call Park >

Topic Last Modified: *2012-09-10*

Call Park is a call management feature that is installed by default when you deploy Enterprise Voice. This topic describes what you need to have in place before you can configure Call Park and the user rights that you need to perform configuration tasks.

◆**Important:**
Customized music-on-hold files for the Call Park application are not backed up as part of the Lync Server 2013 disaster recovery process, and the files will be lost if the files uploaded to the pool are damaged, corrupted, or erased. Always keep a separate backup copy of the customized music-on-hold files that you have uploaded for Call Park.

This section assumes that you have read the planning documentation related to Call Park (see Planning for Call Management Features).

Call Park Configuration Prerequisites

Call Park requires the following components:

- Application service
- Call Park application

These components are installed automatically when you deploy Enterprise Voice.

If you want callers to hear music while the call is parked, a music-on-hold file is also required. A default music-on-hold file is installed automatically when you deploy Enterprise Voice. You can substitute the default file with your own music-on-hold file. Call Park uses File Store to hold the audio file.

Call Park Configuration User Rights

You can use the following administrative tools to configure Call Park:

- Lync Server Control Panel
- Lync Server Management Shell

You use these tools to set up the Call Park orbit table and to configure other settings used by Call Park.

Configuring Call Park requires any of the following administrative roles, depending on the task:

- **CsVoiceAdministrator:** This administrator role can create, configure, and manage all voice-related settings and policies.
- **CsUserAdministrator:** This administrator role can enable Call Park in voice policy. This administrator role also has read-only view access to all voice configurations.
- **CsServerAdministrator:** This administrator role can manage, monitor, and troubleshoot servers and services.
- **CsAdministrator:** This administrator role can perform all of the tasks of

CsVoiceAdministrator, CsServerAdministrator, and CsUserAdministrator.

Note:

For details about administrative rights, see Planning for Role-Based Access Control in the Planning documentation.

See Also

Concepts

Deploying Enterprise Voice

Other Resources

Planning for Call Management Features

1.4.3.13.1.2 Deployment Process for Call Park

Deployment Process for Call Park

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Call Park >

Topic Last Modified: *2013-02-25*

This section provides an overview of the steps involved in deploying the Call Park application. You must deploy Enterprise Edition or Standard Edition with Enterprise Voice before you configure Call Park. The components required by Call Park are installed and enabled when you deploy Enterprise Voice.

Call Park Deployment Process

Phase	Steps	Required groups and roles	Deployment documentation
Configure the call park orbit ranges in the orbit table	Use Lync Server Control Panel or the **New-CSCallParkOrbit** cmdlet to create the orbit ranges in the call park orbit table and associate them with the Application service that hosts the Call Park application. **Note:** For seamless integration with existing dial plans, orbit ranges are typically configured as a block of virtual extensions. Assigning Direct Inward Dialing (DID) numbers as orbit numbers in the call park orbit table is not supported.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Create or Modify a Call Park Orbit Range
Configure Call Park settings	Use the **Set-CsCpsConfiguration** cmdlet to configure Call Park settings. At a minimum, we recommend that you configure the **OnTimeoutURI** option to configure the fallback destination to use when a parked call times out. You can also configure the following settings: - (Optional)	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Configure Call Park Settings

	EnableMusicOnHold to enable or disable music on hold. • (Optional) **MaxCallPickupAttempts** to determine the number of times a parked call rings back to the answering phone before forwarding the call to the fallback Uniform Resource Identifier (URI). • (Optional) **CallPickupTimeoutThreshold** to determine the amount of time that elapses after a call has been parked before it rings back to the phone where the call was answered.		
Optionally, customize the music on hold	Use the **Set-CsCallParkServiceMusicOnHoldFile** cmdlet to customize and upload an audio file, if you don't want to use the default music on hold.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Customize Call Park Music on Hold
Configure voice policy to enable Call Park for users	Use Lync Server Control Panel or the **Set-CSVoicePolicy** cmdlet with the **EnableCallPark** option to enable Call Park for users in voice policy. **Note:** By default, Call Park is disabled for all users. **Note:** If you have multiple voice policies, make sure the EnableCallPark property is set for each voice policy, not just for the default policy.	RTCUniversalServerAdmins CsVoiceAdministrator CsUserAdministrator CsAdministrator	Enable Call Park for Users
Verify normalization rules for Call Park	Call park orbits must not be normalized. Verify that your normalization rules do not include any of your orbit ranges. If necessary, create additional normalization rules to	RTCUniversalServerAdmins CsVoiceAdministrator	Verify Normalization Rules for Call Park

	prevent orbits being normalized.	CsServerAdministrator CsAdministrator	
Verify your Call Park deployment	Test parking and retrieving calls to make sure that your configuration works as expected.	-	(Optional) Verify Call Park Deployment

1.4.3.13.1.3 Configure the Call Park Orbit Table

Configure the Call Park Orbit Table

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Call Park >

Topic Last Modified: *2012-09-10*

Call Park uses orbits for parking calls. Before users can park and retrieve calls, you must configure the Call Park orbit table. You need to specify the ranges of extension numbers (orbits) that your organization will reserve for parking calls and define the routing for those ranges by specifying which Call Park pool handles each range. When you define orbit ranges, the goal is to have enough orbits so that any one orbit is not reused too quickly, but not so many orbits that you limit the number of extensions available for users or other services. You can create multiple Call Park orbit ranges for each Lync Server pool where the Call Park application is deployed. Each Call Park orbit range must have a globally unique name and a unique set of extensions.

Important:

An orbit range typically encompasses 100 or fewer orbits. Each range can be much larger, as long as it is smaller than the maximum of 10,000 orbits per range and you have fewer than 50,000 orbits per pool. If a range is too small, the orbits are reused more quickly.

Use blocks of virtual extensions (extensions that have no user or phone assigned to them) for your orbit ranges.

Note:

Assigning Direct Inward Dialing (DID) numbers as orbit numbers in the Call Park orbit table is not supported.

Create or Modify a Call Park Orbit Range

Create or Modify a Call Park Orbit Range

See Also

Deploying Call Management Features > Configuring Call Park > Configure the Call Park Orbit Table >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to create or modify a call park orbit range.

⊟To use Lync Server Control Panel to create or modify a range of numbers for parking calls

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Features** and then click **Call Park**.
4. On the **Call Park** page, do one of the following:
   - To create a new orbit range, click **New**. In **Name**, type an identifying name for this range of numbers.

     > **Note:**
     > After you commit the orbit range to the database, you cannot change this name.

   - To modify an existing orbit range, type all or part of the name of the orbit range in the search field. In the resulting list of orbits, click the orbit you want, click **Edit**, and then click **Show details**.
5. In the first **Number range** field, type the beginning number of the range of extensions for this call park orbit, and in the second **Number range** field, type the ending number of the range.

   > **Note:**
   > - The beginning number of the range must be less than or equal to the ending number of the range.
   > - The value of the beginning number of the range must be the same length as the ending number of the range.
   > - The orbit range must be unique. This range cannot overlap with any other range.
   > - If the orbit range begins with the character * or #, the range must be greater than 100.
   > - Valid values: Must match the regular expression string ([*|#]?[1-9]\d{0,7})|([1-9]\d{0,8}). This means the value must be a string beginning with either the character * or # or a number 1 through 9 (the first character cannot be a zero). If the first character is * or #, the following character must be a number 1 through 9 (it cannot be a zero). Subsequent characters can be any number 0 through 9 up to seven additional characters (for example, "#6000", "*92000", "*95551212", and "915551212"). If the first character is not * or #, the first character must be a number 1 through 9 (it cannot be zero), followed by up to eight characters, each a number 0 through 9 (for example, "915551212", "41212", "300").
   > - You should not have more than a total of 50,000 orbits per pool. Each orbit range typically encompasses 100 or fewer orbits, but it can be much larger as long as it includes fewer than 10,000 orbits. For example, instead of specifying a starting number of "7000000" and an ending number of "8000000," consider specifying a starting number of "7000000" and an ending number of "7000100."

1. In **FQDN of destination server**, click the fully qualified domain name (FQDN) or service ID of the Application service that hosts the Call Park application. All calls parked to numbers within the range specified by the start number and end number in the orbit range will be routed to this server or pool.
2. Click **Commit**.

To use Windows PowerShell to create or modify a range of numbers for parking calls

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user

rights as described in Delegate Setup Permissions.

2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Use **New-CsCallParkOrbit** to create a new range of orbit numbers. Use **Set-CsCallParkOrbit** to modify an existing range of orbit numbers.

   At the command line, run:

   ```
   New-CsCallParkOrbit -Identity <name of orbit range> -NumberRangeStart
   ```

   For example:

   ```
   New-CsCallParkOrbit -Identity "Redmond orbit 1" -NumberRangeStart 100
   ```

   The following example shows how to modify the numbers in an existing orbit range,

   ```
   Set-CsCallParkOrbit -Identity "Redmond orbit 1" -NumberRangeStart 500
   ```

Tasks

Delete a Call Park Orbit Range

Other Resources

New-CsCallParkOrbit
Set-CsCallParkOrbit

1.4.3.13.1.4 Configure Call Park Settings

Configure Call Park Settings

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Call Park >

Topic Last Modified: *2012-11-01*

If you don't want to use default Call Park settings, you can customize them. When you install the Call Park application, global settings are configured by default. You can modify the global settings, and you can also specify site-specific settings. Use the **New-CsCpsConfiguration** cmdlet to create new site-specific settings. Use the **Set-CsCpsConfiguration** cmdlet to modify existing settings.

Note:

At a minimum, we recommend that you configure the **OnTimeoutURI** option for the fallback destination to use when a parked call times out and ringback fails.

Use **New-CsCpsConfiguration** cmdlet or the **Set-CsCpsConfiguration** cmdlet to configure any of the following settings:

This option:	Specifies this:
CallPickupTimeoutThreshold	The amount of time that elapses after a call has been parked before it rings back to the phone where the call was answered. The value must be entered in the format hh:mm:ss to specify the hours, minutes, and seconds. The minimum value is 10 seconds, and the maximum value is 10 minutes. The default is 00:01:30.
EnableMusicOnHold	Whether music plays for a caller while a call is parked. Values are True or False. The default is True.

MaxCallPickupAttempts	The number of times a parked call rings back to the answering phone before it is forwarded to the fallback Uniform Resource Identifier (URI) that is specified for **OnTimeoutURI**. The default is 1.
OnTimeoutURI	The SIP address of the user or response group to which an unanswered parked call is routed when **MaxCallPickupAttempts** is exceeded. Value must be a SIP URI beginning with the string sip:. For example, sip:bob@contoso.com. The default is no forwarding address.

⊟To configure Call Park settings

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

```
New-CsCpsConfiguration -Identity site:<sitename to apply settings> [-C
```

Tip:

Use the **Get-CsSite** cmdlet to identify the site. For details, see Lync Server Management Shell documentation.

For example:

```
New-CsCpsConfiguration -Identity site:Redmond1 -CallPickupTimeoutThres
```

Tasks

Customize Call Park Music on Hold

Other Resources

New-CsCpsConfiguration
Set-CsCpsConfiguration
Get-CsSite

1.4.3.13.1.5 Customize Call Park Music on Hold

Customize Call Park Music on Hold

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Call Park >

Topic Last Modified: *2012-09-10*

You can specify your own music file to use for music on hold, instead of the default music file that ships with Lync Server 2013. To customize music on hold, use the **Set-CsCallParkServiceMusicOnHoldFile** cmdlet.

Note:

If you customize music on hold and want the same music for multiple sites, you must configure the music file for each site that runs the Call Park application.

To customize the music file

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

```
Set-CsCallParkServiceMusicOnHoldFile -Service <ServiceID where the Cal
```

Tip:

Use the **Get-CsService** cmdlet to identify the service. For details, see Get-CsService.

The following example shows how to obtain the contents of a file, soothingmusic.wma, as a byte array and assign it to a variable. Then the audio file is assigned as the music-on-hold file for Call Park. For details, see Set-CsCallParkServiceMusicOnHoldFile.

```
$a = Get-Content -ReadCount 0 -Encoding byte "C:\MoHFiles\soothingmusi
Set-CsCallParkServiceMusicOnHoldFile -Service Redmond1-applicationserv
```

Other Resources

Set-CsCallParkServiceMusicOnHoldFile
Get-CsService

1.4.3.13.1.6 Enable Call Park for Users

Enable Call Park for Users

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Call Park >

Topic Last Modified: *2012-09-11*

Users cannot park calls or retrieve parked calls until they are enabled for Call Park in voice policy.

Note:

By default, Call Park is disabled for all users.

You can enable Call Park at the global scope, or at the site scope or user scope. User scope takes precedence over site scope, and site scope takes precedence over global scope. If you have multiple voice policies, review all the policies to enable Call Park, not just the global policy.

To Use Lync Server Control Panel to Enable Call Park for Users

1. Log on to the computer as a member of the **RTCUniversalServerAdmins** group, or as a member of the **CsVoiceAdministrator**, **CsServerAdministrator**, or **CsAdministrator** administrative role.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.
4. Click the **Voice Policy** tab.
5. Double-click an existing voice policy to open the **Edit Voice Policy** dialog box.
6. Under **Calling features**, select **Enable call park**.
7. Click **OK** to save the voice policy

To Use Cmdlets to Enable Call Park for Users

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator administrative role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

   ```
   Set-CsVoicePolicy -Identity <VoicePolicy> -EnableCallPark $true
   ```

   For example, to enable Call Park for the default global voice policy:

   ```
   Set-CsVoicePolicy -EnableCallPark $true
   ```

Tasks

Create a Voice Policy and Configure PSTN Usage Records

1.4.3.13.1.7 Verify Normalization Rules for Call Park

Verify Normalization Rules for Call Park

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Call Park >

Topic Last Modified: *2012-09-11*

Call Park orbits must not be normalized. Check your dial plans to be sure that your orbit numbers are not normalized. If you must create an additional normalization rule to prevent your orbits from being normalized, follow the procedure in Create a Dial Plan to define a new normalization rule, so that **Pattern to match** identifies the orbit range and **Translation pattern** is **$1**. For example, if your Call Park orbit range is 7000 – 7999, the **Pattern to match** is **^(7\d{3})$** and **Translation pattern** is **$1**.

Important:
Be sure that the default normalization rule in your dial plans does not contain **^(\d*)**. Otherwise, your Call Park normalization rule will never run.

Tasks

Create a Dial Plan

1.4.3.13.1.8 (Optional) Verify Call Park Deployment

(Optional) Verify Call Park Deployment

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Call Park >

Topic Last Modified: *2012-09-11*

After you install and configure Call Park, you need to verify the configuration to make sure that parking and retrieving calls works as expected. At minimum, verify the following:

- Call a user who has Call Park enabled and have the user park the call.

  Note:
  If you enabled Call Park in voice policy just before performing this test, the user who is parking the call needs to sign out of Lync Server, and then sign back in, to be able to see the Call Park option in the transfer call list.

- Dial the orbit number to retrieve the call.

- Park another call, let the parked call time out, and do not pick up the ringback. Verify that the timed-out call is correctly routed to the fallback destination that is specified for **OnTimeoutURI**.

1.4.3.13.2 Configuring Group Call Pickup

Configuring Group Call Pickup

Deployment > Deploying Enterprise Voice > Deploying Call Management Features >

Topic Last Modified: *2013-02-01*

Cumulative update for Lync Server 2013: February 2013 introduces Group Call Pickup as a new Enterprise Voice feature. Group Call Pickup lets users pick up calls that are ringing for another user by dialing a call pickup group number.

The components that Group Call Pickup uses are automatically installed and enabled on the Front End Server or Standard Edition server when you deploy Enterprise Voice. However, you must configure Group Call Pickup before it is available to users.

This section guides you through the configuration of Group Call Pickup.
Group Call Pickup Configuration Prerequisites and User Rights

Deployment Process for Group Call Pickup

Deploy the SEFAUtil tool

Configure Call Pickup Group Numbers

Enable Group Call Pickup for Users and Assign a Group Number

Communicate Group Call Pickup Assignment to Users

(Optional) Verify the Group Call Pickup Deployment

1.4.3.13.2.1 Group Call Pickup Configuration Prerequisites and User Rights

Group Call Pickup Configuration Prerequisites and User Rights

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Group Call Pickup >

Topic Last Modified: *2013-01-30*

Group Call Pickup is a call management feature that is installed by default when you deploy Enterprise Voice. This topic describes what you need to have in place before you can configure Group Call Pickup and the user rights that you need to perform configuration tasks.

This section assumes that you have read the planning documentation related to Group Call Pickup (see Planning for Group Call Pickup).

Group Call Pickup Configuration Prerequisites

Group Call Pickup requires the following components:

- Application service
- Call Park application

These components are installed automatically when you deploy Enterprise Voice.

Group Call Pickup Configuration User Rights

You use the following administrative tools to configure Group Call Pickup:

- Lync Server Management Shell
- SEFAUtil resource kit tool

Use Lync Server Management Shell to create and manage call pickup groups in the Call Park orbit table. Use the SEFAUtil resource kit tool to assign a call pickup group and enable Group Call Pickup for users or to disable Group Call Pickup for users.

Configuring Group Call Pickup requires any of the following administrative roles, depending on the task:

- **CsVoiceAdministrator:** This administrator role can create, configure, and manage all voice-related settings and policies.
- **CsUserAdministrator:** This administrator role can enable Group Call Pickup for users. This administrator role also has read-only view access to all voice configurations.
- **CsServerAdministrator:** This administrator role can manage, monitor, and troubleshoot servers and services.
- **CsAdministrator:** This administrator role can perform all of the tasks of CsVoiceAdministrator, CsServerAdministrator, and CsUserAdministrator.

Note:

For details about administrative rights, see Planning for Role-Based Access Control in the Planning documentation.

See Also

Concepts

Deploying Enterprise Voice

Other Resources

Planning for Call Management Features

1.4.3.13.2.2 Deployment Process for Group Call Pickup

Deployment Process for Group Call Pickup

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Group Call Pickup >

Topic Last Modified: *2013-02-25*

This section provides an overview of the steps involved in deploying Group Call Pickup. You must deploy Enterprise Edition or Standard Edition with Enterprise Voice before you configure Group Call Pickup. The components required by Group Call Pickup are installed and enabled when you deploy Enterprise Voice.

Group Call Pickup Deployment Process

Phase	Steps	Required groups and roles	Deployment documentation
Enable the SEFAUtil resource kit tool in the topology	1. Use the **New-CsTrustedApplicationPool** cmdlet to create a new trusted application pool. 2. Use the **New-CsTrustedApplication** cmdlet to specify the SEFAUtil tool as trusted application. 3. Run the **Enable-CsTopology** cmdlet to enable the topology. 4. Install the resource kit tools on a Front End Server that is in the trusted application pool created in step 1. 5. Verify that SEFAUtil is running correctly by running it to display the call forwarding settings of a user in the deployment.	RTCUniversalServerAdmins	Deploy the SEFAUtil tool
Configure call pickup number ranges in the call park orbit table	Use the **New-CSCallParkOrbit** cmdlet to create call pickup number ranges in the call park orbit table and assign the call pickup ranges the type GroupPickup. **Note:** You must use Lync Server Management Shell to create, modify, remove, and view Group Call Pickup number ranges in the call park orbit table. Group Call Pickup number ranges are not available in Lync Server Control Panel. **Note:** For seamless integration with existing dial plans, number ranges are typically configured as a block of virtual extensions. Assigning Direct Inward Dialing (DID) numbers as range numbers in the call park orbit table is not supported.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Configure Call Pickup Group Numbers
Assign a call pickup number to users, and enable	Use the /enablegrouppickup parameter in the SEFAUtil resource kit tool to enable Group	-	Enable Group Call Pickup for Users and Assign a

Group Call Pickup for the users	Call Pickup and assign a call pickup number for users.		Group Number
Notify users of their assigned call pickup number and any other number of interest	Because any user can retrieve a call made to a Group Call Pickup user, users may want to monitor more than one group.	-	Communicate Group Call Pickup Assignment to Users
Verify your Group Call Pickup deployment	Test placing and retrieving calls to make sure that your configuration works as expected.	-	(Optional) Verify the Group Call Pickup Deployment

1.4.3.13.2.3 Deploy the SEFAUtil tool

Deploy the SEFAUtil tool

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Group Call Pickup >

Topic Last Modified: *2013-01-30*

To deploy and manage Group Call Pickup, you need to use the SEFAUtil resource kit tool. The tool is part of the Lync Server 2013 resource kit tools. Before you can install SEFAUtil, you must have a trusted application pool in your topology, specify SEFAUtil as a trusted application, and enable the topology.

Important:

Microsoft Unified Communications Managed API (UCMA) 3.0 Core SDK must be installed on any computer where you plan to run the SEFAUtil tool.

You can run the SEFAUtil in any Front End pool in your deployment.

Note:

For more details about running SEFAUtil, see the Technet blog article, "How to get SEFAutil running?" at http://go.microsoft.com/fwlink/?LinkId=278940.

To deploy SEFAUtil

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. The SEFAUtil tool can be run only on a computer that is part of a trusted application pool. If needed, define a trusted application pool for the Front End pool where you plan to run SEFAUtil. At the command line, run:

   ```
   New-CsTrustedApplicationPool -id <Pool FQDN> -Registrar <Pool Registra
   ```

4. Define the SEFAUtil tool as a trusted application. At the command line, run:

   ```
   New-CsTrustedApplication -ApplicationId sefautil -TrustedApplicationPo
   ```

   Note:

   You can use a different port if needed.

5. Enable the topology with your changes. At the command line, run:

```
Enable-CsTopology
```

6. Install the Lync Server 2013 resource kit tools on a Front End Server that is in the trusted application pool that you created in step 3.
7. Verify that the SEFAUtil tool is running correctly, as follows:
   7.a. Run the tool from the Windows command prompt with administrator privileges to display the call forwarding settings of a user in your deployment.

   > **Note:**
   > The tool is located at \Program Files\Microsoft Lync Server 2013 \Reskit.

   7.b. Display the call forwarding settings of a user. At the command line, run:

   ```
   SEFAUtil.exe <user SIP address> /server:<Lync Server/Pool F
   ```

   The call forwarding settings for the user will be displayed.

1.4.3.13.2.4 Configure Call Pickup Group Numbers

Configure Call Pickup Group Numbers

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Group Call Pickup >

Topic Last Modified: *2013-01-30*

Group Call Pickup is based on the Call Park application. When you deploy Group Call Pickup, you configure the call park orbit table with ranges of phone numbers that are designated as call pickup group numbers. These group numbers are the numbers that users dial to pick up calls that are ringing for another user.

Like call park orbit numbers, call pickup group numbers need to be virtual extensions that have no user or phone assigned to them. Each Front End pool where you deploy Group Call Pickup can have one or more ranges of call pickup group numbers. The group number ranges must be globally unique across the Lync Server deployment.
Create or Modify a Group Call Pickup Number Range

Create or Modify a Group Call Pickup Number Range

See Also

Deploying Call Management Features > Configuring Group Call Pickup > Configure Call Pickup Group Numbers >

Topic Last Modified: *2013-01-30*

Use the following procedure to create or modify a call pickup group number range in the call park orbit table.

> **Note:**
> You must use Lync Server Management Shell to create, modify, remove, and view Group Call Pickup number ranges in the call park orbit table. Group Call Pickup number ranges are not available in Lync Server Control Panel.

> **Important:**
> The call pickup group number range must be assigned a type of GroupPickup. Users are enabled for Group Call Pickup only if the group number that they are assigned is type GroupPickup.

The call pickup group number ranges must comply with the following rules:

- The beginning number of the range must be less than or equal to the ending number of the range.
- The value of the beginning number of the range must be the same length as the ending number of the range.
- The number range must be unique. This range cannot overlap with any other range.
- If the number range begins with the character * or #, the range must be greater than 100.
- Valid values: Must match the regular expression string ([*|#]?[1-9]\d{0,7})|([1-9]\d{0,8}). This means the value must be a string beginning with either the character * or # or a number 1 through 9 (the first character cannot be a zero). If the first character is * or #, the following character must be a number 1 through 9 (it cannot be a zero). Subsequent characters can be any number 0 through 9 up to seven additional characters (for example, "#6000", "*92000", "*95551212", and "915551212"). If the first character is not * or #, the first character must be a number 1 through 9 (it cannot be zero), followed by up to eight characters, each a number 0 through 9 (for example, "915551212", "41212", "300").

To create or modify a call pickup group range

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Use **New-CsCallParkOrbit** to create a new range of call pickup group numbers. Use **Set-CsCallParkOrbit** to modify an existing range of call pickup numbers.

   At the command line, run:

   ```
   New-CsCallParkOrbit -Identity <name of call pickup group range> -Numbe
   ```

   For example:

   ```
   New-CsCallParkOrbit -Identity "Redmond call pickup" -NumberRangeStart
   ```

   The following example shows how to change a range of numbers from call park orbits to call pickup groups.

   ```
   Set-CsCallParkOrbit -Identity "Redmond call pickup" -Type GroupPickup
   ```

   Important:

   Use this cmdlet to change the type assigned to number ranges only if you initially specified the incorrect type and the group range is not yet in use. If you change the number range from CallPark to GroupPickup or vice versa and the number range is already in use, either Call Park or Group Call Pickup will stop working for that number range. For example, if you change a number range from CallPark to GroupPick, the Call Park application can no longer use that range of orbits to park calls.

Tasks

Delete a Call Park Orbit Range

Other Resources

New-CsCallParkOrbit
Set-CsCallParkOrbit

1.4.3.13.2.5 Enable Group Call Pickup for Users and Assign a Group Number

Enable Group Call Pickup for Users and Assign a Group Number

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Group Call Pickup >

Topic Last Modified: *2013-01-30*

After you add call pickup group numbers to the call park orbit table, you assign the group numbers to users and enable Group Call Pickup for them. Use the secondary extension feature activation (SEFAUtil) resource kit tool to assign group numbers and enable Group Call Pickup.

Note:

In a hybrid deployment, do not assign a Group Call Pickup group to users who are homed online. Users who are homed online cannot participate in Group Call Pickup. That is, their calls cannot be answered by other users, and they cannot answer calls to other users.

To assign a group number and enable Group Call Pickup for a user

1. Log on to the computer where you installed the SEFAUtil tool with administrator rights.
2. At the command line, run:

```
SEFAUtil.exe sip:<sip address of user> /server:<pool FQDN> /enablegrou
```

For example, to assign group number 199 to a user:

```
SEFAUtil.exe katarina@contoso.com /server:pool01.contoso.com /enablegr
```

Tasks

Disable Group Call Pickup for Users

1.4.3.13.2.6 Communicate Group Call Pickup Assignment to Users

Communicate Group Call Pickup Assignment to Users

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Group Call Pickup >

Topic Last Modified: *2013-01-30*

After you enable Group Call Pickup for users, use email or some other mechanism to notify users of their call pickup group number. Notify users of the call pickup group number for any group that they might want to monitor. Because users can retrieve calls for other users even if they are not in the same group, users might need the call pickup group number for multiple groups.

1.4.3.13.2.7 (Optional) Verify the Group Call Pickup Deployment

(Optional) Verify the Group Call Pickup Deployment

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Group Call Pickup >

Topic Last Modified: *2013-01-30*

After you enable Group Call Pickup for users, verify that the configuration works as expected. At a minimum, verify the following:

- Call a user who is enabled for Group Call Pickup and have another user retrieve the call. The other user can be in the same group, in a different group, or not have Group Call Pickup enabled.
- Call a user who is enabled for Group Call Pickup and do not answer the call.

1.4.3.13.3 Configuring Response Group

Configuring Response Group

See Also

Deployment > Deploying Enterprise Voice > Deploying Call Management Features >

Topic Last Modified: *2012-10-30*

Response Group is an Enterprise Voice feature that routes and queues incoming calls to groups of people, called *agents*, such as a help desk or a customer service desk.

The components that Response Group requires are installed and enabled automatically on the Front End Server or Standard Edition server when you deploy Enterprise Voice. To make Response Group available to users, you must configure agent groups, then queues, and then workflows. Additionally, a Response Group Administrator can delegate configuration of an existing workflow to a Response Group Manager, who can then modify and reconfigure the workflow and its associated agent groups and queues.

This section guides you through the configuration of Lync Server 2013 Response Group. It assumes that you have already read the planning sections related to Response Group and have deployed an Enterprise Edition server or a Standard Edition server with Enterprise Voice.

Tip:

For details about creating a Response Group by using Lync Server Management Shell, including a sample script, see "Creating Your First Response Group Using Lync Server Management Shell" at http://go.microsoft.com/fwlink/p/?linkId=204108.

- Response Group Configuration Permissions and Prerequisites
- Deployment Process for Response Group
- Overview of Workflow Creation Scenarios
- Create Response Group Agent Groups
- Create Response Group Queues
- (Optional) Define Response Group Business Hours
- (Optional) Define Response Group Holiday Sets
- Create Response Group Workflows
- (Optional) Verify Response Group Deployment

⊟See Also

Other Resources

Planning for Call Management Features

1.4.3.13.3.1 Response Group Configuration Permissions and Prerequisites

Response Group Configuration Permissions and Prerequisites

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response

Group >

Topic Last Modified: *2012-10-05*

Response Group is an Enterprise Voice call management feature. This topic describes what you need to have in place before you can configure Response Group and the administrative credentials and permissions you need to perform configuration tasks.

This section assumes that you have read the planning documentation related to Response Group. For details, see Planning for Call Management Features in the Planning documentation.

Configuration Tools and Administrative Roles

You can use the following administrative tools to configure Response Group:

- Lync Server Control Panel
- Response Group Configuration Tool
- Lync Server Management Shell

To configure response groups, you must be a member of at least one of the following administrative roles:

Active Directory Security Group (1)	Create Workflow	Assign Manager	Create / assign agents, queues	Create / manage holiday and business hours	Activate / deactivate workflow	Configure workflow (IVR or Hunt Group)
CsResponseGroupAdministrator	√	√	√	√	√	√
CsResponseGroupManager		√(2)	√(3)	√(3)	√(3)	√(3)
CsVoiceAdministrator	√	√	√	√	√	√
CsServerAdministrator	√	√	√	√	√	√
CsAdministrator	√	√	√	√	√	√
CsViewOnlyAdministrator	√(4)	√(4)	√(4)	√(4)	√(4)	√(4)

Note:

(1) An Active Directory Domain Services (AD DS) user object must be a member of the specified Active Directory security group listed. An administrator or other delegated Active Directory group member with appropriate permissions to add users to a security group (For example, Administrator, Account Operators) must add a user object to the listed security group or group for the user to be able to perform the functions listed. **(2)** Only for workflows that the CsResponseGroupAdministrator has assigned to the CsResponseGroupManager. **(3)** A Response Group Manager can assign another member of CsResponseGroupManager to a workflow that the current manager already manages.

(4) CsViewOnlyAdministrator can only run verb "Get" Lync Server Management Shell cmdlets.

Response Group Configuration Prerequisites

Response Group requires the following components:

- Application service
- Response Group application
- Language packs
- File store (to hold audio files)
- Web Services (includes the Response Group Configuration Tool and the agents' sign-in and sign-out console)

All of these components are installed by default when you deploy Enterprise Voice.

You might need to perform the following tasks before configuring Response Group:

- Enable users for Lync Server 2013 and Enterprise Voice.
- Modify a configuration file to be compliant with Federal Information Processing Standards (FIPS).
- Modify the database collation to support Yi, Meng, and Zang characters for queue names and agent group names.

Enabling Users

The first step in configuring Response Group is to create agent groups. Before you can create an agent group, you must enable the users who will be agents for Response Group for Lync Server 2013 and Enterprise Voice. Enabling users for Lync Server 2013 is typically a step in the Enterprise Edition server or Standard Edition server deployment. For details about enabling users for Lync Server 2013, see Disable or Re-Enable User Account for Lync Server. Enabling users for Enterprise Voice is typically a step in the Enterprise Voice deployment. For details, see Enable Users for Enterprise Voice.

Complying with FIPS requirements

This section applies to you only if your organization needs to comply with Federal Information Processing Standards (FIPS).

To be compliant with FIPS, you need to modify the application-level Web.config file to use a different cryptography algorithm after you install Web Services. You need to specify that ASP.NET use the Triple Data Encryption Standard (3DES) algorithm to process view state data. For the Response Group application, this requirement applies to the Response Group Configuration Tool and the agent sign-in and sign-out console. For details about this requirement, see Microsoft Knowledge Base article 911722, "You may receive an error message when you access ASP.NET webpages that have ViewState enabled after you upgrade from ASP.NET 1.1 to ASP.NET 2.0," at http://go.microsoft.com/fwlink/p/?linkId=196183.

To modify the Web.config file, do the following:

1. In a text editor such as Notepad, open the application-level Web.config file.
2. In the Web.config file, locate the **<system.web>** section.
3. Add the following **<machineKey>** section to in the **<system.web>** section:

   ```
   <machineKey validationKey="AutoGenerate,IsolateApps" decryptionKey="Au
   ```

4. Save the Web.config file.
5. Restart the Internet Information Services (IIS) service by running the following command at a command prompt:

   ```
   iisreset
   ```

Supporting Yi, Meng, and Zang Characters

This section applies to you only if your organization needs to support Yi, Meng, or Zang characters.

Note:

For information on what the Yi, Meng, and Zang characters are and why they may be important to your deployment, see the information on the GB18030 character sets http://go.microsoft.com/fwlink/p/?linkId=240223.

To support Yi, Meng, or Zang characters, you need to modify the collation for the Rgsconfig database. Change the collation of the **Name** column in the following tables in each Rgsconfig database:

- dbo.AgentGroups
- dbo.BusinessHours
- dbo.HolidaySets
- dbo.Queues
- dbo.Workflows

For SQL Server 2008 R2 and SQL Server 2012, use the Latin_General_100 (Accent Sensitive) collation. If you use this collation, all object names are not case-sensitive.

You can change the collation by using Microsoft SQL Server Management Studio. For details about using this tool, see "Using SQL Server Management Studio" at http://go.microsoft.com/fwlink/p/?linkId=196184. Follow these steps to change the collation:

1. Be sure that SQL Server Management Studio is configured to allow changes that require tables to be recreated. For details, see "Save (Not Permitted) Dialog Box" at http://go.microsoft.com/fwlink/p/?linkId=196186. For details about setting a column collation, see "How to: Set Column Collation (Visual Database Tools)" at http://go.microsoft.com/fwlink/p/?linkId=196185.
2. Using Microsoft SQL Server Management Studio, connect to the Rgsconfig database.
3. Find the table you want to change in the Rgsconfig database, right-click the table, and click **Design**.
4. Change the collation of the **Name** column and save the table.

1.4.3.13.3.2 Deployment Process for Response Group

Deployment Process for Response Group

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Response Groups >

Topic Last Modified: *2012-09-27*

This section provides an overview of the phases and steps involved in deploying the Response Group application.

Response Group Deployment Process

Phase	Steps	Permissions	Deployment documentation
Install the Response Group application	The Response Group application is installed and activated by default when you deploy Enterprise Voice.	RTCUniversalServerAdmins	Deploying Enterprise Voice

Install components for Response Group	Lync Server cmdlets, the Lync Server Control Panel, Response Group Configuration Tool, agents' sign-in and sign-out console, and Response Group Client Web service are installed as part of Web Services. Web Services is installed when you deploy an Enterprise Edition pool or a Standard Edition server.	RTCUniversalServerAdmins	Deploying Lync Server 2013
Enable users for Lync 2013 and for Enterprise Voice	Enable users who will be agents for Lync Server and Enterprise Voice. Users must be enabled before you can add them to agent groups. Typically, users are enabled for Lync Server during the Enterprise Edition or Standard Edition server deployment. Users are enabled for Enterprise Voice during the Enterprise Voice deployment.	RTCUniversalUserAdmins CsUserAdministrator CsAdministrator	Disable or Re-Enable User Account for Lync Server Enable Users for Enterprise Voice
Create and configure response groups, which consist of agent groups, queues, and workflows	1. Use the Lync Server Control Panel or Lync Server Management Shell to do the following: 1.a. Create and configure agent groups. 1.b. Create and configure queues. 2. Optionally, use Lync Server Management Shell to create predefined response group business hours and holidays. 3. Use the Response Group Configuration Tool or Lync Server Management Shell to create workflows (hunt groups or interactive voice response (IVR) call flows), including custom response group business hours and holidays. **Note:** You can access the Response Group Configuration Tool through Lync Server Control Panel.	RTCUniversalServerAdmins CsResponseGroupAdministrator CsVoiceAdministrator CsServerAdministrator CsAdministrator CsResponseGroupManager	Create Response Group Agent Groups Create Response Group Queues (Optional) Define Response Group Business Hours (Optional) Define Response Group Holiday Sets Create or Modify a Workflow
(Optional) Customize application-level	Use Lync Server Management Shell to customize the default music-on-hold configuration, the default	RTCUniversalServerAdmins CsResponseGrou	Managing Application-Level Response Group

settings	music-on-hold audio file, the agent ringback grace period, and the call context configuration.	pAdministrator CsVoiceAdministrator CsServerAdministrator CsAdministrator	Settings
(Optional) Delegate management of response groups	Assign users the CsResponseGroupManager role to delegate configuration of response groups. Response Group Managers can then configure the response groups assigned to them.	RTCUniversalServerAdmins CsResponseGroupAdministrator CsVoiceAdministrator CsServerAdministrator CsAdministrator	Planning for Role-Based Access Control
Verify your Response Group deployment	Test answering calls to your hunt group and interactive voice response workflows to ensure that your configuration works as expected.	-	-

1.4.3.13.3.3 Overview of Workflow Creation Scenarios

Overview of Workflow Creation Scenarios

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-10-17*

When you create workflows, there are two possible scenarios:

- **The Administrator creates and configures the workflow** — The CsResponseGroupAdministrator role member (or equivalent) creates and activates the workflow and all elements in the workflow, such as the agent groups, queues, holiday and business hours, music on hold, and so on.
- **The Administrator creates the workflow and the Manager configures options** — The CsResponseGroupAdministrator role member (or equivalent) defines the primary SIP URI, Display Name, assigns a member or members of the CsResponseGroupManager role, and selects a queue and activates the workflow. The CsResponseGroupManager can then log on and edit the configuration of the workflow by creating agent groups and also assigns the group to the queue, configuring the telephone number, holiday and business hours, music on hold, and so on.

Note:

When you want to create a managed workflow, you need to create the workflow as active. After you save an active, managed workflow, you can then modify and deactivate the workflow.

1.4.3.13.3.4 Create Response Group Agent Groups

Create Response Group Agent Groups

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-09-12*

When you create an agent group, you select the agents that are assigned to the group and specify additional group settings, such as the routing method and whether an agent can sign in to and out of the group.

An agent who must sign in and out of the group, which is different from signing in or out of Lync Server, is called a *formal agent*. Formal agents must be signed in to the group before they can receive calls routed to the group. This can be useful for agents who answer calls from the group on a part-time basis. Formal agents sign in and out of their groups by clicking a menu item in Lync 2013 to open the Windows Internet Explorer Internet browser and display a webpage console.

An agent who does not sign in or out of the group is called an *informal agent*. Informal agents are automatically signed in to the group when they sign in to Lync Server, and they cannot sign out of the group.

Note:

Only on-premises users can be agents. If an agent is moved from on-premises to online, Response Group calls will not be routed to that agent.

Create or Modify an Agent Group

Create or Modify an Agent Group

See Also

Deploying Call Management Features > Configuring Response Group > Create Response Group Agent Groups >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to create or modify an agent group.

Note:

An Administrator—for example, CsVoiceAdministrator—must enable users for Enterprise Voice and Lync Server before the users can be assigned to agent groups. If you are one of the delegated Response Group Managers for a managed workflow, you can create agent groups and use the agent groups in the workflows that you manage.

Important:

When you assign users as response group agents, inform them that, if they have Privacy mode enabled, they need to search for "RGS Presence Watcher" contacts and add them to their Contacts list. Agents who have Privacy mode enabled, but who do not have "RGS Presence Watcher" in their Contacts list, cannot receive calls to the response group. Agents who do not have Privacy mode enabled are not affected.

⊟To use Lync Server Control Panel to create or modify an agent group

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.

   Note:
   If you are one of the delegated Response Group Managers for a managed workflow, you can create groups and use them in the workflows that you manage.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Group**.
4. On the **Group** page, do one of the following:
   - To create a new agent group, click **New**. In the **Select a Service** search field, type all or part of the name of the **ApplicationServer** service where you want to add the group. In the resulting list of services, click the service that you want, and then click **OK**.
   - To modify an existing agent group, type all or part of the name of the agent group in the search field. In the resulting list, click the group that you want, click **Edit**, and then click **Show details**.
5. In **Name**, type an identifying name for the agent group.
6. In **Description**, type a description for the group.
7. In the **Participation policy**, select one of the following to set up the sign-in behavior for the group:
   - Select **Informal** to specify that agents in the group do not need to sign in and out of the group. Agents are automatically signed in to the group when they sign in to Lync Server 2013.
   - Select **Formal** to specify that agents in the group must sign in and out of the group. When you select this option, agents click a menu item in Lync to open Internet Explorer and display a webpage console for signing in and out of the group.
8. In **Alert time (seconds)**, specify the number of seconds to ring an agent before offering the call to the next available agent (the default is 20 seconds).

   Important:
   The agent alert time setting cannot exceed 180 seconds. If the agent alert time exceeds 180 seconds, the client application rejects the call because the SIP transaction timer reaches its maximum wait time.

9. In **Routing method**, select the method for routing calls to agents in the group as follows:
   - To offer a new call first to the agent who has been idle the longest (has had a presence of **Available** or **Inactive** in Lync Server the longest), click **Longest idle**.
   - To offer a new call to all available agents at the same time, click **Parallel**. The call is sent to the first agent who accepts it.
   - To offer a new call to each agent in turn, click **Round robin**.
   - To always offer a new call to the agents in the order in which they are listed in the **Agent** list, click **Serial**.
   - To offer a new call to all agents who are signed into Lync Server 2013 and the Response Group application at the same time, regardless of their current presence, click **Attendant**. Lync 2010 Attendant users who are configured as agents can see all the calls that are waiting and answer waiting calls in any order. The call is sent to the first agent who accepts it, after which the other Lync 2010 Attendant users no longer see the call.
10. In **Agents**, specify how you want to create your agents list:
    - To use a custom list of agents, click **Define a custom group of agents**, and do one of the following:

    - To add a user to the agent group, click **Select**, and then in the **Select Agents** search field, type all or part of the name of the user that you want to add to this group, and then click **Find**. In the resulting list of agents, click the user, and then click **OK**.
    - To remove a user from the agent group, in the list of agents, click the user you want to remove, and then click **Remove**.
    - To change the order in which agents are offered calls in groups that use either round robin routing or serial routing, in the list of agents, click a user, and then click the up arrow or down arrow.
- To use a Microsoft Exchange Server distribution list as your agent group, click **Use an existing email distribution list**, and then in **Distribution list address**, type the email address of the distribution list (for example, NetworkSupport@contoso.com).

  If you use an email distribution list, you are subject to the following constraints:

    - You cannot select multiple distribution lists for the agent group. Each group supports only a single distribution list.
    - If the distribution list contains one or more distribution lists, members of the nested distribution lists are not added to the agent list.
    - If serial or round robin routing is selected, the server offers an incoming call to the appropriate agent according to the routing method and according to the order in which agents are listed in the distribution list.

> **Important:**
> If you use an email distribution list, hidden memberships or hidden lists might become visible to the Response Group administrator or users.

  Hidden memberships or hidden lists can become visible as follows:

    - If a distribution list was configured so that the membership is hidden and the Response Group administrator assigns the distribution list to the agent list, users can call the group to find out who the members are.
    - If a distribution list was configured so that it is hidden in the Exchange Global Address List, the Response Group administrator might be able to see the distribution list and assign it to the agent list if the Response Group process has the appropriate user rights and permissions, even if the administrator does not have the appropriate user rights and permissions.

11. Click **Commit**.

To use Windows PowerShell to create or modify an agent group

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Retrieve the service name for the Response Group service and assign it to a variable. At the command line, run:

```
$serviceId="service:"+(Get-CsService | ?{$_.Applications -Like "*RGS*"
```

> **Note:**
> If you run **Get-CsService** in a topology that has multiple pools, the variable $serviceId returns an array of all the service elements found in the topology.

4. Use **New-CsRgsAgentGroup** to create a new agent group. Use **Set-CsRgsAgentGroup** to modify an existing agent group. At the command line, run:

```
$ag = New-CsRgsAgentGroup -Name "<agent group name>" -Parent $serviceI
```

For example:

```
$ag = New-CsRgsAgentGroup -Name "Help Desk" -Parent $serviceId -Descri
```

> **Important:**
> The agent alert time setting cannot exceed 180 seconds. If the agent alert time is greater than 180 seconds, the client application rejects the call because the SIP transaction timer reaches its maximum wait time.

5. Confirm that the agent group is created. Run:

```
Get-CsRgsAgentGroup -Name "Help Desk"
```

Tasks

Delete an Agent Group

Other Resources

Managing Response Group Agent Groups
Get-CsService
New-CsRgsAgentGroup
Set-CsRgsAgentGroup
Get-CsRgsAgentGroup

1.4.3.13.3.5 Create Response Group Queues

Create Response Group Queues

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-01-18*

Queues hold callers until an agent answers the call. When the Response Group application searches for an available agent, it searches agent groups in the order that you list them. You can select the agent groups that are assigned to the queue and specify queue behavior, such as limiting the number of calls that the queue can hold and the period of time that a call waits until an agent answers the call.
Create or Modify a Queue

Create or Modify a Queue

See Also

Deploying Call Management Features > Configuring Response Group > Create Response Group Queues >

Topic Last Modified: *2013-02-23*

Use one of the following procedures to create or modify a queue.

⊟To use Lync Server Control Panel to create or modify a queue

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.

> **Note:**
> If you are one of the delegated Response Group Managers for a managed workflow, you can create or modify response group queues and assign them to the workflows that you manage.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Queue**.
4. On the **Queue** page, do one of the following:

- To create a new queue, click **New**. In **Select a Service**, type part or all of the name of the **ApplicationServer** service where you want to add the queue in the search field. In the resulting list of services, click the service that you want, and then click **OK**.
- To modify an existing queue, type all or part of the queue name in the search field. In the resulting list of queues, click the queue that you want, click **Edit**, and then click **Show details**.

5. In **Name**, type an identifying name for the queue.
6. In **Description**, type a description for the queue.
7. In **Groups**, specify the groups you want to assign to the queue. Do one of the following:
   - To add a group to the queue, click **Select**. In the **Select Groups** search field, type all or part of the name of the agent group that you want to assign to the queue, click the agent group that you want, and then click **OK**.
   - To remove a group from the queue, in the list of agent groups, click the group that you want to remove, and then click **Remove**.
   - To change the order in which agents are searched, in the list of agent groups, click a group, and then click the up arrow or down arrow.

   > **Note:**
   > When the server searches for an available agent for the queue, it uses group order. That is, the first group in the list is searched first, followed by the second group in the list, and so on.

8. To specify a maximum period of time for a caller to wait on hold before an agent answers the call, select the **Enable queue time-out** check box, and then do the following:
   - In **Time-out period (seconds)**, specify the maximum number of seconds a caller waits for an agent to answer the call.
   - In **Call Action**, select the action that occurs when a call times out as follows:
   - To disconnect the call after the timeout, click **Disconnect**.
   - To forward the call to voice mail, click **Forward to voice mail**, and then in the **SIP address** field, type a voice mail address in the format sip:<*username*>@<*domainname*> (for example, sip:bob@contoso.com).
   - To forward the call to another telephone number, click **Forward to telephone number**, and then in the **SIP address** field, type the telephone number in the format sip:<*number*>@<*domainname*> (for example, sip:+14255550121@contoso.com).
   - To forward the call to another user, click **Forward to SIP address**, and then in the **SIP address** field, type the URI for the user in the format sip:<*username*>@<*domainname*>.
   - To forward the call to another queue, click **Forward to another queue**, and then browse to the queue that you want to use.
9. To specify a maximum number of calls that the queue can hold, select the **Enable queue overflow** check box, and then do the following:
   - In **Maximum number of calls**, select the maximum number of calls that you want the queue to hold.
   - In **Forward the call**, select which call is to be forwarded when the queue is full: **Newest Call** or **Oldest Call**.
   - In **Call action**, select the action that occurs when the overflow threshold is met as follows:
   - To disconnect the call after the timeout, click **Disconnect**.
   - To forward the call to voice mail, click **Forward to voice mail**, and then in the **SIP address** field, type a voice mail address in the format sip:<*username*>@<*domainname*> (for example, sip:bob@contoso.com).
   - To forward the call to another telephone number, click **Forward to telephone number**, and then in the **SIP address** field, type the telephone number in the format sip:<*number*>@<*domainname*> (for example,

sip:+14255550121@contoso.com).

- To forward the call to another user, click **Forward to SIP address**, and then in the **SIP address** field, type the URI for the user in the format sip:<*username*>@<*domainname*>.
- To forward the call to another queue, click **Forward to another queue**, and then browse to the queue that you want to use.

10.Click **Commit**.

To use Windows PowerShell to create or modify a queue

1.Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.

> **Note:**
> If you are one of the delegated Response Group Managers for a managed workflow, you will be able to create agent groups and queues, and assign agent groups to queues.

2.Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

3.Create the prompt to be played when the queue timeout threshold is met, and save it in a variable. At the command line, run:

```
$promptTO = New-CsRgsPrompt -TextToSpeechPrompt "<text for TTS prompt>
```

For example:

```
"All agents are currently busy. Please call back later."
```

> **Note:**
> To use an audio file for the prompt, use the **Import-CsRgsAudioFile** cmdlet. For details, see Import-CsRgsAudioFile.

4.Define the action to be taken when the queue timeout threshold is met, and save it in a variable. At the command line, run:

```
$actionTO = New-CsRgsCallAction -Prompt <saved prompt from previous st
```

> **Note:**
> For details about possible actions and their syntax, see New-CsRgsCallAction.

For example:

```
$action = New-CsRgsCallAction -Prompt $promptTO -Action Terminate
```

5.Create the prompt to be played when the queue overflow threshold is met, and save it in a variable. At the command line, run:

```
$promptOV = New-CsRgsPrompt -TextToSpeechPrompt "<text for TTS prompt>
```

For example:

```
$promptOV = New-CsRgsPrompt -TextToSpeechPrompt "Too many calls are wa
```

> **Note:**
> To use an audio file for the prompt, use the **Import-CsRgsAudioFile** cmdlet. For details, see Import-CsRgsAudioFile.

6.Define the action to be taken when the queue overflow threshold is met, and save it in a variable. At the command line, run:

```
$actionOV = New-CsRgsCallAction -Prompt <saved prompt from previous st
```

> **Note:**
> For details about possible actions and their syntax, see New-CsRgsCallAction.

For example:

```
$action = New-CsRgsCallAction -Prompt $promptOV -Action Terminate
```

7. Retrieve the service name for the Response Group service and assign it to a variable. At the command line, run:

```
$serviceId="service:"+(Get-CSService | ?{$_.Applications -Like "*RGS*"
```

8. Get the identity of the agent group to be assigned to the queue. At the command line, run:

```
$agid = (Get-CsRgsAgentGroup -Name "Help Desk").Identity;
```

Note:
For details about creating the agent group, see New-CsRgsAgentGroup

9. Create the queue. At the command line, run:

```
$q = New-CsRgsQueue -Parent <saved service ID from previous step> -Nam
```

For example:

```
$q = New-CsRgsQueue -Parent $serviceId -Name "Help Desk" -Description
```

10. Confirm that the queue is created. Run:

```
Get-CsRgsQueue -Name "Help Desk"
```

Other Resources

New-CsRgsQueue
Set-CsRgsQueue
New-CsRgsPrompt
New-CsRgsCallAction
Get-CsRgsQueue
Import-CsRgsAudioFile
Remove-CsRgsQueue

1.4.3.13.3.6 (Optional) Define Response Group Business Hours

(Optional) Define Response Group Business Hours

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-11-01*

Defining Business Hours

Business hour settings define when the workflow is available to answer calls and specify the actions to take for calls outside of business hours. Response Group administrators can use the **New-CsRgsHoursOfBusiness** cmdlet to create predefined schedules that you can use for any number of response groups.

Tip:
When you create or modify a workflow, you can specify a custom schedule that applies only to that workflow. For details, see Create or Modify a Hunt Group Workflow or Create or Modify an Interactive Workflow.

Note:
If a workflow is defined as a Managed workflow, then any user who is assigned the CsResponseGroupManager role can set and modify custom business hours for workflows that they manage.

Important:

Use 24-hour notation for the parameters in the following cmdlets (for example, 20:00=8:00 P.M.).

To create a predefined business hours collection

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. For each unique range of hours you want to define, run:

   ```
   $x = New-CsRgsTimeRange [-Name <name of time range>] -OpenTime <time w
   ```

   To create the business hours collection that uses the ranges you defined, run:

   ```
   New-CsRgsHoursOfBusiness -Parent <service where the workflow is hosted
   ```

   The following example specifies business hours of 9:00 A.M. to 5:00 P.M. for weekdays, 8:00 A.M. to 10:00 A.M. and again from 2:00 P.M. to 6:00 P.M. for Saturdays, and no business hours for Sundays:

   ```
   $a = NewRgsTimeRange -Name "Weekday Hours" -OpenTime "9:00" -CloseTime
   $b = NewRgsTimeRange -Name "Saturday Morning Hours" -OpenTime "8:00" -
   $c = NewRgsTimeRange -Name "Saturday Afternoon Hours" -OpenTime "14:00
   New-CsRgsHoursOfBusiness -Parent "ApplicationServer:Redmond.contoso.co
   ```

See Also

Concepts

Create or Modify a Hunt Group Workflow
Create or Modify an Interactive Workflow

Other Resources

New-CsRgsTimeRange
New-CsRgsHoursOfBusiness

1.4.3.13.3.7 (Optional) Define Response Group Holiday Sets

(Optional) Define Response Group Holiday Sets

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-11-01*

Holiday settings define the days that a response group is closed for business and specify the action to take on those days. A holiday set is the collection of holidays that apply to a response group.

Note:

If a workflow is defined as a Managed workflow, then any user is assigned the CsResponseGroupManager role can set and modify holidays for workflows that they manage.

To create a holiday set

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

3. For each holiday you want to define, run:

```
$x = New-CsRgsHoliday [-Name <holiday name>] -StartDate <starting date
```

To create the holiday set that contains the holidays you defined, run:

```
New-CsRgsHolidaySet -Parent <service where the workflow is hosted> -Na
```

The following example shows a holiday set that includes two holidays:

```
$a = New-CsRgsHoliday -Name "New Year's Day" -StartDate "1/1/2013" -En
$b = New-CsRgsHoliday -Name "Independence Day" -StartDate "7/4/2013" -
New-CsRgsHolidaySet -Parent "ApplicationServer:Redmond.contoso.com -Na
```

Concepts

Create or Modify a Hunt Group Workflow
Create or Modify an Interactive Workflow

Other Resources

New-CsRgsHoliday
New-CsRgsHolidaySet

1.4.3.13.3.8 Create Response Group Workflows

Create Response Group Workflows

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-09-12*

A workflow defines the behavior of a call from the time that the phone rings to the time that someone answers the call. The workflow specifies the queue to use for holding the call, and specifies the routing method to use for hunt groups or the questions and answers to use for interactive response groups. A workflow also defines settings such as a welcome message, music on hold, business hours, and holidays.

You use the Response Group Configuration Tool to create workflows. You can access the Response Group Configuration Tool from the Response Group page of Lync Server Control Panel.

> **Note:**
> You must create agent groups and queues before you create a workflow that uses them.

- Create or Modify a Hunt Group Workflow
- Design Interactive Voice Response Call Flows
- Create or Modify an Interactive Workflow

Related Sections

- Create Response Group Agent Groups
- Create Response Group Queues

Create or Modify a Hunt Group Workflow

See Also

Deploying Call Management Features > Configuring Response Group > Create Response Group Workflows >

Topic Last Modified: *2012-11-27*

Use one of the following procedures to create or modify a hunt group workflow.

Note:

You can use Lync Server Management Shell or the Response Group Configuration Tool to create and modify hunt group workflows. You can access the Response Group Configuration Tool from Lync Server Control Panel, or by opening the webpage directly from a web browser by typing the following URL: **https://***<webPoolFqdn>***/RgsConfig**.

To use Response Group Configuration Tool to create or modify a hunt group workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Workflow**.
4. On the **Workflow** page, click **Create or edit a workflow**.
5. In the **Select a Service** search field, type all or part of the name of the **ApplicationServer** service that hosts the workflow that you want to create or change. In the resulting list of services, click the service that you want, and then click **OK**.

   Note:

   The Response Group Configuration Tool opens. You can also open the Response Group Configuration Tool directly from a web browser by typing the following URL: **https://***<webPoolFqdn>***/RgsConfig**.
6. Do one of the following:
   - Under **Create a New Workflow**, next to **Hunt Group, click Create**.
   - Under **Manage an Existing Workflow**, locate the workflow you want to change, and then under **Action**, click **Edit**.
7. If you are ready for users to start calling the workflow, select **Activate the workflow**.

   Note:

   If you are to creating a managed workflow, you need to select **Activate the workflow**. After you save the active, managed workflow, you can then modify and deactivate it.
8. To allow federated users to call the group, select the **Enable for federation** check box. You must also have an external access policy that applies to the Response Group application configured for federation.

   Note:

   The global external access policy applies to the Response Group application. You can configure the global policy for response group federation by using Lync Server Control Panel or by using the **Set-CsExternalAccessPolicy** cmdlet to set the EnableOutsideAccess parameter to True. Keep in mind that global policy settings apply to all users unless they are assigned a site or user policy. Therefore, before changing this setting for response groups, make sure that the federation setting meets the requirements of your organization. For details about how policies apply to users, see Manage External Access Policy for Your Organization. For details about the federation setting, see Set-CsExternalAccessPolicy.
9. To hide the identity of agents during calls, select the **Enable agent anonymity** check box.

   Note:

   Anonymous calls cannot start with instant messaging (IM) or video, although

> the agent or the caller can add IM and video after the call is established. An anonymous agent can also put calls on hold, transfer calls (both blind and consultative transfers), and park and retrieve calls. Anonymous calls do not support conferencing, application sharing and desktop sharing, file transfer, whiteboarding and data collaboration, and call recording. Agents using the Lync VDI Plugin can receive incoming calls anonymously, but they cannot make outgoing calls anonymously.

10.Under **Enter the address of the group that will receive the calls**, type the primary SIP uniform resource identifier (URI) address of the group that will answer calls to the workflow.

> **Note:**
>
> The primary URI for a workflow is how the workflow is identified and referenced. The SIP URI that you enter is created as a contact object in Active Directory Domain Services (AD DS). To create the URI, the object must be unique in Active Directory.

11.In **Display name**, type the name that you want to display for the workflow (for example, Sales Response Group).

> **Note:**
>
> Do not include the "<" or ">" characters in the display name. Do not use the following display names because they are reserved: **RGS Presence Watcher** or **Announcement Service**.

12.Under **Telephone number**, type the line URI for the response group (for example, +14255550165).

13.In **Display number**, type the number as you want it to appear for the response group (for example, +1 (425) 555-0165).

14.(Optional) In **Description**, type a description for the workflow as you want it to appear on the contact card in Lync client.

15.In **Workflow Type**, select **Managed** if this workflow will be managed by a Response Group Manager. Do the following to assign Response Group Managers to the workflow:

- Type the SIP URI of a manager for this workflow, and click **Add**.
- Type the SIP URI of additional managers to add to the workflow, and click **Add**.

> **Important:**
>
> Every user who is designated as a manager of a response group must be assigned the CsResponseGroupManager role. If users are not assigned this role, they cannot manage response groups.

16.Under **Step 2 Select a Language**, click the language that you want to use for speech recognition and text-to-speech.

17.If you want to configure a welcome message, under **Step 3 Configure a Welcome Message**, select the **Play a welcome message** check box, and then do one of the following:

- To enter the welcome message as text that is converted to speech for callers, click **Use text-to-speech**, and then type the welcome message in the text box.

  > **Note:**
  >
  > Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use a wave (.wav) or Windows Media audio (.wma) file recording for the welcome message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the audio file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

  > **Note:**

> All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

18. Under **Step 4 Specify Your Business Hours**, in **Your time zone**, click the time zone for the workflow.

> **Note:**
> The time zone is the time zone where the callers and agents of the workflow reside. It is used to calculate the open and close hours. For example, if the workflow is configured to use the North American Eastern Time zone and the workflow is scheduled to open at 7:00 A.M. and close at 11:00 P.M., the open and close times are assumed to be 7:00 Eastern Time and 23:00 Eastern Time respectively. (You must enter the times in 24-hour time notation.)

19. Select the type of business hours schedule you want to use by doing one of the following:
    - To use a predefined schedule of business hours, click **Use a preset schedule**, and then select the schedule you want to use from the drop-down list.

      > **Note:**
      > You must have defined at least one preset schedule previously to be able to select this option. You define preset schedules by using the **New-CSRgsHoursOfBusiness** cmdlet. For details, see (Optional) Define Response Group Business Hours.

      > **Note:**
      > When you select a preset schedule, **Day**, **Open**, and **Close** are automatically filled with the days and hours that the response group is available.

    - To use a custom schedule that applies only to this workflow, click **Use a custom schedule**.
20. If you are creating a custom schedule for this workflow, click the check boxes for the days of the week that the response group is available.
21. If you are creating a custom schedule, type the **Open** and **Close** hours for each day of the week that the response group available.

> **Note:**
> The **Open** and **Close** hours must be in 24-hour time notation. For example, if your office works a 9-to-5 work day and closes at noon for lunch, the business hours are specified as **Open** 9:00, **Close** 12:00, **Open** 13:00, and **Close** 17:00.

22. If you want to play a message when the office is not open, select the **Play a message when the response group is outside of business hours** check box, and then specify the message to play by doing one of the following:
    - To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

      > **Note:**
      > Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

    - To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

      > **Note:**
      > All user-provided audio files must meet certain requirements. For details about supported audio file formats, see Technical

> Requirements for Response Groups.

23.Specify how to handle calls after the message is played (if a message is configured):

- To disconnect the call, click **Disconnect Call**.
- To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is *<username>*@*<domainName>* (for example, bob@contoso.com).
- To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is *<username>*@*<domainName>*.
- To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is *<number>*@*<domainName>* (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.

24.Under **Step 5 Specify Your Holidays**, click the check boxes for one or more sets of holidays that define the days when the response group is closed for business.

> **Note:**
> You need to define holidays and holiday sets before you configure the workflow. Use the **New-CsRgsHoliday** and **New-CsRgsHolidaySet** cmdlets to define holidays and holiday sets. For details, see (Optional) Define Response Group Holiday Sets.

25.If you want to play a message on holidays, select the **Play a message during holidays** check box, and then specify the message to play by doing one of the following:

- To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

> **Note:**
> Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

> **Note:**
> All user-provided audio files must meet certain requirements. For details about supported audio file formats, see Technical Requirements for Response Groups.

26.Specify how to handle calls after the message is played (if a message is configured):

- To disconnect the call, click **Disconnect Call**.
- To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is *<username>*@*<domainName>* (for example, bob@contoso.com).
- To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is *<username>*@*<domainName>*.
- To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is *<number>*@*<domainName>* (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.

27.Under **Step 6 Configure a Queue**, in **Select the queue that will receive the calls**, select the queue that you want to hold callers until an agent becomes available.

28. Under **Step 7 Configure Music on Hold**, choose the music you want callers to listen to while waiting for an agent by doing one of the following:
    - To use the default music-on-hold recording, click **Use default**.
    - To use an audio file recording for the music on hold, click **Select a music file**. If you want to upload a new audio file, click the **a music file** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

> **Note:**
> All user provided audio files must meet certain requirements. For details about supported audio file formats, see Technical Requirements for Response Groups.

29. Click **Deploy**.

To use Windows PowerShell to create or modify a hunt group workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Create the prompt to be played for the welcome message, and save it in a variable. At the command line, run:

```
$promptWM = New-CsRgsPrompt -TextToSpeechPrompt "<text for TTS prompt>
```

For example:

```
$promptWM = New-CsRgsPrompt -TextToSpeechPrompt "Welcome to Contoso. P
```

> **Note:**
> To use an audio file for the prompt, use the **Import-CsRgsAudioFile** cmdlet. For details, see Import-CsRgsAudioFile.

4. Get the identity of the queue or question where the calls will be directed. At the command line, run:

```
$qid = (Get-CsRgsQueue -Name "Help Desk").Identity
```

For details about creating the queue, see New-CsRgsQueue.

5. Define the default action to be taken when a workflow is opened during business hours, and save it in a variable. At the command line, run:

```
$actionWM = New-CsRgsCallAction -Prompt <saved prompt from previous st
```

> **Note:**
> For hunt group workflows, the default action must direct the call to a queue. This is parameter is required for active workflows. It is not required for inactive workflows.

For example:

```
$actionWM = New-CsRgsCallAction -Prompt $promptWM -Action TransferToQu
```

6. If you want to define business hours and holidays, you need to create them before you create or modify the workflow. For details, see (Optional) Define Response Group Business Hours and (Optional) Define Response Group Holiday Sets.
7. If you want to have prompts for calls that are received out of business hours or on holidays, use the **New-CsRgsPrompt** cmdlet to define the prompt, and use the **New-CsRgsCallAction** to define the action to be taken after the prompt. For details, see New-CsRgsPrompt and New-CsRgsCallAction.
8. Retrieve the service name for the Lync Server Response Group service and assign it to a variable. At the command, run:

```
$serviceId="service:"+(Get-CSService | ?{$_.Applications -like "*RGS*"
```

9. Create or modify the workflow. To create a workflow, use **New-CsRgsWorkflow**. To modify a workflow, use **Set-CsRgsWorkflow**. At the command line, type:

   ```
   $workflowHG = New-CsRgsWorkflow -Parent <service ID for the Response G
   ```

   For example:

   ```
   $workflowHG = New-CsRgsWorkflow -Parent $serviceID -Name "Human Resour
   ```

   > **Important:**
   > All users who are designated managers for workflows must be assigned the CsResponseGroupManager role.

   > **Note:**
   > For details about additional optional parameters, see New-CsRgsWorkflow or Set-CsRgsWorkflow

See Also

Tasks

(Optional) Define Response Group Holiday Sets

Concepts

(Optional) Define Response Group Business Hours

Other Resources

New-CsRgsWorkflow
Set-CsRgsWorkflow
New-CsRgsPrompt
New-CsRgsCallAction

Design Interactive Voice Response Call Flows

Deploying Call Management Features > Configuring Response Group > Create Response Group Workflows >

Topic Last Modified: *2013-02-25*

You can use interactive voice response (IVR) to obtain information from callers and direct the call to the appropriate queue. Question-and-answer pairs determine which queue to use. Depending on the caller's response, the caller either hears a follow-up question, or is routed to the appropriate queue. The IVR questions and the caller's responses are provided to the responding agent who accepts the call, providing valuable information to the agent.

Overview of IVR Features

The Response Group application offers speech recognition and text-to-speech capabilities in 26 languages. You can enter IVR questions using text-to-speech or a wave (.wav) or Windows Media audio (.wma) file. Callers can respond by using voice or dual-tone multifrequency (DTMF) responses.

Interactive workflows support up to two levels of questions, with each question having up to four possible answers. The IVR asks the caller a question, and depending on the caller's response, routes the caller to a queue or asks a second question. The second question can also have four possible answers. Depending on the answer to the second-level question, the caller is routed to the appropriate queue.

> **Note:**

When you design call flows by using Lync Server Management Shell, you can define any number levels of IVR questions and any number of answers. However, for caller usability, we recommend that you not use more than three levels of questions, with not more than five answers each. In addition, if you design a call flow that has more than two levels of questions with more than four answers each, you cannot edit the call flow by using Lync Server 2013 Control Panel.

The IVR questions and the caller's responses are provided to the responding agent who accepts the call.

Working with Speech Technologies

Speech technologies, such as speech recognition and text-to-speech, can enhance customer experience and let people access information more naturally and effectively. However, there can be cases where the specified text or the user voice response is not recognized correctly by the speech engine. For example, the "#" symbol is translated by the text-to-speech engine as the word "number." This issue can be mitigated by the following:

- The speech engine gives the caller five attempts to answer the question. If the caller answers the question incorrectly (that is, the answer is not one of the specified responses) or does not provide an answer at all, the caller gets another chance to answer the question. The caller has five attempts to answer the question before being disconnected. You can configure the IVR to play a customized message after each caller error. The question is repeated each time.
- To minimize the potential for ambient noise to be interpreted by the speech engine as a response, use longer responses. For example, responses should have more than one syllable and should sound significantly different from each other.
- If your questions have both speech and DTMF responses, configure the speech responses with words that represent the concept rather than the DTMF response. For example, instead of using "Press or say one" use "Press 1 or say billing."
- After you design your IVR, call the workflow, listen to the prompts, respond to each of the prompts using voice, and verify that the IVR sounds and behaves as expected. You can then modify the IVR to fix any interpretation issues. Following the previous example, if you need to refer to the # key, you can rewrite your IVR prompt to use the key name, rather than the # symbol. For example, "To talk to sales, press the pound key."

IVR Design Examples

The following sections contain examples of different IVR scenarios and question-and-answer pairs.

IVR with One Level of Questions

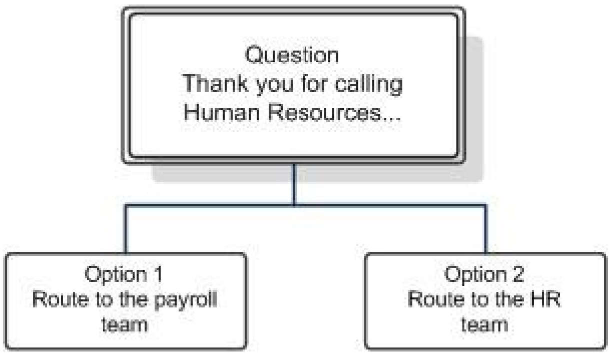
The following example shows an IVR that uses one level of questions. It uses speech recognition to detect the caller's response.

Question: "Thank you for calling Human Resources. If you would like to speak to payroll, say payroll. Otherwise, say HR."

- **Option 1 is selected:** The caller is routed to the payroll team.
- **Option 2 is selected:** The caller is routed to the human resources team.

The following figure shows the call flow.

One-level interactive call flow



IVR with Two Levels of Questions

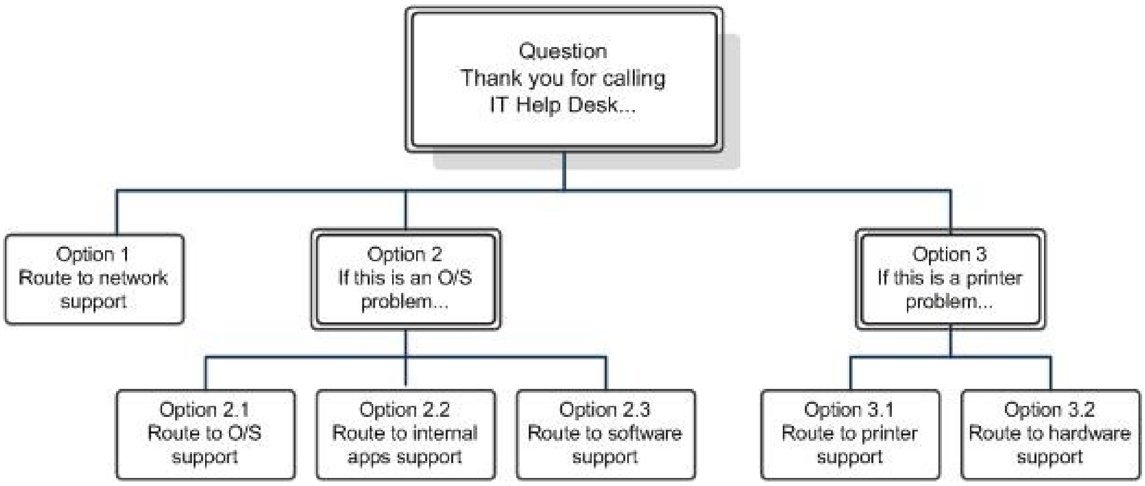
The following example shows an IVR that uses two levels of questions. It allows callers to respond using either speech or DTMF keypad input.

Question: "Thank you for calling the IT Help Desk. If you have a network access problem, press 1 or say network. If you have a software problem, press 2 or say software. If you have a hardware problem, press 3 or say hardware."

- **Option 1 is selected:** The caller is routed to the network support team.
- **Option 2 is selected:** The caller is asked a follow-up question:
  Question: "If this is an operating system problem, press 1 or say operating system. If this is a problem with an internal application, press 2 or say internal application. Otherwise, press 3 or say other."
  - **Option 1 is selected:** The caller is routed to the operating systems support team.
  - **Option 2 is selected:** The caller is routed to the internal applications support team.
  - **Option 3 is selected:** The caller is routed to the software support team.
- **Option 3 is selected:** The caller is asked a follow-up question:
  Question: "If this is a printer problem press 1. Otherwise, press 2."
  - **Option 1 is selected:** The caller is routed to the printer support team.
  - **Option 2 is selected:** The caller is routed to the hardware support team.

The following figure shows the call flow.

Two-level interactive call flow



Best Practices

The following list describes some best practices for designing your IVR:

- Let the caller get to the task quickly. Avoid providing too much information or lengthy marketing messages in your IVR.
- If you want to include a lengthy message, consider appending it to the first question instead of to the welcome message. Callers can bypass the message if it is part of the first question by answering the question, but they cannot bypass the welcome message.
- Speak in the caller’s language. Avoid stilted language. Speak naturally.
- Write efficient and effective prompts. Remove any unnecessary options. Structure the information so that the caller’s expected response is at the end of the sentence. For example, “To speak to the sales team, press 1."
- Make voice responses user friendly. For example, if you specify both DTMF and voice responses, use something like: "To speak to the sales team, press 1 or say sales."
- Test the IVR on a group of users before you deploy it across your organization.

Create or Modify an Interactive Workflow

Deploying Call Management Features > Configuring Response Group > Create Response Group Workflows >

Topic Last Modified: *2012-11-27*

Use one of the following procedures to create or modify an interactive workflow.

Note:
You can use Lync Server Management Shell or the Response Group Configuration Tool to create and modify interactive workflows. You can access the Response Group Configuration Tool from Lync Server Control Panel, or by opening the webpage directly from a web browser by typing the following URL: **https://***<webPoolFqdn>***/RgsConfig**.

To use Response Group Configuration Tool to create or modify an Interactive workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Workflow**.
4. On the **Workflow** page, click **Create or edit a workflow**.
5. In the **Select a Service** search field, type all or part of the name of the **ApplicationServer** service that hosts the workflow that you want to create or modify. In the resulting list of services, click the service that you want, and then click **OK**.

   Note:
   The Response Group Configuration Tool opens. You can also open the Response Group Configuration Tool directly from a web browser by typing the following URL: **https://***<webPoolFqdn>***/RgsConfig**.

6. Do one of the following:
   - Under **Create a New Workflow**, next to **Interactive**, click **Create**.
   - Under **Manage an Existing Workflow**, locate the workflow you want to change, and then under **Action**, click **Edit**.
7. If you are not ready for users to start calling the workflow, clear the **Activate**

the workflow check box.

> **Note:**
> If you are to creating a managed workflow, you need to select **Activate the workflow**. After you save the active, managed workflow, you can then modify and deactivate it.

8. To allow federated users to call the group, select the **Enable for federation** check box. You must also have an external access policy that applies to the Response Group application configured for federation.

> **Note:**
> The global external access policy applies to the Response Group application. You can configure the global policy for response group federation by using Lync Server Control Panel or by using the **Set-CsExternalAccessPolicy** cmdlet to set the EnableOutsideAccess parameter to True. Keep in mind that global policy settings apply to all users unless they are assigned a site or user policy. Therefore, before changing this setting for response groups, make sure that the federation setting meets the requirements of your organization. For details about how policies apply to users, see Manage External Access Policy for Your Organization. For details about the federation setting, see **Set-CsExternalAccessPolicy** in Lync Server Management Shell documentation.

9. To hide the identity of agents during calls, select the **Enable agent anonymity** check box.

> **Note:**
> Anonymous calls cannot start with instant messaging (IM) or video, although the agent or the caller can add IM and video after the call is established. An anonymous agent can also put calls on hold, transfer calls (both blind and consultative transfers), and park and retrieve calls. Anonymous calls do not support conferencing, application sharing and desktop sharing, file transfer, whiteboarding and data collaboration, and call recording. Agents using the Lync VDI Plugin can receive incoming calls anonymously, but they cannot make outgoing calls anonymously.

10. Under **Enter the address of the group that will receive the calls**, type the primary SIP uniform resource identifier (URI) address of the group that will answer calls to the workflow.
11. In **Display name**, type the name that you want to display for the workflow (for example, Sales IVR Response Group).

> **Note:**
> Do not include the "<" or ">" characters in the display name. Do not use the following display names because they are reserved: RGS Presence Watcher or Announcement Service.

12. In **Telephone number**, type the line URI for the response group (for example, +14255550165).
13. In **Display number**, type the number as you want it to appear for the response group (for example, +1 (425) 555-0165).
14. (Optional) In **Description**, type a description for the workflow that you want to appear on the contact card in the Lync client.
15. In **Workflow Type**, select **Managed** if this workflow will be managed by a Response Group Manager. Do the following to assign Response Group Managers to the workflow:
    - Type the SIP URI of a manager for this workflow, and click **Add**..
    - Type the SIP URI of additional managers to add to the workflow, and click **Add**..

> **Important:**
> Every user who is designated as a manager of a response group must be assigned the CsResponseGroupManager role. If users are not assigned this

role, they cannot manage response groups.

16. Under **Step 2 Select a Language**, click the language to use for speech recognition and text-to-speech.
17. If you want to configure a welcome message, under **Step 3 Configure a Welcome Message**, select the **Play a welcome message** check box, and then do one of the following:
    - To enter the welcome message as text that is converted to speech for callers, click **Use text-to-speech**, and then type the welcome message in the text box.

      Note:
      Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

    - To use a Wave or Windows Media Audio file recording for the welcome message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the audio file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

      Note:
      All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

18. Under **Step 4 Specify Your Business Hours**, in the **Your time zone** box, click the time zone of the workflow.

    Note:
    The time zone is the time zone where the callers and agents of the workflow reside. It is used to calculate the open and close hours. For example, if the workflow is configured to use the North American Eastern Time zone and the workflow is scheduled to open at 7:00 A.M. and close at 11:00 P.M., the open and close times are assumed to be 7:00 Eastern Time and 11:00 Eastern Time respectively. (You must enter the times in 24-hour time notation.)

19. Select the type of business hours schedule you want to use by doing one of the following:
    - To use a predefined schedule of business hours, click **Use a preset schedule**, and then select the schedule you want to use from the drop-down list.

      Note:
      You must have defined at least one preset schedule previously to be able to select this option. You define preset schedules by using the **New-CSRgsHoursOfBusiness** cmdlet. For details, see (Optional) Define Response Group Business Hours. When you select a preset schedule, **Day**, **Open**, and **Close** are automatically filled with the days and hours that the response group is available.

    - To use a custom schedule that applies only to this workflow, click **Use a custom schedule**.
20. If you are creating a custom schedule for this workflow, click the check boxes for the days of the week that the response group is available.
21. If you are creating a custom schedule, type the **Open** and **Close** hours when the response group available.

    Note:
    The **Open** and **Close** hours must be in 24-hour time notation. For example, if your office works a 9-to-5 work day and closes at noon for lunch, the business hours are specified as **Open** 9:00, **Close** 12:00, **Open** 13:00, and

Close 17:00.

22.If you want to play a message when the office is not open, select the **Play a message when the response group is outside of business hours** check box, and then specify the message to play by doing one of the following:

- To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

  Note:
  Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

  Note:
  All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

23.Specify how to handle calls after the message is played (if a message is configured):

- To disconnect the call, click **Disconnect Call**.
- To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is <*username*>@<*domainname*> (for example, bob@contoso.com).
- To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is <*username*>@<*domainname*>.
- To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is <*number*>@<*domainname*> (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.

24.Under **Step 5 Specify Your Holidays**, click the check boxes for one or more sets of holidays that define the days when the response group is closed for business.

Note:
You need to define holidays and holiday sets before you configure the workflow. Use the **New-CsRgsHoliday** and **New-CsRgsHolidaySet** cmdlets to define holidays and holiday sets. For details, see (Optional) Define Response Group Holiday Sets.

25.If you want to play a message on holidays, select the **Play a message during holidays** check box, and then specify the message to play by doing one of the following:

- To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

  Note:
  Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

  Note:
  All user-provided audio files must meet certain requirements. For details about supported audio file formats, see Technical

> Requirements for Response Groups.

26. Specify how to handle calls after the message is played (if a message is configured):
    - To disconnect the call, click **Disconnect Call**.
    - To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is *<username>*@*<domainname>* (for example, bob@contoso.com).
    - To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is *<username>*@*<domainname>*.
    - To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is *<number>*@*<domainname>* (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.
27. Under **Step 6 Configure Music on Hold**, choose what you want callers to listen to while waiting for an agent by doing one of the following:
    - To use the default music on-hold recording, click **Use default**.
    - To use an audio file recording for the on-hold music, click **Select a music file**. If you want to upload a new audio file, click the **a music file** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

> **Note:**
>
> All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

28. Under **Step 7 Configure Interactive Voice Response**, under the **The user will hear the following text or recorded message** heading, specify the question to ask callers as follows:
    - To enter the question in text format, click **Use text-to-speech**, and type the question in the text box.

> **Note:**
>
> Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

> **Note:**
>
> The "#" symbol is translated by the text-to-speech engine as the word "number". If you need to refer to the # key, you should use the key name, rather than the symbol, in your prompt. For example, "To talk to sales, press the pound key."

- To use a prerecorded audio file that contains the question, click **Select a recording**, and then click the **a recording** link to upload the file. In the new browser window, click **Browse**, select the audio file, and then click **Open**. Click **Upload** to load the file, and then optionally you can type the question in the text box (this enables the question, and the caller's response, to be forwarded to the responding agent).

> **Note:**
>
> All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

29. Under **Response 1**, specify the first possible answer to the question by doing the following:

> **Important:**
>
> Do not use quotation marks (") in any voice responses. Quotation marks cause the IVR to fail.

Note:
You can choose to allow callers to answer using speech, alphanumeric keypad input, or both.

- If you want to allow the caller to respond using speech, enter the answer in **Enter a voice response**.
- If you want to allow the caller to respond by pressing a key on the keypad, in **Digit**, click the keypad digit.

30. Specify whether to route the caller to a queue, or to ask another question as follows:
    - To route the caller to a queue, click **Send to a queue**, and in **Select a queue**, click the queue that you want to use.
    - To ask another question, click **Ask another question**, and then click **Use text-to-speech** and type the question, or click **Select a recording**. Use the response groupings in this section to specify up to four possible responses to the additional question and the queue to use for each response. To specify a third or fourth possible response, click the **Response 3** check box or the **Response 4** check box.
31. Specify up to three more possible answers to the original question by repeating steps 28 and 29 to specify the possible responses and the action to take for each response. To specify a third or fourth possible answer, click the **Response 3** check box or the **Response 4** check box.
32. Click **Deploy**.

To use Windows PowerShell to create or modify an Interactive workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Retrieve the service name for the Response Group service and assign it to a variable. At the command line, run:

```
$serviceId="service:"+(Get-CSService | ?{$_.Applications -like "*RGS*"
```

4. An interactive workflow requires two or more queues and two or more agent groups. First, create the agent groups. Run:

```
$AGSupport = New-CsRgsAgentGroup -Parent $serviceId -Name "Technical S
$AGSales = New-CsRgsAgentGroup -Parent $serviceId -Name "Sales Team" [
```

5. Create the queues. Run:

```
$QSupport = New-CsRgsQueue -Parent $ServiceId -Name "Contoso Support"
$QSales = New-CsRgsQueue -Parent $ServiceId -Name "Contoso Sales" -Age
```

6. Create the first response group prompt. Run:

```
$SupportPrompt = New-CsRgsPrompt -TextToSpeechPrompt "Please be patien
```

7. Then create the action to be performed after the prompt. Run:

```
$SupportAction = New-CsRgsCallAction -Prompt $SupportPrompt -Action Tr
```

8. Create the first response group answer. Run:

```
$SupportAnswer = New-CsRgsAnswer -Action $SupportAction [-DtmfResponse
```

9. Now create the second prompt, call action, and answer. First create the prompt. Run:

```
$SalesPrompt = New-CsRgsPrompt -TextToSpeechPrompt "Please hold while
```

10. Create the second call action. Run:

```
$SalesAction = New-CsRgsCallAction -Prompt $SalesPrompt -Action Transf
```

11. Create the second response group answer. Run:

```
$SalesAnswer = New-CsRgsAnswer -Action $SalesAction [-DtmfResponse 2]
```

12. Create the top-level prompt. Run:

```
$TopLevelPrompt = New-CsRgsPrompt -TextToSpeechPrompt "Thank you for c
```

13. Create the top-level question. Run:

```
$TopLevelQuestion = New-CsRgsQuestion -Prompt $TopLevelPrompt [-Answer
```

14. Now create the workflow. Run:

```
$IVRAction = New-CsRgsCallAction -Action TransferToQuestion [-Question
$IVRWorkflow = New-CsRgsWorkflow -Parent $ServiceId -Name "Contoso Hel
```

Note:
All users who have been designated as manager of a response group must be assigned th CsResponseGroupManager role. If users are not assigned this role, they cannot manage response groups.

1.4.3.13.3.9 Managing Application-Level Response Group Settings

Managing Application-Level Response Group Settings

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-11-01*

Application-level settings for Response Group application include the default music-on-hold configuration, the default music-on-hold audio file, the agent ringback grace period, and the call context configuration. You can define only one set of application-level settings per pool. To view application-level settings, use the **Get-CsRgsConfiguration** cmdlet. To modify the application-level settings, use the **Set-CsRgsConfiguration** cmdlet.

The default music on hold is played when a call is placed on hold only if no custom music on hold is defined. Call context is available only for queues assigned to interactive workflows. If call context is enabled, an agent can see information such as caller wait time or workflow questions and answers when the call is received.

⊟To modify Response Group application-level settings

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. At the command line, run:

```
Set-CsRgsConfiguration -Identity <name of service hosting Response Gro
```

For example:

```
Set-CsRgsConfiguration -Identity "service:ApplicationServer:redmond.co
```

To specify an audio file to use as the default music on hold, you need to import the audio file first. For example:

```
$x = Import-CsRgsAudioFile -Identity "service:ApplicationServer:redmon
Set-CsRgsConfiguration -Identity "service:ApplicationServer:redmond.co
```

Other Resources

Get-CsRgsConfiguration
Set-CsRgsConfiguration

Import-CsRgsAudioFile

1.4.3.13.3.10 (Optional) Verify Response Group Deployment

(Optional) Verify Response Group Deployment

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-09-11*

After you configure Response Group, you need to verify the configuration to make sure your response groups work as expected. At minimum, verify the following scenarios by using the following types of users:

Users

- A user who is homed on Lync Server 2013
- An external user who uses the public switched telephone network (PSTN)
- An agent who is homed on Lync Server 2013

Scenarios

- The Lync Server 2013 user calls the response group.
- The external user calls the response group.
- A user calls the response group while the agent is on another call and goes to the queue.

1.4.3.13.4 Configuring Announcements for Unassigned Numbers

Configuring Announcements for Unassigned Numbers

See Also

Deployment > Deploying Enterprise Voice > Deploying Call Management Features >

Topic Last Modified: *2012-09-11*

The Announcement application is an Enterprise Voice feature that enables you to configure what happens to calls to unassigned extensions (extensions that are valid for your organization, but are not assigned to a person or a phone). For example, you can configure calls to unassigned numbers to play a message, or to be transferred to a different destination, or both.

The Announcement application is installed as a feature of Response Group application on the Front End Server or Standard Edition server when you deploy Enterprise Voice. You need to configure Announcements by uploading your audio files or by configuring text-to-speech (TTS) and configuring the unassigned number table.

This section guides you through the configuration of Lync Server Announcements. It assumes that you have already read the planning sections related to Announcements and deployed an Enterprise Edition server or a Standard Edition server with Enterprise Voice.

- Announcement Configuration Prerequisites and Roles
- Deployment Process for Announcements
- Create an Announcement
- Configure the Unassigned Number Table
- (Optional) Verify Announcement Deployment

⊟See Also

Other Resources

Planning for Call Management Features

1.4.3.13.4.1 Announcement Configuration Prerequisites and Roles

Announcement Configuration Prerequisites and Roles

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Announcements for Unassigned Numbers >

Topic Last Modified: *2013-02-25*

Announcement is an Enterprise Voice call management feature. This topic describes what you need to have in place before you can configure Announcement and the role assignments that you need to perform configuration tasks.

This section assumes that you have read the planning documentation related to Announcement (see Planning for Call Management Features).

Announcement Configuration Prerequisites

The Announcement application requires the following components:

- Application service
- Response Group application
- File Store, to hold audio files

All of these components are installed by default when you deploy Enterprise Voice.

Announcement Configuration Roles

You can use the following administrative tools to configure announcements:

- Lync Server Control Panel
- Lync Server Management Shell

Configuring Announcement application requires one of the following administrative roles:

- **CsVoiceAdministrator** This administrator role can create, configure, and manage all voice-related settings and policies, including Announcement settings.
- **CsServerAdministrator** This administrator role can manage, monitor, and troubleshoot servers and services, and configure all Announcement settings.
- **CsAdministrator** This administrator role can perform all administrative tasks and modify all settings.
- **CsViewOnlyAdministrator** This administrator role can view the deployment to monitor deployment health.

Note:

For details about administrative user rights, see Planning for Role-Based Access Control in the Planning documentation.

See Also

Concepts

Deploying Enterprise Voice

Other Resources

Planning for Call Management Features

1.4.3.13.4.2 Deployment Process for Announcements

Deployment Process for Announcements

Planning for Enterprise Voice > Planning for Call Management Features > Planning for Announcements >

Topic Last Modified: *2012-09-12*

This section provides an overview of the steps involved in deploying the Announcement application. You must deploy Enterprise Voice before you configure announcements. The components required by the Announcement application are installed and enabled when you deploy Enterprise Voice.

Announcement Deployment Process

Phase	Steps	Roles	Deployment documentation
Configure Announcement settings	• Create the announcement by recording and uploading audio files or by using text-to-speech (TTS). • Configure the unassigned number ranges in the unassigned number table and associate them with the appropriate announcement.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator CsViewOnlyAdministrator	Create an Announcement Configure the Unassigned Number Table
Verify your Announcement deployment	Test by listening to announcements to verify that your configuration works as expected.	-	(Optional) Verify Announcement Deployment

1.4.3.13.4.3 Create an Announcement

Create an Announcement

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Announcements for Unassigned Numbers >

Topic Last Modified: *2012-11-01*

To create a new announcement, you need to perform the following steps:

1. For audio prompts, record the audio file by using your favorite audio recording application.
2. For audio prompts, run the **Import-CsAnnouncementFile** cmdlet to import the contents of the audio file to File Store.
3. Run the **New-CsAnnouncement** cmdlet to create and name the announcement. Perform this step to create announcements with an audio

prompt, a text-to-speech (TTS) prompt, or no prompt.

Tip:

You might want to create an announcement with no prompt (for example, if you want to transfer calls to a specific destination without playing a message).

4. Assign the new announcement to a number range in the unassigned number table.

This topic describes how to import and create announcements. For details about assigning announcements in the unassigned number table, see Configure the Unassigned Number Table.

⊟To create a new announcement

1. For audio prompts, create the audio file.
2. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
3. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
4. For audio prompts, run:

```
Import-CsAnnouncementFile -Parent <service of the Application Server r
```

5. Run:

```
New-CsAnnouncement -Parent <service of Application Server running the
```

For transferring calls to voice mail, type SIPAddress in the format sip:username@domainname;opaque=app:voicemail (for example, sip:bob@contoso.com;opaque=app:voicemail). For transferring calls to a phone number, type SIPAddress in the format sip:number@domainname;user=phone (for example, sip:+14255550121@contoso.com;user=phone).

For example, to specify an audio prompt:

```
$a = Get-Content ".\PromptFile.wav" -ReadCount 0 -Encoding Byte
Import-CsAnnouncementFile -Parent service:ApplicationServer:pool0@cont
New-CsAnnouncement -Parent service:ApplicationServer:pool0.contoso.com
```

For example, to specify a TTS prompt:

```
New-CsAnnouncement -Parent service:ApplicationServer:pool0.contoso.com
```

For more detail about these cmdlets, and to see a list of the language codes to use in the **TextToSpeechPrompt** parameter, see New-CsAnnouncement.

Other Resources

Import-CsAnnouncementFile
New-CsAnnouncement
Configure the Unassigned Number Table

1.4.3.13.4.4 Configure the Unassigned Number Table

Configure the Unassigned Number Table

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Announcements for Unassigned Numbers >

Topic Last Modified: *2012-10-30*

In Lync Server 2013, you can specify what happens to incoming calls to phone numbers that are valid for your organization, but are not assigned to a user or phone. Callers can hear a message, or can be routed to another destination, or both.

How you configure the unassigned number table depends on how you want to use it. You can configure the table with all the valid extensions for your organization, with only unassigned extensions, or with a combination of both types of numbers. The unassigned number table can include both assigned and unassigned numbers, but it is invoked only when a caller dials a number that is not currently assigned. If you include all the valid extensions in the unassigned number table, you can specify the action that occurs whenever someone leaves your organization, without needing to reconfigure the table. If you include unassigned extensions in the table, you can modify the action that occurs for specific numbers. For example, if you change the extension for your customer service desk, you can include the old customer service number in the table and then assign it to an announcement that provides the new number.

Important:
Before you configure the unassigned number table, your system must already either have Announcements defined or an Exchange Unified Messaging (UM) Auto Attendant set up.

Tip:
When someone calls an unassigned number, Lync Server searches the unassigned number table from top to bottom and uses the first matching range. Therefore, an action that you want to be performed as a last resort should be specified for the last range in the table.

Create or Modify an Unassigned Number Range Create an Announcement

Create or Modify an Unassigned Number Range

See Also

Deploying Call Management Features > Configuring Announcements for Unassigned Numbers > Configure the Unassigned Number Table >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to configure unassigned number ranges for the Announcement application.

Important:
Before you configure the unassigned number table, you must have already defined one or more announcements or set up an Exchange Unified Messaging (UM) Auto Attendant.

To use Lync Server Control Panel to configure unassigned phone numbers

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Features**, and then click **Unassigned Number**.
4. On the **Unassigned Number** page, do one of the following:
   - To create a new number range, click **New**. In **Name**, type an identifying name for this range of numbers.

     Note:
     After you commit the new unassigned number range to the database, you cannot change this name.

- To modify an existing number range, type all or part of the name of the number range in the search field. In the resulting list of number ranges, click the name you want, click **Edit**, and then click **Show details**.

5. In the first **Number range** field, type the beginning number of the range, and in the second **Number range** field, type the ending number of the range.

Note:

- The beginning number of the range must be less than or equal to the ending number of the range.
- If the beginning number of the range or the ending number of the range includes an extension number, both the beginning number and the ending number of the range must include an extension, and the extension number must be the same for both the beginning number and the ending number.
- The number must match the regular expression (tel:)?(\+)?[1-9]\d{0,17}(;ext=[1-9]\d{0,9})?. This means the number may begin with the string tel: (if you don't specify that string, it will be automatically added for you), a plus sign (+), and a digit 1 through 9. The phone number can be up to 17 digits and may be followed by an extension in the format ;ext= followed by the extension number.

1. In **Announcement service**, do one of the following:
   - Click **Announcement**.
   - Click **Exchange UM**.
2. If, in the previous step, you clicked **Announcement**, do the following:
   - Under **FQDN of destination server**, click **Select**, click the service ID of the Application service that runs the Announcement application that will handle incoming calls to this range of unassigned numbers, and then click **OK**.
   - In **Announcement**, click the announcement to be played for this range of unassigned numbers.
3. If, in the previous step, you clicked **Exchange UM**, under **Auto Attendant phone number**, click **Select**, click the phone number to be used for this range of unassigned numbers, and then click **OK**.
4. Click **OK**.
5. On the **Unassigned Number** page, be sure that the unassigned number ranges are arranged in the order that you want. To change a range's position in the table, click one or more consecutive names in the list of ranges, and then click the up arrow or the down arrow.

Tip:

Lync Server searches the unassigned number table from top to bottom and uses the first range that matches the unassigned number. If you have overlapping ranges and one range specifies a last resort action, make sure that range is at the bottom of the list.

6. When you have the unassigned number ranges in the order that you want, click **Commit all**.

To use Windows PowerShell to configure unassigned phone numbers

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Use **New-CsUnassignedNumber** to create a new unassigned number range. Use **Set-CsUnassignedNumber** to modify an existing unassigned number range.

Tip:

If you have overlapping ranges and want the ranges to be applied in a specific order, include the Priority parameter. The range with the highest priority will be applied to the call.

At the command line, do one of the following:

- To create a number range for an Announcement service, run:

```
New-CsUnassignedNumber -Identity <unique identifier for unas
```

- Or, to create a number range for Exchange UM Auto Attendant, run:

```
New-CsUnassignedNumber -ExUmAutoAttendantPhoneNumber <phone
```

For example:

```
New-CsUnassignedNumber -Identity "Unassigned range 1" -NumberRangeStar
```

Or

```
New-CsUnassignedNumber -ExUmAutoAttendantPhoneNumber "+12065551234" -I
```

The following example shows how to modify the numbers in an existing unassigned number range:

```
Set-CsUnassignedNumber -Identity "Unassigned range 1" -NumberRangeStar
```

Tasks

Delete an Unassigned Number Range

Other Resources

New-CsUnassignedNumber
Set-CsUnassignedNumber
Get-CsUnassignedNumber

1.4.3.13.4.5 (Optional) Verify Announcement Deployment

(Optional) Verify Announcement Deployment

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Announcements for Unassigned Numbers >

Topic Last Modified: *2013-02-25*

After you install and configure Announcement, you need to verify the configuration to make sure that calls to unassigned numbers work as expected. At minimum, verify the following:

- Call a number that is valid for your organization but is an unassigned number.
- Call the unassigned number and verify that the correct announcement plays.

1.4.3.14 Enable Users for Enterprise Voice

Enable Users for Enterprise Voice

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-11-01*

After you install files for one or more Mediation Servers, configure outbound call routing, and optionally deploy one or more advanced Enterprise Voice features, you can use the following procedures to enable a user to make calls by using Enterprise Voice:

Note:

Of the following procedures, only the first can be performed by using Lync Server Control Panel. For the remaining procedures, you can use only Lync Server Management Shell.

- Enable the user account for Enterprise Voice.
- (Optional) Assign the user account a user-specific voice policy.
- (Optional) Assign the user account a user-specific dial plan.

To enable a user account for Enterprise Voice

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to enable, and then click **Find**.
5. In the table, click the user account that you want to enable for Enterprise Voice.
6. On the **Edit** menu, click **Show details**.
7. On the **Edit Lync Server User** page, under **Telephony**, click **Enterprise Voice**.
8. Click **Line URI**, and then type a unique, normalized phone number (for example, tel:+14255550200).
9. Click **Commit**.

To finish enabling a user for Enterprise Voice, be sure that the user is assigned a voice policy and a dial plan, whether global (assigned by default) or user-specific.

By default, all users are assigned a global voice policy and dial plan. If a voice policy or dial plan exists at the site level for the site on which the user account is homed, those site policies will automatically apply to the user. To apply a per-user voice policy or dial plan to a user, you must run the **Grant-CsVoicePolicy** and **Grant-CsDialPlan** cmdlets. For details, see the Lync Server Management Shell documentation.

Voice Policy Assignment

Global and site-level voice policies are automatically assigned to all user accounts that are enabled for Enterprise Voice. You can also create voice policies that apply to specific users or groups. These per-user policies must be explicitly assigned to the users or groups. If you want to use the global or site voice policy for all users who are enabled for Enterprise Voice, you can skip this section and continue to Dial Plan Assignment section later in this topic.

To assign a user-specific voice policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. To assign an existing user voice policy to a user, run the following at the command prompt:

```
Grant-CsVoicePolicy -Identity <UserIdParameter> -PolicyName <String>
```

For example:

```
Grant-CsVoicePolicy -Identity "Bob Kelly" -PolicyName VoicePolicyJapan
```

In this example, the user with the display name Bob Kelly is assigned the voice policy with the name **VoicePolicyJapan**.

For details about assigning a user-specific voice policy or about running the **Grant-CsVoicePolicy** cmdlet, see the Lync Server Management Shell documentation.

Dial Plan Assignment

To complete user account configuration for either users of Enterprise Voice or users of dial-in conferencing, the user must be assigned a dial plan. User accounts will automatically use the global dial plan or, if one exists, the site-level dial plan, when you do not explicitly assign an existing per-user dial plan. If you want to use the global or site dial plan for all users who are enabled for Enterprise Voice, you can skip this section.

To assign a dial plan

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. To assign a user-specific dial plan, run the following at the command prompt:

   ```
   Grant-CsDialPlan -Identity <UserIdParameter> -PolicyName <String>
   ```

   For example:

   ```
   Grant-CsDialPlan -Identity "Bob Kelly" -PolicyName DialPlanJapan
   ```

   In this example, the user with the display name Bob Kelly is assigned the user dial plan with the name **DialPlanJapan**.

For details about assigning a user dial plan or about running the **Grant-CsDialPlan** cmdlet, see the Lync Server Management Shell documentation.

See Also

Tasks

Disable a User for Enterprise Voice

1.4.4 Deploying Conferencing

Deploying Conferencing

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-09-27*

This section describes how to set up dial in conferencing and Office Web Apps Server.

- Configuring Dial-in Conferencing
- Configuring Integration with Office Web Apps Server and Lync Server 2013
- Configuring the Meeting Join Page

1.4.4.1 Configuring Dial-in Conferencing

Configuring Dial-in Conferencing

Microsoft Lync Server 2013 > Deployment > Deploying Conferencing >

Topic Last Modified: *2012-06-19*

This section guides you through the configuration of Lync Server 2013 dial-in conferencing.

- Dial-in Conferencing Configuration Prerequisites and Permissions
- Deployment Checklist for Dial-In Conferencing
- Configure Dial Plans for Dial-in Conferencing
- Make Sure Dial Plans Have Assigned Regions
- (Optional) Verify PIN Policy Settings
- Configure Conferencing Policy for Dial-in
- Configure Dial-in Conferencing Access Numbers
- (Optional) Verify Dial-in Conferencing Settings
- (Optional) Modify Key Mapping for DTMF Commands
- (Optional) Enable and Disable Conference Join and Leave Announcements
- (Optional) Verify Dial-in Conferencing
- Deploy the Online Meeting Add-in for Lync 2013
- Configure User Account Settings
- (Optional) Welcome Users to Dial-in Conferencing

⊟Related Sections

Deploying Lync Server 2013

1.4.4.1.1 Dial-in Conferencing Configuration Prerequisites and Permissions

Dial-in Conferencing Configuration Prerequisites and Permissions

See Also

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2012-06-20*

Dial-in conferencing is an optional component of the Lync Server 2013 Conferencing workload. The components you need to install before you can configure dial-in conferencing are deployed when you use the Topology Builder to design your topology and then set up your Front End pool or Standard Edition server. This topic describes what you need to have accomplished before you can configure dial-in conferencing.

This section assumes that you have read the planning sections related to the Conferencing workload and dial-in conferencing in particular.

Dial-in Conferencing Configuration Prerequisites

Dial-in conferencing requires the following Lync Server 2013 components:

- Unified Communications Application Service (UCAS) (called the *Application service*)
- Conferencing Attendant application
- Conferencing Announcement application
- Dial-in Conferencing Settings webpage
- At least one Lync Server 2013 Mediation Server and at least one PSTN gateway

You deploy these components when you use the Topology Builder to define and publish your topology and then deploy a Front End pool or a Standard Edition server. If you are deploying Enterprise Voice, you should deploy it before you configure dial-in conferencing. If you are not deploying Enterprise Voice, you can deploy a Mediation Server and a public switched telephone network (PSTN) gateway when you deploy your Front End pool or Standard Edition server.

Note:

If you are upgrading from Office Communications Server 2007 R2 to Lync Server 2013, deploy dial-in conferencing in every pool that you plan to use to host Lync Server 2013 conferences. For details about migrating dial-in conferencing, see Migration from Office Communications Server 2007 R2 to Lync Server 2013.

This section assumes that you have done the following:

- Applied the latest updates to your Office Communications Server 2007 R2 environment, if you are migrating to Lync Server 2013.
- Used Topology Builder to design and configure your topology. While specifying the Conferencing workload, you selected the dial-in conferencing option. For details about defining your topology, see Defining and Configuring the Topology in the Deployment documentation.
- Published your topology, and set up the Front End pool or Standard Edition server. For details about publishing the topology and installing Lync Server 2013, see Deploying Lync Server 2013 in the Deployment documentation.

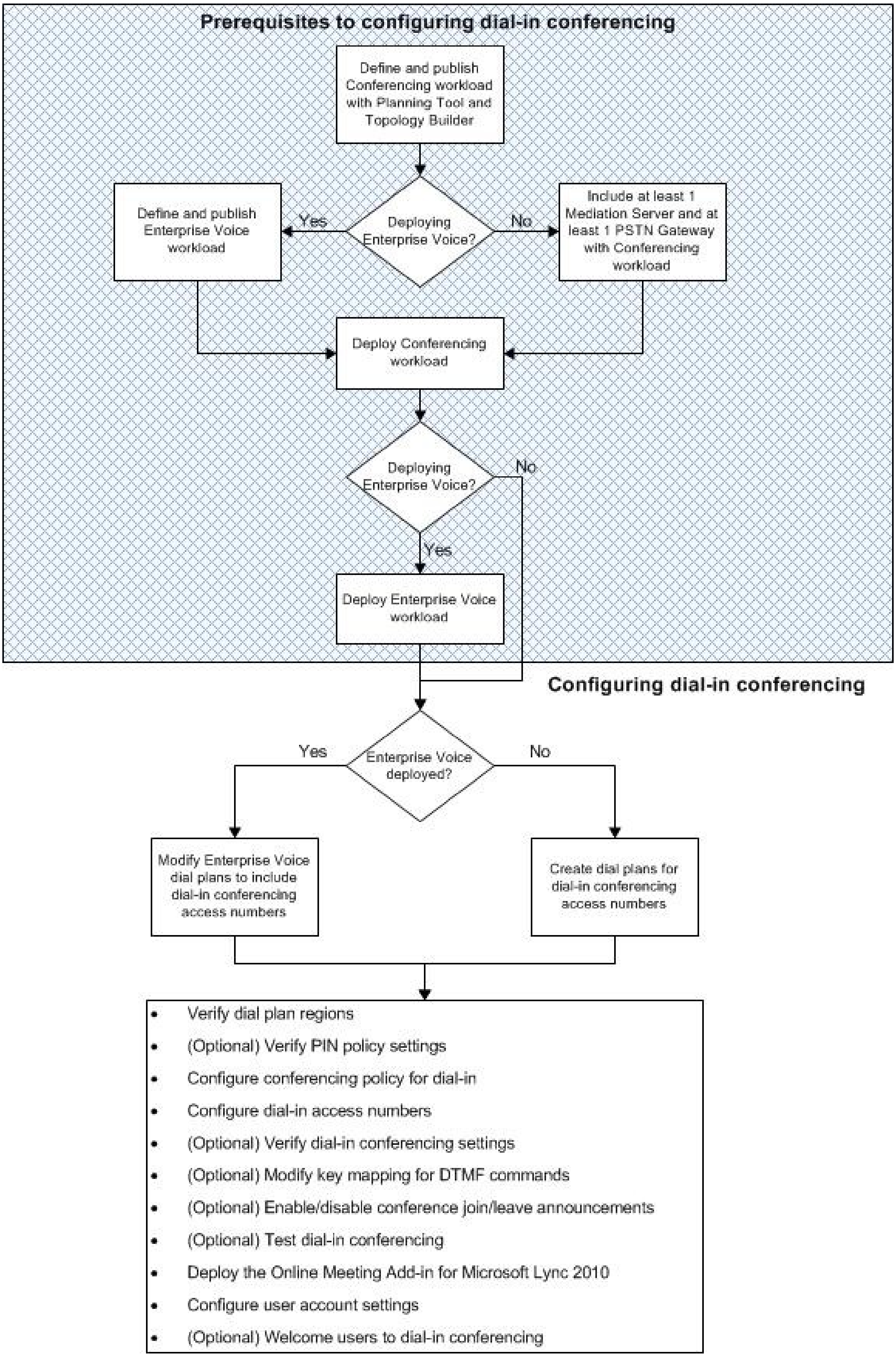
  Note:

  When you install your published topology, the Dial-in Conferencing Settings webpage is installed on the Front End Server or Standard Edition server as part of Web Services.

  Important:

  If you change the path for the File Store in Topology Builder after you deploy Lync Server 2013, you need to restart the Conferencing Attendant and Conferencing Announcement applications to use the new path.
- Deployed Enterprise Voice. If you are not deploying Enterprise Voice, you either collocated a Mediation Server on the Enterprise Edition Front End Server or the Standard Edition server, or you deployed a stand-alone Mediation Server, and you deployed a PSTN gateway. For details about deploying Enterprise Voice, see Deploying Enterprise Voice in the Deployment documentation. For details about installing a stand-alone Mediation Server and PSTN gateway, see Deploying Mediation Servers and Defining Peers in the Deployment documentation.

The following flowchart shows the steps that you must perform before you can configure dial-in conferencing and the steps that you perform to configure dial-in conferencing.


Prerequisites to configuring dial-in conferencing
Define and publish Conferencing workload with Planning Tool and Topology Builder
Deploying Enterprise Voice?
Yes
No
Define and publish Enterprise Voice workload
Include at least 1 Mediation Server and at least 1 PSTN Gateway with Conferencing workload
Deploy Conferencing workload
Deploying Enterprise Voice?
No
Yes
Deploy Enterprise Voice workload
Configuring dial-in conferencing
Enterprise Voice deployed?
Yes
No
Modify Enterprise Voice dial plans to include dial-in conferencing access numbers
Create dial plans for dial-in conferencing access numbers
• Verify dial plan regions
• (Optional) Verify PIN policy settings
• Configure conferencing policy for dial-in
• Configure dial-in access numbers
• (Optional) Verify dial-in conferencing settings
• (Optional) Modify key mapping for DTMF commands
• (Optional) Enable/disable conference join/leave announcements
• (Optional) Test dial-in conferencing
• Deploy the Online Meeting Add-in for Microsoft Lync 2010
• Configure user account settings
• (Optional) Welcome users to dial-in conferencing

Dial-in Conferencing Permissions

To configure dial-in conferencing, you need to use the following administrative tools:

- Lync Server 2013 Control Panel
- Lync Server Management Shell

You use these administrative tools to configure dial-in conferencing settings, and the dial plans, policies, and other settings that dial-in conferencing requires.

Configuring dial-in conferencing requires any of the following administrative roles, depending on the task:

- **CsVoiceAdministrator** This administrator role can create, configure, and manage voice-related settings and policies.
- **CsUserAdministrator** This administrator role can enable and disable users for Lync Server and assign existing policies, such as conferencing policies and PIN policies, to users.
- **CsAdministrator** This administrator role can perform all of the tasks of CsVoiceAdministrator and CsUserAdministrator.

See Also

Concepts

Deploying Enterprise Voice

1.4.4.1.2 Deployment Checklist for Dial-In Conferencing

Deployment Checklist for Dial-In Conferencing

Planning > Planning for Conferencing > Deployment Checklist for Conferencing >

Topic Last Modified: *2013-02-25*

The components required for dial-in conferencing are deployed when you deploy the conferencing workload. Before you can configure dial-in conferencing, you need to deploy either Enterprise Voice or a Mediation Server and a public switched telephone network (PSTN) gateway.

All the steps in the following table must be performed before users can dial in from the PSTN to join an audio/video conference.

Note:

If you are migrating from Office Communications Server 2007 R2, you must apply the latest updates to your Office Communications Server 2007 R2 environment before deploying dial-in conferencing.

Dial-in Conferencing Deployment Process

Phase	Steps	Permissions	Deployment documentation
Create a topology that includes the Conferencing workload, including a Mediation Server and PSTN gateway, and	1. Run Topology Builder to configure your topology. While configuring the topology, select the dial-in conferencing option. 2. Publish the	Domain Admins RTCUniversalServerAdmins Administrator	• Deploying Lync Server 2013 • To create a stand-alone Mediation Server pool: Deploying Mediation Servers and Defining Peers

deploy the Front End pool or Standard Edition server	topology and deploy the Front End pool or Standard Edition server. 3. If necessary, create a stand-alone Mediation Server and associate it with a PSTN gateway. **Note:** This step is required only if you do not deploy Enterprise Voice and do not collocate the Mediation Server with the Enterprise Edition Front End Server or Standard Edition server. If you deploy Enterprise Voice, you install and configure Mediation Servers and PSTN gateways as part of the Enterprise Voice deployment. If you collocate the Mediation Server, you install and configure the Mediation Server as part of the Front End pool or Standard Edition server deployment.		
Configure dial plans	A dial plan is a set of phone number normalization rules that translate phone numbers dialed from a specific location to a single standard (E.164) format for purposes of phone authorization and call routing. The same phone number dialed from different	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrato	Configure Dial Plans for Dial-in Conferencing

	locations can, based on the respective dial plans, resolve to different E.164 numbers, as appropriate to each location. If you deploy Enterprise Voice, you set up dial plans as part of that deployment, and you need to make sure that the dial plans also accommodate dial-in conferencing. If you do not deploy Enterprise Voice, you need to set up dial plans for dial-in conferencing. Use the Lync Server 2013 Control Panel or Lync Server Management Shell to set up dial plans as follows: 1. Create one or more dial plans for routing dial-in access phone numbers. 2. Assign a default dial plan to each pool. Set the **Dial-in conferencing region** to the geographic location to which the dial plan applies. The region associates the dial plan with dial-in access numbers.	r	
Make sure that dial plans are assigned regions	Run the **Get-CsDialPlan** and **Set-CsDialPlan** cmdlets to make sure that all dial plans have a region assigned.	RTCUniversalServerAdmins CsVoiceAdministrator CsServerAdministrator CsAdministrator	Make Sure Dial Plans Have Assigned Regions
(Optional) Verify or modify user personal identification number (PIN) requirements	Use Lync Server 2013 Control Panel or Lync Server Management Shell to view or modify the Conferencing **PIN Policy**. You can specify minimum PIN length, maximum number of logon attempts, PIN expiration, and	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	(Optional) Verify PIN Policy Settings

	whether common patterns are allowable.		
Configure conferencing policy to support dial-in conferencing	Use Lync Server 2013 Control Panel or Lync Server Management Shell to configure **Conferencing Policy** settings. Specify whether: • PSTN conference dial-in is enabled. • Users can invite anonymous participants. • Unauthenticated users can join a conference by using dial-out phoning. With dial-out phoning, the conference server calls the user, and the user answers the phone to join the conference.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	Configure Conferencing Policy for Dial-in
Configure dial-in access numbers	Use Lync Server 2013 Control Panel or Lync Server Management Shell to set up dial-in access numbers that users call to dial in to a conference, and specify the regions that associate the access number with the appropriate dial plans. The first three access numbers for the region specified by the organizer's dial plan are included in the conference invitation. All access numbers are available on the Dial-in Conferencing Settings page. **Note:** After you create dial-in access numbers, you can use the **Set-CsDialInConferencingAccessNumber** cmdlet to modify the display name of the Active Directory contact objects so that users can more easily identify the correct access number.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	Configure Dial-in Conferencing Access Numbers
(Optional) Verify dial-in conferencing settings	Use the **Get-CsDialinConferencingAccessNumber** cmdlet to search for dial plans that have a dial-in conferencing region that is	RTCUniversalServerAdmins CsServerAdministrator	(Optional) Verify Dial-in Conferencing Settings

	not used by any access number and for access numbers that have no region assigned.	CsAdministrator CsViewOnlyAdministrator CsHelpDesk	
(Optional) Modify key mapping of DTMF commands	Use the **Set-CsDialinConferencingDtmfConfiguration** cmdlet to modify the keys used for dual-tone multifrequency (DTMF) commands, which participants can use to control conference settings (such as mute and unmute or lock and unlock).	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	(Optional) Modify Key Mapping for DTMF Commands
(Optional) Modify conference join and leave announcement behavior	Use the **Set-CsDialinConferencingConfiguration** to change how announcements work when participants join and leave conferences.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	(Optional) Enable and Disable Conference Join and Leave Announcements
(Optional) Verify dial-in conferencing	Use the **Test-CsDialInConferencing** cmdlet to test that the access numbers for the specified pool work correctly.	RTCUniversalServerAdmins CsServerAdministrator CsAdministrator	(Optional) Verify Dial-in Conferencing
Deploy the Online Meeting Add-in for Lync 2013	Deploy the Online Meeting Add-in for Lync 2013 so that users can schedule conferences that support dial-in conferencing. The Online Meeting Add-in for Lync 2013 is installed automatically when you install Lync 2013.	Administrators	Deploy the Online Meeting Add-in for Lync 2013
Configure user account settings	Use Lync Server 2013 Control Panel or Lync Server Management Shell to configure the telephony **Line URI** as a unique, normalized phone number (for example, tel:+14255550200).	RTCUniversalServerAdmins CsAdministrator CsUserAdministrator	Configure User Account Settings
(Optional) Welcome users to dial-	Use the **Set-CsPinSendCAWelcomeMail** script to set users' initial PINs	RTCUniversalServerAdmins	(Optional) Welcome Users to Dial-in Conferencing

in conferencing and set the initial PIN	and send a welcome email that contains the initial PIN and a link to the Dial-in Conferencing Settings page.		

1.4.4.1.3 Configure Dial Plans for Dial-in Conferencing

Configure Dial Plans for Dial-in Conferencing

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2013-02-25*

When you deploy dial-in conferencing, you need to create or modify one or more dial plans for routing dial-in access phone numbers. Make sure that at least one normalization rule in each dial plan converts telephone extensions into complete phone numbers in E.164 format. Users of dial-in conferencing join conferences as authenticated enterprise users by entering their personal identification number (PIN) and their phone number. You need a normalization rule to convert extensions into complete phone numbers so that users can be authenticated when they enter just a telephone extension.

To set up dial plans for dial-in conferencing, do the following:

- Whether or not you deploy Enterprise Voice, modify the global dial plan to add a dial-in conferencing region and to make sure that a normalization rule accurately converts your dial-in access numbers. For detailed instructions, see Modify a Dial Plan.
- If you did not deploy Enterprise Voice, create dial plans for your dial-in conferencing access numbers. Be sure to include a dial-in conferencing region. For detailed instructions, see Create a Dial Plan.
- If you deployed Enterprise Voice, modify Enterprise Voice dial plans as necessary to include regions and use appropriate normalization rules for dial-in access numbers. For detailed instructions, see Modify a Dial Plan. You can also create dedicated dial plans that are used only for dial-in access numbers. For detailed instructions, see Create a Dial Plan.

For details about planning regions, see Dial-In Conferencing Requirements in the Planning documentation.

- View Dial Plan Information
- Create a Dial Plan
- Modify a Dial Plan
- Defining Normalization Rules

1.4.4.1.3.1 View Dial Plan Information

View Dial Plan Information

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-11-01*

To view information for an existing dial plan, perform the steps in the following procedure. If you want to create a new dial plan, see Create a Dial Plan.

⊟To view information about a dial plan from Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins

group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, double-click a dial plan name.

> **Note:**
>
> You can view information for only one dial plan at a time.

⊟To view dial plans by using Windows PowerShell cmdlets

- Dial plans can be viewed by using the Windows PowerShell command-line interface and the **Get-CsDialPlan** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

  To view information about all your dial plans, type the following command in the Lync Server Management Shell, and then press ENTER:

```
Get-CsDialPlan
```

  That command will return information similar to this:

```
Identity                   : Global
Description                :
DialinConferencingRegion   :
NormalizationRules         : {Description=;
                             Pattern=^(\d+)$;Translation=$1;Name=
                             KeepAll;IsInternalExtension=False}
CountryCode                :
State                      :
City                       :
ExternalAccessPrefix       :
SimpleName                 : DefaultProfile
OptimizeDeviceDialing      : False
```

Tasks

Create a Dial Plan
Modify a Dial Plan

1.4.4.1.3.2 Create a Dial Plan

Create a Dial Plan

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-10-06*

To create a new dial plan, perform the steps in the following procedure. If you want to edit a dial plan, see Modify a Dial Plan.

⊟To create a dial plan

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, click **New** and select a scope for the dial plan:
   - **Site dial plan** applies to an entire site, except any users or groups that are assigned to a user dial plan. If you select **Site** for a dial plan's scope, you must choose the site from the **Select a Site** dialog box. If a dial plan has already been created for a site, the site does not appear in the **Select a Site** dialog box.
   - **Pool dial plan** can apply to a public switched telephone network (PSTN) gateway or a Registrar. If you select **Pool** for a dial plan's scope, choose the PSTN gateway or Registrar from the **Select a Service** dialog box. If a dial plan has already been created for a service (PSTN gateway or Registrar), the service does not appear in the list.
   - **User dial plan** can be applied to specified users or groups.

Note:

After you select the dial plan scope, it cannot be changed.

5. If you are creating a user dial plan, enter a descriptive name in the **Name** field on the **New Dial Plan** dialog box. After this name is saved, it cannot be changed.

Note:

For site dial plans, the **Name** field is prepopulated with the site name and cannot be changed.
For pool dial plans, the **Name** field is prepopulated with the PSTN gateway or Registrar name and cannot be changed.

6. The **Simple name** field is prepopulated with the same name that appears in the **Name** field. You can optionally edit this field to specify a more descriptive name that reflects the site, service, or user to which the dial plan applies.

Important:

The **Simple name** must be unique among all dial plans within the Lync Server deployment. It cannot exceed 256 Unicode characters, each of which can be an alphabetic or numeric character, a hyphen (-), a period (.), a plus sign (+), or an underscore (_).
Spaces are not allowed in the **Simple name**.

7. (Optional) In the **Description** field, you can type additional descriptive information about the dial plan.
8. (Optional) If you want to use this dial plan as a region for dial-in access numbers, specify a **Dial-in conferencing region**. If you do not want to use this dial plan for dial-in access numbers, leave this field empty.

Note:

Dial-in conferencing regions are required to associate dial-in conferencing access numbers with one or more dial plans.

9. (Optional) In the **External access prefix** field, specify a value only if users need to dial one or more additional leading digits (for example, 9) to get an external line. You can type in a prefix value of up to four characters (#, *, and 0-9).

Note:

If you specify an external access prefix, you do not need to create a new normalization rule to accommodate the prefix.

10. Associate and configure normalization rules for the dial plan as follows:
    - To choose one or more rules from a list of all normalization rules available in your Enterprise Voice deployment, click **Select**. In **Select Normalization Rules**, highlight the rules you want to associate with the dial plan and then click **OK**.
    - To define a new normalization rule and associate it with the dial plan, click **New**. For details about defining a new rule, see Defining Normalization Rules.

- To edit a normalization rule that is already associated with the dial plan, highlight the rule name and click **Show details**. For details about editing the rule, see Defining Normalization Rules.
- To copy an existing normalization rule to use as a starting point for defining a new rule, highlight the rule name and click **Copy**, and then click **Paste**. For details about editing the copy, see Defining Normalization Rules.
- To remove a normalization rule from the dial plan, highlight the rule name and click **Remove**.

> **Note:**
> Each dial plan must have at least one associated normalization rule. For information about how to determine all of the normalization rules a dial plan requires, see Dial Plans and Normalization Rules in the Planning documentation.

11. Verify that the dial plan's normalization rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name and then click the up or down arrow.

> **Important:**
> Lync Server traverses the normalization rule list from the top down and uses the first rule that matches the dialed number. If you configure a dial plan so that a dialed number can match more than one normalization rule, make sure the more restrictive rules are sorted above the less restrictive ones.
> The default **Keep All** normalization rule **^(\d{11})$** matches any 11-digit number. For example, if you add a normalization rule that matches 11-digit numbers that start with 1425, make sure that **Keep All** is sorted below the more restrictive **^(1425\d{7})$** rule.

12. (Optional) Enter a number to test the dial plan and then click **Go**. The test results are displayed under **Enter a number to test**.

> **Note:**
> You can save a dial plan that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

13. Click **OK**.
14. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

> **Note:**
> Any time you create a dial plan, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Modify a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Defining Normalization Rules

1.4.4.1.3.3 Modify a Dial Plan

Modify a Dial Plan

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-11-01*

To modify an existing dial plan, perform the steps in the following procedure. If you want to create a new dial plan, see Create a Dial Plan.

To modify a dial plan

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, double-click a dial plan name.

   Note:

   The dial plan scope and name were set when the dial plan was created. They cannot be changed.

5. (Optional) In **Edit Dial Plan**, edit the **Simple name** field, which is prepopulated with the same name that appears in the **Name** field to specify a more descriptive name that reflects the site, service, or user to which the dial plan applies.

   Important:

   The **Simple name** must be unique among all dial plans within the Lync Server 2013 deployment. It cannot exceed 256 Unicode characters, each of which can be an alphabetic or numeric character, a hyphen (-), a period (.), a plus sign (+), or an underscore (_).

   Spaces are not allowed in the **Simple name** field.

6. (Optional) In the **Description** field, type descriptive information about the dial plan.
7. (Optional) If you want to use this dial plan as a region for dial-in access numbers, specify a **Dial-in conferencing region**. If you do not want to use this dial plan for dial-in access numbers, leave this field empty.

   Note:

   Dial-in conferencing regions are required to associate dial-in conferencing access numbers with one or more dial plans.

8. (Optional) In the **External access prefix** field, specify a value only if users need to dial one or more additional leading digits to get an external line (for example, 9). You can type in a prefix value of up to four characters (that is, #, *, and 0-9).

   Note:

   If you specify an external access prefix, you do not need to create a new normalization rule to accommodate the prefix.

9. Associate and configure normalization rules for the dial plan:
   - To choose one or more rules from a list of all normalization rules available in your Enterprise Voice deployment, click **Select**. In the **Select Normalization Rules** dialog box, highlight the rules that you want to associate with the dial plan and then click **OK**.
   - To define a new normalization rule and associate it with the dial plan, click **New**. For details about defining a new rule, see Defining Normalization Rules.
   - To edit a normalization rule that is already associated with the dial plan, highlight the rule name and click **Show details**. For details about editing the rule, see Defining Normalization Rules.
   - To copy an existing normalization rule to use as a starting point for defining a new rule, highlight the rule name and click **Copy**, and then click **Paste**. For details about editing the copy, see Defining Normalization Rules.
   - To remove a normalization rule from the dial plan, highlight the rule name and click **Remove**.

   Note:

Each dial plan must have at least one associated normalization rule. For details about how to determine all of the normalization rules a dial plan requires, see Dial Plans and Normalization Rules in the Planning documentation.

10. Verify that the dial plan’s normalization rules are arranged in the correct order. To change a rule’s position in the list, highlight the rule name and then click the up or down arrow.

> **Important:**
>
> Lync Server traverses the normalization rule list from the top down and uses the first rule that matches the dialed number. If you configure a dial plan so that a dialed number can match more than one normalization rule, make sure the more restrictive rules are sorted above the less restrictive ones.
> The default **Keep All** normalization rule **^(\d{11})$** matches any 11-digit number. If, for example, you add a normalization rule that matches 11-digit numbers that start with 1425, make sure that **Keep All** is sorted below the more restrictive **^(1425\d{7})$** rule.

11. (Optional) Enter a number to test the dial plan and then click **Go**. The test results are displayed under **Enter a number to test**.

> **Note:**
>
> You can save a dial plan that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

12. Click **OK**.
13. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

> **Note:**
>
> Any time you create or modify a dial plan, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Defining Normalization Rules

1.4.4.1.3.4 Defining Normalization Rules

Defining Normalization Rules

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-09-23*

Lync Server 2013 normalization rules use .NET Framework regular expressions to translate dialed phone numbers to E.164 format. Each dial plan must be assigned one or more normalization rules.

For details about normalization rules, see Dial Plans and Normalization Rules in the Planning documentation.

For details about how to write regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.

You can use either of the following methods to define or edit a normalization rule:

- Use the **Build a Normalization Rule** tool to specify values for the starting digits, length, digits to remove and digits to add, and then let Lync Server Control Panel generate the corresponding matching pattern and translation rule for you.

- Write regular expressions manually to define the matching pattern and translation rule.
- Create or Modify a Normalization Rule by Using Build a Normalization Rule
- Create or Modify a Normalization Rule Manually

⊟See Also

Tasks

Create a Dial Plan
Modify a Dial Plan

Create or Modify a Normalization Rule by Using Build a Normalization Rule

See Also

Deploying Enterprise Voice > Configuring Dial Plans > Defining Normalization Rules >

Topic Last Modified: *2012-11-01*

Complete the following steps if you want to create or modify a normalization rule in Lync Server Control Panel. Alternatively, if you want to create or modify a normalization rule manually, see Create or Modify a Normalization Rule Manually.

⊟To define a rule by using Build a Normalization Rule

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. (Optional) Follow the steps in Create a Dial Plan through step 11 or Modify a Dial Plan through step 10.
4. In **New Normalization Rule** or **Edit Normalization Rule**, type a name that describes the number pattern being normalized in **Name** (for example, **5DigitExtension**).
5. (Optional) In **Description**, type a description of the normalization rule (for example, "Translates 5-digit extensions").
6. In **Build a Normalization Rule**, enter values in the following fields:
   - **Starting digits** (Optional) Specify the leading digits of dialed numbers you want the pattern to match. For example, type **425** if you want the pattern to match dialed numbers beginning with 425.
   - **Length** Specify the number of digits in the matching pattern and select whether you want the pattern to match this length exactly, match dialed numbers that are at least this length, or match dialed numbers of any length.
   - **Digits to remove** (Optional) Specify the number of starting digits to be removed from dialed numbers you want the pattern to match.
   - **Digits to add** (Optional) Specify digits to be added to dialed numbers you want the pattern to match.

   The values you enter in these fields are reflected in **Pattern to match** and **Translation rule**. For example, if you leave **Starting digits** empty, type **7** into the **Length** field and select **Exactly**, and specify **0** in **Digits to remove**, the resulting regular expression in the **Pattern to match** is:

   ^(\d{7})$

7. In **Translation rule**, specify a pattern for the format of translated E.164 phone numbers as follows:
   - A value that represents the number of digits specified in the matching pattern. For example, if the matching pattern is **^(\d{7})$** then **$1** in the translation rule represents 7-digit dialed numbers.
   - (Optional) Type a value into the **Digits to add** field to specify digits to be prepended to the translated number (for example, **+1425**).

   For example, if **Pattern to match** contains **^(\d{7})$** as the pattern for dialed numbers and **Translation rule** contains **+1425$1** as the pattern for E.164 phone numbers, the rule normalizes 5550100 to +14255550100.
8. (Optional) If the normalization rule results in a phone number that is internal to your organization, select **Internal extension**.
9. (Optional) Enter a number to test the normalization rule, and then click **Go**. The test results are displayed under **Enter a number to test**.

   > **Note:**
   > You can save a normalization rule that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

10. Click **OK** to save the normalization rule.
11. Click **OK** to save the dial plan.
12. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

   > **Note:**
   > Whenever you create or change a normalization rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Normalization Rule Manually
Create a Dial Plan
Modify a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

Create or Modify a Normalization Rule Manually

See Also

Deploying Enterprise Voice > Configuring Dial Plans > Defining Normalization Rules >

Topic Last Modified: *2012-09-22*

Complete the following steps if you want to create or modify a normalization rule manually. If you want to create or modify a normalization rule by using Build a Normalization Rule in Lync Server Control Panel, see Create or Modify a Normalization Rule by Using Build a Normalization Rule.

⊟To define a normalization rule manually

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. (Optional) Follow the steps in Create a Dial Plan or Modify a Dial Plan.
4. In **New Normalization Rule** or **Edit Normalization Rule**, type a name that describes the number pattern being normalized in **Name** (for example, name

the normalization rule **5DigitExtension**).

5. (Optional) In **Description** field, type a description of the normalization rule (for example, "Translates 5-digit extensions").
6. In **Build a Normalization Rule**, click **Edit**.
7. Enter the following in **Type a Regular Expression**:
   - In **Match this pattern**, specify the pattern that you want to use to match the dialed phone number.
   - In **Translation rule**, specify a pattern for the format of translated E.164 phone numbers.

   For example, if you enter **^(\d{7})$** in **Match this pattern** and **+1425$1** in **Translation rule**, the rule normalizes 5550100 to +14255550100.
8. (Optional) If the normalization rule results in a phone number that is internal to your organization, select **Internal extension**.
9. (Optional) Enter a number to test the normalization rule and then click **Go**. The test results are displayed under **Enter a number to test**.

   Note:
   You can save a normalization rule that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.
10. Click **OK** to save the normalization rule.
11. Click **OK** to save the dial plan.
12. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

    Note:
    Whenever you create or change a normalization rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Normalization Rule by Using Build a Normalization Rule
Create a Dial Plan
Modify a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

1.4.4.1.4 Make Sure Dial Plans Have Assigned Regions

Make Sure Dial Plans Have Assigned Regions

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2010-11-02*

Dial plans that are used for dial-in conferencing need to have a **Dial-in conferencing region** specified to associate dial-in conferencing access numbers with the appropriate dial plan. When you set up a dial plan, you specify the dial-in conferencing region that applies to that dial plan. Then, when you create the dial-in access number, you select the regions that associate the access number with the appropriate dial plans.

Because it important to specify a region for all dial plans, we recommend that you use this procedure to verify that all dial plans have regions. This step is optional.

Use the **Get-CsDialPlan** cmdlet to verify whether the region is set for all dial-in conferencing dial plans. If the region is missing from dial plans, you can use the **Set-CsDialPlan** cmdlet to set the region. You can also use Lync Server Control Panel to update the region in existing dial plans. For details about using Lync Server Control Panel, see Modify a Dial Plan.

To verify whether dial plans have the region property set

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-VoiceAdministrator**, **Cs-ServerAdministrator**, or **CsAdministrator** role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run the following at the command prompt:

   ```
   Get-CsDialPlan [-Identity <Identifier of the dial plans to be retrieve
   ```

   For example:

   ```
   Get-CsDialPlan
   ```

   In this example, all the dial plans configured for your organization are returned.
4. Review the returned dial plans to identify any that are missing the dial-in conferencing region. For details, see the Lync Server Management Shell documentation.

To set the region property for a dial plan

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-VoiceAdministrator**, **Cs-ServerAdministrator**, or **CsAdministrator** role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. For any dial plans that are missing the dial-in conferencing region, run:

   ```
   Set-CsDialPlan [-Identity <Identity of the dial plan to be modified>]
   ```

   For example:

   ```
   Set-CsDialPlan -Identity Redmond -DialinConferencingRegion "US West Co
   ```

   In this example, the dial plan with the Identity of Redmond is modified to set the DialinConferencingRegion property to "US West Coast". For details, see the Lync Server Management Shell documentation.

1.4.4.1.5 (Optional) Verify PIN Policy Settings

(Optional) Verify PIN Policy Settings

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2012-06-20*

Lync Server 2013 users who have Active Directory Domain Services (AD DS) credentials can enter a personal identification number (PIN) to join dial-in conferences as authenticated users. A PIN policy defines the rules for how dial-in conferencing PINs work.

When you deploy dial-in conferencing, you should verify that the default global PIN policy meets your requirements. If you need to make changes, you can modify the default global policy or you can create a new PIN policy. You can create PIN policies that apply to a specific site, a specific user, or a specific group of users.

- Modify the Default Dial-in Conferencing PIN Settings
- Create or Modify Dial-in Conferencing PIN Settings for a Site or Group of Users

1.4.4.1.5.1 Modify the Default Dial-in Conferencing PIN Settings

Modify the Default Dial-in Conferencing PIN Settings

Deploying Conferencing > Configuring Dial-in Conferencing > (Optional) Verify PIN Policy Settings >

Topic Last Modified: *2012-10-18*

The global PIN policy defines the rules for dial-in conferencing PINs at the forest level. Follow these steps to modify the global dial-in conferencing PIN policy. For details about creating or modifying a dial-in conferencing PIN policy at the site or user level, see Create or Modify Dial-in Conferencing PIN Settings for a Site or Group of Users.

⊟To modify the global PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click the **Global** policy, click **Edit**, and then click **Show details**.
5. In **Edit PIN Policy**, in **Minimum PIN length**, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
6. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum number of attempts is automatically determined.
7. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
8. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
9. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
10. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
11. To allow common patterns of digits in PINs, such as sequential numbers and repetitive sets of numbers, select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

◆**Important:**
We recommend that you do not allow common patterns.

12. Click **Commit**.

1.4.4.1.5.2 Create or Modify Dial-in Conferencing PIN Settings for a Site or Group of Users

Create or Modify Dial-in Conferencing PIN Settings for a Site or Group of Users

Deploying Conferencing > Configuring Dial-in Conferencing > (Optional) Verify PIN Policy Settings >

Topic Last Modified: *2012-10-18*

Follow these steps to create or modify a user-level or a site-level dial-in conferencing personal identification number (PIN) policy. For details about how to change the global PIN policy, see Modify the Default Dial-in Conferencing PIN Settings.

⊟To create a user or site PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click **New**, and then do one of the following:
   - To create a user-level policy, click **User policy**. In **New PIN Policy**, in **Name**, type a name that describes the policy.
   - To create a site-level policy, click **Site policy**. In the **Select a Site** search field, type all or part of the name of the site for which you want to create a policy. In the list of sites, click the site you want, and then click **OK**.
5. In the **Description** field, type a description of the PIN policy.
6. In the **Minimum PIN length** field, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
7. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum number of attempts is automatically determined.
8. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
9. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
10. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
11. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
12. To allow common patterns of digits in PINs, such as sequential numbers and repetitive sets of numbers, select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

◆**Important:**
We recommend that you do not allow common patterns.

13. Click **Commit**.

⊟To change a user or site PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.

4. On the **PIN Policy** page, click the PIN policy that you want to change, click **Edit**, and then click **Show details**.
5. In **Edit PIN Policy**, modify any of the policy settings (except for the policy name, which cannot be modified).

6. Click **Commit**.

1.4.4.1.6 Configure Conferencing Policy for Dial-in

Configure Conferencing Policy for Dial-in

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2012-10-07*

Conferencing policy is a user account setting that specifies the conferencing experience for participants. You can create conferencing policies with a site scope or a user scope. Conferencing policy settings encompass many aspects of conference scheduling and participation. Several conferencing policy settings support dial-in conferencing for participants. When you configure dial-in conferencing, you should verify that these fields are set appropriately for your organization, and modify them as necessary.

Verify the following fields in your conferencing policy:

- **Allow participants to invite anonymous users** This setting allows meeting organizers to invite anonymous (that is, unauthenticated) participants to meetings. This setting is optional for dial-in conferencing. This setting is selected by default in the default global conferencing policy.
- **Enable PSTN dial-in conferencing** This setting allows users to join the audio portion of a conference by dialing in from the PSTN. This setting is required for dial-in conferencing. This setting is selected by default in the default global conferencing policy.
- **Allow anonymous participants to dial out** This setting allows anonymous users who are already joined to the meeting to dial out to a phone number to join the audio portion of the conference. This setting is optional for dial-in conferencing. This setting is not selected by default in the default global conferencing policy.
- **Allow participants not enabled for Enterprise Voice to dial out** This setting allows meeting participants and organizers that are not enabled for Enterprise Voice to dial out to a phone number to join the audio portion of the conference. The dial-out call is authorized based on the organizer’s assigned voice policy. This setting is not selected by default in the default global conferencing policy. The setting default value is disabled.

Note:
To enable this capability, a meeting organizer that is not enabled for Enterprise Voice should have an appropriate voice policy assigned to them to authorize any dial-out from a conference organized by that user. A voice policy can be assigned to a user that is not enabled for Enterprise Voice from the Lync Server Management Shell. If the user does not have a voice policy explicitly assigned to him, the global voice policy will be used to authorize the dial-out request.

The procedure in this section explains how to modify conferencing policy. For details about how to configure all of the settings that define the participant experience in the default conferencing policy, see Create or Modify a Collection of Meeting Configuration Settings. For details about how to create a conferencing policy for a specific user or group of users, see Create or Modify a Conferencing Policy. For a list of all available conferencing policy settings, see Conferencing Policy Settings Reference.

⊟To modify the conferencing policy for dial-in

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-ServerAdministrator** or **CsAdministrator** role.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**.
4. On the **Conferencing Policy** tab, double-click a conferencing policy name to open the **Edit Conferencing Policy** dialog box.
5. Verify that the fields for dial-in conferencing are appropriate for your organization, and modify the settings if necessary.
6. Click **Commit**.

1.4.4.1.7 Configure Dial-in Conferencing Access Numbers

Configure Dial-in Conferencing Access Numbers

See Also

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2011-07-17*

When you deploy dial-in conferencing, you need to set up phone numbers that users can dial from the public switched telephone network (PSTN) to join the audio portion of conferences. These dial-in access numbers appear in meeting invitations and on the Dial-in Conferencing Settings webpage.

Before you can create dial-in access numbers, you must first plan your dial-in conferencing regions and then configure dial plans with the regions. For details about regions, see Dial-In Conferencing Requirements in the Planning documentation. For details about configuring dial plans for dial-in conferencing, see Configure Dial Plans for Dial-in Conferencing.

Note:
You cannot use a new dial-in access number until Active Directory Domain Services (AD DS) replication of that access number is complete. Replication can take several hours to complete.

Note:
After you create dial-in access numbers, you can modify the display name for the Active Directory contact objects so that users can more easily identify the correct access number. Use the **Set-CsDialInConferencingAccessNumber** cmdlet to modify the display name. You should not modify Active Directory objects manually. For details about modifying an access number, see Lync Server Management Shell documentation for the **Set-CsDialInConferencingAccessNumber** cmdlet.

Create or Modify a Dial-in Conferencing Access Number

⊟See Also

Concepts

Dial-In Conferencing Requirements

Other Resources

Configure Dial Plans for Dial-in Conferencing

1.4.4.1.7.1 Create or Modify a Dial-in Conferencing Access Number

Create or Modify a Dial-in Conferencing Access Number

Deploying Conferencing > Configuring Dial-in Conferencing > Configure Dial-in Conferencing Access Numbers >

Topic Last Modified: *2012-09-17*

Follow these steps if you want to create or modify a dial-in conferencing access number.

Important:
Before you create a new dial-in access number, you must set a dial-in conferencing region in the dial plan that is associated with the new dial-in access number. Multiple dial plans can use the same region.

⊟To create or modify a dial-in access number

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Dial-in Access Number**.
4. On the **Dial-in Access Number** page, do one of the following:
   - Click **New** to open **New Dial-in Access Number**.
   - Click one of the dial-in access numbers in the list, click **Edit**, and then click **Show details**.

Note:
Using the search field to search for the contents of a column in the list of dial-in access numbers may not yield the results you expect. Instead, sort the list by the column of interest to identify the dial-in access number you want to view or change.

5. In **Display number**, type the phone number that public switched telephone network (PSTN) phone users dial to join a conference.

Note:
This number is displayed in meeting invitations and on the Dial-in Conferencing Settings webpage.

6. In **Display name**, type a description for the dial-in access number. This is the name that is associated with the dial-in access number in Lync search results.

Note:
This name is displayed in the client when a user calls the access number.

7. In **Line URI**, type the E.164 number of the dial-in access number in TEL URI format, including the + symbol before the number and excluding spaces. For example, tel:+14255550200.

Note:
The same Line URI cannot be reused by another dial-in conferencing access number.

8. In **SIP URI**, do the following:
   - In the text box, type a unique SIP URI for this dial-in conferencing access number. This SIP URI is displayed in various locations including, but not limited to, call notification messages and previous versions of Communicator clients.

Note:

> The same SIP URI cannot be reused by another dial-in conferencing access number. The SIP URI cannot be modified after the access number is created. The only way to change the SIP URI is to delete and recreate the access number.

- In the drop-down list box, click the domain of the Conferencing Attendant application that supports this dial-in access number.

9. In **Pool**, click the pool that is running the instance of Conferencing Attendant that supports this dial-in access number.

> **Note:**
> If you need to change the pool after you create the access number, you must use the **Move-CsApplicationEndpoint** cmdlet or delete and recreate the access number.

10. In **Primary language**, click the language in which prompts are played for this dial-in access number.

> **Note:**
> The primary language is the language that the Conferencing Attendant uses to answer the call. Supported languages are displayed alongside each access phone number on the Dial-in Conferencing Settings webpage.

11. (Optional) In **Secondary languages (maximum of four)**, click **Add**, select one or more additional languages that you want to support for callers to this dial-in access number, and then click **OK**.

> **Note:**
> You can choose up to four secondary languages for each dial-in access number. Users can select a secondary language before entering the conference ID when they dial in to a conference.

12. To add a region for the dial-in access number, under **Associated regions**, click **Add**, click one or more regions that are associated with the dial plans for this dial-in access number, and then click **OK**.
13. To delete a region from the dial-in access number, under **Associated regions**, click the region you want to delete, and then click **Remove**.

14. Click **Commit**.

1.4.4.1.8 (Optional) Verify Dial-in Conferencing Settings

(Optional) Verify Dial-in Conferencing Settings

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2010-11-02*

As final verification of your dial-in conferencing configuration, you can search for dial plans that have a dial-in conferencing region that is not used by any access number and for access numbers that have not specified a dial-in conferencing region. This step is optional.

⊟To find dial plans with a dial-in conferencing region that is not used by an access number

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-ServerAdministrator** or **CsAdministrator** role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

3. Run the following at the command prompt:

```
Get-CsDialinConferencingAccessNumber -EmptyRegion
```

This cmdlet returns all of the dial plans that have a dial-in conferencing region that is not used by an access number.

⊟To find access numbers without assigned regions

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-ServerAdministrator** or **CsAdministrator** role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run the following at the command prompt:

```
Get-CsDialinConferencingAccessNumber -Region NULL
```

This cmdlet returns all the dial-in conferencing access numbers that are not associated with a region.

1.4.4.1.9 (Optional) Modify Key Mapping for DTMF Commands

(Optional) Modify Key Mapping for DTMF Commands

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2012-09-30*

Dial-in conferencing users can press keys on the telephone keypad to perform dual-tone multi-frequency (DTMF) commands. DTMF commands enable users who dial in to a conference to control conference settings (such as muting and unmuting themselves or locking and unlocking the conference) by using the keypad on their telephone. You can use cmdlets to modify the keys used for the DTMF commands. This step is optional.

Note:

For details about these cmdlets and the possible DTMF options, see Lync Server Management Shell documentation or Lync Server Management Shell command-line Help.

⊟To modify the key mapping of DTMF commands

1. Log on to the computer as a member of the **RTCUniversalServerAdmins** group, or as a member of the **Cs-ServerAdministrator** or **CsAdministrator** role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run the following at the command prompt:

```
Get-CsDialinConferencingDtmfConfiguration
```

This cmdlet returns the DTMF settings used for dial-in conferencing.

4. Run the following cmdlet and specify the key to be pressed for each option that you want to change:

```
Set-CsDialinConferencingDtmfConfiguration [-Identity <global or site c
[-AdmitAll <default key is 8>] [-AudienceMuteCommand <default key is 4
[-CommandCharacter <* (default) | #>] [-EnableDisableAnnouncementsComm
[-HelpCommand <default key is 1>] [-LockUnlockConferenceCommand <defau
[-MuteUnmuteCommand <default key is 6>] [-PrivateRollCallCommand <defa
```

This cmdlet modifies the DTMF settings used for dial-in conferencing.

For example:

```
Set-CsDialinConferencingDtmfConfiguration -EnableDisableAnnouncementsC
```

This example swaps the key that is pressed to enable or disable announcements and the key that is pressed to mute and unmute all participants. Because no Identity is specified, these changes apply to the global DTMF settings.

5. (Optional) To create additional sets of DTMF commands for specific sites, use the **New-CsDialinConferencingDtmfConfiguration** cmdlet with a site identity. When you create new DTMF settings for sites, the site settings take precedence over the global settings. For details, see Lync Server Management Shell documentation or Lync Server Management Shell command-line Help.

1.4.4.1.10 (Optional) Enable and Disable Conference Join and Leave Announcements

(Optional) Enable and Disable Conference Join and Leave Announcements

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2012-09-30*

When dial-in users join or leave a conference, the Conferencing Announcement application can announce their entrance or exit by playing a tone or saying their names. You can change how announcements work by running cmdlets. This step is optional.

To modify the conference join and leave announcement behavior

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-ServerAdministrator** or **CsAdministrator** role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run the following at the command prompt:

```
Get-CsDialinConferencingConfiguration
```

This cmdlet retrieves information about whether participants are required to record their name when joining a conference and how Lync Server responds when participants join or leave a dial-in conference.

4. Run the following at the command prompt:

```
Set-CsDialinConferencingConfiguration -Identity <identity of dial-in c
[-EnableNameRecording <$true | $false>]
[-EntryExitAnnouncementsEnabledByDefault <$true | $false>]
[-EntryExitAnnouncementsType <UseNames | ToneOnly]
```

EnableNameRecording Determines whether anonymous participants are asked to record their name before entering the conference. The default value is "$true," which means that anonymous participants are prompted to state their name when joining a conference. (Authenticated participants do not record their name because their display name is used instead.)

EntryExitAnnouncementsEnabledByDefault Indicates whether announcements are turned on or off by default. The default value is "$false," which means that by default there are no announcements when participants join or leave a conference. The meeting organizer can override this setting when scheduling a meeting.

EntryExitAnnouncementsType Indicates the action taken whenever a participant joins or leaves a conference for which announcements are enabled. The default value is "UseNames," which means there is an announcement similar to the following: "Ken Myer has joined the conference" when announcements are turned on.

You can configure these settings at the global scope or at the site scope. Settings configured at the site scope take precedence over settings configured at the global scope.

For example:

```
Set-CsDialinConferencingConfiguration -Identity site:Redmond
-EnableNameRecording $false
-EntryExitAnnouncementsEnabledByDefault $true
-EntryExitAnnouncementsType ToneOnly
```

In this example, settings are configured at the site scope for Redmond. Announcements are turned on, but participants are not prompted to say their name when they join a conference. A tone is played when participants enter or leave a conference.

1.4.4.1.11 (Optional) Verify Dial-in Conferencing

(Optional) Verify Dial-in Conferencing

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2011-01-21*

To verify that the Dial-in Conferencing Settings webpage and the dial-in access numbers work correctly, you need to do the following:

- Test the Dial-in Conferencing Settings webpage by signing in to the simple URL.
- Test that access numbers work correctly for a specific pool by running the script later in this topic. This script simulates calls to access numbers. You need the SIP address and credentials of one unified communications (UC) client that is hosted on the specific pool to use this script.

This step is optional.

To test access numbers for a specific pool

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-ServerAdministrator** or **CsAdministrator** role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run the following at the command prompt:

```
$credentials = Get-Credential
   User name:  testuser1@contoso.com
   Password:   ********
Test-CsDialInConferencing -UserSipAddress sip:testuser1@contoso.com -U
```

The resulting report shows either Success or Failure, along with specific diagnostic information. The –Verbose flag provides more detailed information about how many access numbers were found and details about them.

1.4.4.1.12 Deploy the Online Meeting Add-in for Lync 2013

Deploy the Online Meeting Add-in for Lync 2013

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2012-09-30*

Deploy the Online Meeting Add-in for Lync 2013 so that users can schedule conferences that support dial-in conferencing.

The Online Meeting Add-in for Lync 2013 is installed automatically when you install Lync 2013. For details about customizing Online Meeting Add-in for Lync 2013 for Lync, see Configuring the Meeting Invitation.

1.4.4.1.13 Configure User Account Settings

Configure User Account Settings

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2012-10-05*

Dial-in users enter their phone number or extension and a PIN to join conferences as authenticated users. The telephony **Line URI** specified on Lync Server user accounts is required for authentication.

The procedure in this topic describes how to assign a **Line URI** for a single user account. If you need to assign a **Line URI** for multiple user accounts, you can create a script that uses the **Set-CsUser** cmdlet. For details about using a sample script to assign **Line URI** to multiple user accounts, see "Assign Line URIs to Multiple Users" at http://go.microsoft.com/fwlink/p/?linkId=196945.

⊟To configure user account settings

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **Cs-UserAdministrator** or **CsAdministrator** role.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the search field, type the name of the user you want to configure for dial-in conferencing or click **Add filter** to specify search fields, and then click **Find**.
5. Double-click the user name to open the **Edit Lync Server User** dialog box.
6. Under **Telephony**, in the **Line URI** field, type a unique, normalized phone number (for example, tel:+14255550200).

   > **Note:**
   >
   > You can specify **Line URI** only if **Telephony** is set to **PC-to-PC only**, **Enterprise Voice**, **Remote call control** or **Remote call control only**.

7. Click **Commit**.

1.4.4.1.14 (Optional) Welcome Users to Dial-in Conferencing

(Optional) Welcome Users to Dial-in Conferencing

Deployment > Deploying Conferencing > Configuring Dial-in Conferencing >

Topic Last Modified: *2012-09-30*

After you configure dial-in conferencing and test to verify that it is functioning properly, you should set initial personal identification numbers (PINs) for users and notify users about the availability of the feature, including introductory instructions such as the initial PIN and the link to the Dial-in Conferencing Settings webpage. This step is optional. Typically, you use the **Set-CsClientPin** cmdlet to reset PINs, but you can use the procedure in this topic the first time if you want to send a welcome email with the information. If you do not want to send the email, you can use **Set-CsClientPin** instead.

You can use the **Set-CsPinSendCAWelcomeMail** script to set the PIN and send a welcome email to a single user. By default, the script does not reset a PIN if it is already set, but you can use the **Force** parameter to force reset a PIN. The email message is sent using Simple Mail Transfer Protocol (SMTP).

You can create a script that runs the **Set-CsPinSendCAWelcomeMail** script iteratively to set PINs and send email to a group of users. You can modify the email template (that is, the **CAWelcomeEmailTemplate.html** file) to add more links to intranet pages or modify the email text.

To set an initial PIN and send welcome email

1. Log on as a member of the RTCUniversalServerAdmins group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run the following at the command prompt:

```
Set-CsPinSendCAWelcomeMail -UserUri <user identifier>
-From <email address of sender> [-Subject <subject for email message>]
[-UserEmailAddress <destination email address>]
[-Cc <email address of recipients who receive copy of email>]
[-Bcc <email address of recipients who receive blind copies>]
[-TemplatePath <path for email template>]
[-SmtpServer] <SMTP server name>]
[-BodyAsPlainText] [-UseSsl]
[-Pin <new numeric PIN>] [-Force] `
[-Credential <SMTP server credentials used to send email with the spec
```

SmtpServer By default, the script uses the value of the reserved environment variable **$PSEmailServer** for this parameter. If the **$PSEmailServer** variable is not set, you must specify this parameter.

Credential By default, the script uses the credentials of the current user. If the current user does not have permission to send email on behalf of the specified From address, you must specify this parameter. As a general rule, specify this parameter if you do not specify your email address as the From address.

For example:

```
Set-CsPinSendCAWelcomeMail -UserUri "bob@contoso.com"
-From "marco@contoso.com"
```

This example creates a new PIN and then sends a welcome email from Marco to Bob. It uses the email text from the default template and creates the email message in HTML format. The default Subject is "Welcome to Dial In Conferencing".

Another example:

```
Set-CsPinSendCAWelcomeMail -UserUri "bob@contoso.com"
-From "marco@contoso.com" -Subject "Your new dial-in conferencing PIN"
-Pin "383042650" -Force
-Credential Admin@contoso.com -UseSsl
```

This example forces a new PIN with a value of "383042650" for Bob, even though Bob had an existing PIN, and then sends a welcome email from Marco to Bob. Because the Credential parameter is specified, the person running the command is prompted to enter a password. The email is sent by using the Secure Sockets Layer (SSL).

1.4.4.2 Enabling Office Web Apps Server and Lync Server 2013

Configuring Integration with Office Web Apps Server and Lync Server 2013

Microsoft Lync Server 2013 > Deployment > Deploying Conferencing >

Topic Last Modified: *2013-01-22*

Lync Server 2013 employs Office Web Apps Server to handle PowerPoint presentations. For information about the advantages to this approach, see Web Conferencing Overview.

In order to use these new capabilities administrators must install Office Web Apps Server and they must configure Lync Server 2013 to communicate with Office Web Apps Server. This documentation provides information on how to configure Lync Server 2013 to work with Office Web Apps Server. What this documentation does not provide is information on how to install Office Web Apps Server itself; for that information, see the Microsoft Office Web Apps Deployment website at http://go.microsoft.com/fwlink/p/?linkid=257525. That guide includes complete prerequisite information for Office Web Apps Server; note that Office Web Apps Server should be installed on a stand-alone computer that is not running Lync Server, Microsoft SQL Server, or any other server application. (You must not have any version of Microsoft office installed on that computer.) Any computer used to run Office Web Apps Server must also have a specific set of software installed (including .NET Framework 4.5 and Windows PowerShell 3.0); these requirements, along with information on configuring certificates and Internet Information Services (IIS), are discussed in detail in the Microsoft Office Web Apps Deployment website at http://go.microsoft.com/fwlink/p/?linkid=257525.

This document covers the following topic areas:

- Configuring Lync Server 2013 to Work with Office Web Apps Server
- Publishing Office Web Apps Server Using a Reverse Proxy Server
- Validating the Configuration of Office Web Apps Server
- Configuring Clients for Use With Office Web Apps Server

1.4.4.2.1 Configuring Lync Server 2013 to Work with Office Web Apps Server

Configuring Lync Server 2013 to Work with Office Web Apps Server

Deployment > Deploying Conferencing > Configuring Integration with Office Web Apps Server and Lync Server 2013 >

Topic Last Modified: *2013-02-25*

Before you can configure Lync Server 2013 to use Office Web Apps Server, Office Web Apps Server must be deployed and configured. See the document **Guide to Deploying Office Web Apps Server and Office Web Apps** for detail information on how to install and configure a single Office Web Apps Server, or for information on how to install and configure an Office Web Apps Server Farm for high availability.

After Office Web Apps Server has been successfully installed and your Web farm correctly configured, you must then configure Lync Server to communicate with the new server; this is done by adding the Office Web Apps Server discovery URL to your Lync Server topology. To add Office Web Apps Server to your topology, complete the following steps:

1. Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013 (Preview)**, and then click **Lync Server Topology Builder**.
2. In the **Topology Builder** dialog box, select **Download Topology from existing deployment** and then click **OK**.
3. In the **Save Topology As** dialog box, type a name for your topology document (for example, **PreWebAppsServerTopology**) in the **File name** box and then click **Save**. This topology can later be retrieved and republished if you encounter problems with your new topology.
4. In Topology Builder, expand **Lync Server 2013 (Preview)**, expand the name of your site, expand **Enterprise Edition Front End pools**, right-click the name of one of your pools, and then click **Edit Properties**.
5. In the **Edit Properties** dialog box, on the **General** tab, find the heading **Associate Office Web Apps Server** and then click **New** (or select an existing Office Web Apps Server from the drop-down list).
6. In the **Define New Office Web Apps Server** dialog box, type the fully qualified domain name (FQDN) of your Office Web Apps Server computer in the **Office Web Apps Server FQDN** box; when you do this, your Office Web Apps Server discovery URL should automatically be entered into the **Office Web Apps Server discovery URL** box.
   If the Office Web Apps Server is installed on-premises and in the same network zone as Lync Server 2013 then the option **Office Web Apps Server is deployed in an external network (that is, perimeter/Internet)** should not be selected.
   If the Office Web Apps Server is deployed outside your internal firewall, then select the option **Office Web Apps Server is deployed in an external network (that is, perimeter/Internet)**.
7. In the **Define New Office Web Apps Server** dialog box, click **OK**, and then click **OK** in the **Edit Properties** dialog box. The Office Web Apps discovery URL will then be listed as one of the pool's Associations.

You will have to repeat this process for each pool that needs to be associated with your Office Web Apps Server.

After you have added the discovery URL to the topology you must then publish this updated topology. To do that in Topology Builder:

1. Click **Action** and then click **Publish Topology**.
2. In the Publish Topology wizard, on the **Publish the Topology** page, click **Next**.
3. On the **Publishing wizard complete** page, click **Finish**.

4. Close Topology Builder.

1.4.4.2.2 Publishing Office Web Apps Server Using a Reverse Proxy Server

Publishing Office Web Apps Server Using a Reverse Proxy Server

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2013-02-25*

If you want external users (that is, users logging on from outside your organization’s firewall) to have access to Office Web Apps Server PowerPoint presentations then you will need to use Office Web Apps Server and a reverse proxy server such as Microsoft Forefront Threat Management Gateway. That also means that you will need to create and configure a website publishing rule; that rule will help ensure that users are able to connect to the server. If you do not need to provide access to external users then you do not need to configure a website publishing rule.

To configure a website publishing rule in Forefront Threat Management Gateway complete the following procedure:

1. Click **Start**, click **All Programs**, click **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In Forefront TMG, right-click **Firewall Policy**, point to **New**, and then click **Web Site Publishing Rule**.
3. In the New Web Publishing Rule Wizard, on the **Welcome to the New Web Publishing Rule Wizard** page, type a name for your new rule in the **Web publishing rule name** box (for example, **Office Web Apps Server Rule**) and then click **Next**.
4. On the **Specify Rule Action** page, select **Allow** and then click **Next**.
5. On the **Publishing Type** page, select **Publish a single Web site or load balancer** and then click **Next**.
6. On the **Server Connection Security** page, select **Use SSL to connect to the published Web server or server farm** and then click **Next**.
7. On the **Internal Publishing Details** page, type the FQDN of your Office Web Apps server (for example, **officewebapps01.contoso.com**) in the **Internal site name** box and then click **Next**. The name entered in the **Internal site name** box must appear in the Subject field or the Subject Alternative Name field of the certificate you have assigned to Office Web Apps Server.
8. On the **Internal Publishing Details** page, type **/*** in the **Path (optional)** box and then click **Next**. The /* syntax will help ensure that all the folders and subfolders for the site are published.
9. On the **Public Name Details** page, select **This domain name (type below)** from the **Accept requests for** drop-down list and then type the fully qualified for your Office Web Apps Server in the Public name box. This name should be the name used to access your website. For example, if your site is accessed using the URL http://officewebapps01.contoso.com then you should enter **officewebapps01.contoso.com** in the **Public name** box.
10. Click **Next**.
11. On the **Select Web Listener** page, click **New**.
12. In the New Web Listener Definition Wizard, type a name for the new Web listener (for example, **SSL**) in the **Web listener name** box and then click **Next**.
13. On the **Client Connection Security** page, select **Require SSL secured connections with clients** and then click **Next**.
14. On the **Web Listener IP Addresses** page, select **External**, select **Internal**, and then click **Next**.
15. On the **Listener SSL Certificates** page, select **Use a single certificate for this Web Listener** and then click **Select Certificate**.
16. In the **Select Certificate** dialog box, select the certificate to be used for this Web Listener and then click **Select**.
17. On the **Listener SSL Certificates** page, click **Next**.
18. On the **Authentication Settings** page, select **No Authentication** from the **Select how clients will provide credentials to Forefront TMG** drop-down list, and then click **Next**.
19. On the **Single Sign On Settings** page, click **Next**.
20. On the **Completing the New Web Listener Wizard** page, review the summary of the configuration choices you have made. When ready, click **Finish**.
21. On the **Select Web Listener** page, click **Next**.
22. On the **Authentication Delegation** page, select **No delegation, but client may authenticate directly** from the **Select the method used by Forefront TMG to authenticate to the published Web server** drop-down list and then click **Next**.
23. On the **User Sets** page, confirm that the appropriate user sets are listed. By default, this is the **All Users** user set. Click **Add** to add other user sets you may have defined. When complete, click **Next**.
24. On the **Completing the New Web Publishing Rule Wizard** page, click

Finish.

Note that clicking **Finish** does not mean that you completed the process; that is, this does not automatically apply and enable the new rule. Instead, you will need to click the **Apply** button that will appear in the Forefront TMG user interface. When you click **Apply** the **Configuration Change Description** dialog box will appear. Click **Apply** in that dialog box to enable the new publishing rule.

After your new rule has been applied, you will then need to make some minor modifications to the rule to make sure that users can use the new PowerPoint presentation capabilities. To do that, complete the following procedure:

1. In Forefront TMG, right-click the name of the new publishing rule and then click **Properties**.
2. In the **Properties** dialog box, on the **To** tab, select the option **Forward the original host header instead of the actual one**.
3. On the **Traffic** tab, click **Filtering** and then click **Configure HTTP**.
4. In the **Configuring HTTP policy for rule** dialog box, clear the **Verify normalization** check box and then click **OK**.
5. In the **Properties** dialog box, click **OK**.
6. In Forefront TMG, click **Apply** to enable the changes. When the **Configuration Change Description** dialog box appears, click **Apply**.

After completing the installation you can test your Office Web Apps Server using the procedures in the topic Validating the Configuration of Office Web Apps Server.

1.4.4.2.3 Validating the Configuration of Office Web Apps Server

Validating the Configuration of Office Web Apps Server

Deployment > Deploying Conferencing > Configuring Integration with Office Web Apps Server and Lync Server 2013 >

Topic Last Modified: *2012-08-29*

After Office Web Apps Server has been added to the topology, and after that topology has been published, you should see two new event log events in the Lync Server event log. First, an LS Data MCU event (event ID 41032) should be added; this event will report that the Office Web Apps Server has been discovered:

Web Conferencing Server WAC is discovered, PowerPoint content is enabled.

In addition to that you should see another LS Data MCU event (event ID 41032) that reports back Office Web Apps Server URLs. For example, you should see something similar to this:

Web Conferencing Server WAS discovery has succeeded.

WAC internal presenter page: https://atl-officewebapps-001.litwareinc.com/m/Presenter.aspx?a=0&embed=

WAC internal attendee page: https://atl-officewebapps-001.litwareinc.com/m/ParticipantFrame.aspx?a=0&embed=true&=

WAC external presenter page: https://atl-officewebapps-001.litwareinc.com/m/Presenter.aspx?a=0&embed

WAC internal attendee page: https://atl-officewebapps-001.litwareinc.com/m/ParticipantFrame.aspx?a=0&embed=true&

If you see an LS Data MCU event with the event ID of 41033 that means that Office Web Apps Server discovery has failed. In that case, Microsoft Lync Server 2013 will try as many times as needed to discover the newly-configured Office Web Apps Server. If the discovery process fails repeatedly you should remove Office Web Apps Server from your topology document, publish the updated topology, and then try adding Office Web Apps Server back to the topology after the connectivity issues have been resolved.

If Office Web Apps Server appears to be configured correctly and has been recognized by the discovery process you can verify that Office Web Apps Server is working as expected by sharing a PowerPoint presentation between a pair of Microsoft Lync 2013 clients. If User A can load and display the PowerPoint presentation and if User B can then join the meeting and see that presentation then Office Web Apps Server is working.

Even if Office Web Apps Server appears to be configured correctly, you could potentially receive the error message “Some sharing features are unavailable due to server connectivity issues” when you try sharing a PowerPoint presentation. If you receive that error message you should restart the Front End server (or servers) associated with the new Office Web Apps Server.

1.4.4.2.4 Configuring Clients for Use With Office Web Apps Server

Configuring Clients for Use With Office Web Apps Server

Deployment > Deploying Conferencing > Configuring Integration with Office Web Apps Server and Lync Server 2013 >

Topic Last Modified: *2013-02-25*

If you want users to experience the full capabilities of Office Web App Server then you should upgrade those users to Microsoft Lync 2013; only users of Lync 2013 will be able to do such things as scroll through PowerPoint slides independent of the actual PowerPoint presentation. (That is, these users can look at any slide in the presentation at any time, without interfering in any way with the actual presentation.) Users who are not using Lync 2013 will still be able to join online conferences and view the PowerPoint presentation; however, they will not be able to independently scroll through the slides, nor will they be able to see slide transitions or view embedded videos.

Note that these capabilities will always be available to users of Lync 2013; this is true even if the PowerPoint presenter is running Microsoft Lync 2010. If a PowerPoint presentation is being hosted by a user running Lync 2010, Lync Server 2013 will coordinate with Office Web Apps Server to make sure that Lync 2013 users will view the Office Web Apps Server version of that presentation. Office Web Apps Server does not provide PowerPoint services for users running clients other than Lync 2013. Instead, those users connect to the Conferencing server service and view PowerPoint presentations the same way they did in Microsoft Lync Server 2010. This also means that these users will only have access to the more-limited capabilities offered by Lync Server 2010.

Although no client configuration is required for Office Web Apps Server (other than upgrading users to Lync 2013), it is recommended that conference attendees be upgrade to Internet Explorer 9. Although conferences can be accessed using Internet Explorer 8, there are some limitations to using that Web browser. For example, users of Internet Explorer 8 will not be able to resize the PowerPoint stage to a custom size; instead, they will be limited to using one of three predefined stage sizes. Likewise, Internet Explorer 8 users will not be able to play media files.

1.4.4.3 Configuring the Meeting Join Page

Configuring the Meeting Join Page

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Conferencing >

Topic Last Modified: *2012-12-14*

When a user clicks a meeting link in a meeting request, the meeting join page detects whether a Lync 2013 client is already installed on the user's computer. If a client is already installed, the client opens and joins the meeting. If a client is not installed, by default the 2013 version of Lync Web App opens.

You can modify the behavior of the meeting join page if you want to allow users to join meetings with Office Communicator 2007 R2 or Lync 2010 Attendant. These configuration options have been removed from the Lync Server 2013 Control Panel, but you configure them by using the Set-CsWebServiceConfiguration cmdlet.

Meeting Join Page Set-CsWebServiceConfiguration Parameters

Set-CsWebServiceConfiguration Parameter	Description
ShowJoinUsingLegacyClientLink	If set to True, users joining a meeting by using a client application other than Lync will be given the opportunity to join the meeting by using Office Communicator 2007 R2. The default value is False.
ShowAlternateJoinOptionsExpanded	When set to True then alternate options for joining an online conference (such as Office Communicator 2007 R2) will automatically be expanded and shown to users. When set to False (the default value) these options will be available, but the user will have to display the list of options for themselves.

To configure the meeting join page by using Lync Server 2013 Management Shell

1. Start the Lync Server 2013 Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. To view the web service configuration settings, run the following cmdlet:

   ```
   Get-CsWebServiceConfiguration
   ```

3. Run the following command, with the parameters set to True or False, depending on your preference (for details about the parameters for this cmdlet, see Set-CsWebServiceConfiguration in the Lync Server 2013 Management Shell documentation):

   ```
   Set-CsWebServiceConfiguration -Identity global -ShowJoinUsingLegacyCli
   ```

⊟See Also

Other Resources

Set-CsWebServiceConfiguration

1.4.5 Deploying Monitoring

Deploying Monitoring

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-08-21*

Major changes have been made to the Microsoft Lync Server 2013 monitoring infrastructure, beginning with the fact that the Monitoring Server role has been deprecated. Instead of separate Monitoring Server roles (which typically required organizations to set up dedicated computers to act as Monitoring servers) monitoring services are now collocated on each Front End server. Among other things, this change helps to:

- Decrease the number of server roles required when implementing Lync Server 2013. In this case, decrementing the Monitoring Server server role also helps to reduce costs by eliminating the need to maintain dedicated servers for monitoring.
- Reduce the complexity of Lync Server setup and administration. By automatically collocating the monitoring services on each Front End server you no longer have to install, configure, and manage the Monitoring Server role.

Note:

The Archiving Server role has also been deprecated in Lync Server 2013. Like the monitoring services, Lync Server 2013 archiving services are now collocated on each Front End server. This is important to note simply because monitoring and archiving often share the same SQL Server database instance.

As you might expect, these changes have a major impact on how monitoring services are installed and managed. For example, because the Monitoring Server role no longer exists, the Monitoring Server node has been removed from the Lync Server Topology Builder; in turn, that means you no longer use Topology Builder's New Monitoring Server Wizard in order to add a new Monitoring Server to your topology. (That wizard no longer exists.) Instead, you will typically implement monitoring services within your topology by completing the following two steps:

1. Enabling monitoring at the same time you set up a new Lync Server pool. (In Lync Server 2013, monitoring is enabled or disabled on a pool-by-pool basis.) Note that you can enable monitoring for a pool without actually collecting monitoring data, a process explained in the Configuring Call Detail Recording and Quality of Experience Settings section of this documentation.
2. Associating a monitoring store (that is, a monitoring database) with the new pool. Note that a single monitoring store can be associated with multiple pools. Depending on the number of users homed on your Registrar pools, that means that you do not have to set up a separate monitoring database for each of your pools. Instead, single monitoring store can be used by multiple pools.

Although it's often easier to enable monitoring at the same time that you create a new pool, it's also possible to create a new pool with monitoring disabled. If you do that, you can later use Topology Builder to enable the service: Topology Builder provides a way to enable or disable monitoring for a pool, or to associate a pool with a different monitoring store. Keep in mind that even though there is no longer a Monitoring Server role you will still need to create one or more monitoring stores: backend databases used to store the data gathered by the monitoring service. These backend databases can be created using either Microsoft SQL Server 2008 R2 or Microsoft SQL Server 2012.

Note:

If monitoring has been enabled for a pool you can disable the process of collecting monitoring data without having to change your topology: Lync Server Management Shell provides a way for you to disable (and then later re-enable) call detail recording (CDR) or Quality of Experience (QoE) data collection. For more information, see the Configuring Call Detail Recording and Quality of Experience Settings section of this document.

One other important enhancement to monitoring in Lync Server 2013 is the fact that Lync Server Monitoring Reports now support IPv6: reports that use the IP Address field will display either IPv4 or IPv6 addresses depending on : 1) the SQL query being used; and, 2) where or not the IPv6 address is stored in the monitoring database.

This documentation walks you through the process of installing and configuring monitoring and Monitoring Reports for Lync Server 2013. The documentation provides step-by-step instructions that will help you to:

- Enable monitoring in your topology and associate a monitoring store with a Front End pool.
- Install SQL Server Reporting Services and the Lync Server Monitoring Reports. Monitoring Reports are preconfigured reports that provide different views into the information stored in a monitoring database.
- Configure call detail recording (CDR) and Quality of Experience (QoE) data collection. Call detail recording provides a way for you to track usage of Lync Server capabilities such as Voice over IP (VoIP) phone calls; instant messaging (IM); file transfers; audio/video (A/V) conferencing; and application sharing sessions. QoE metrics track the quality of audio and video calls made in your organization, including such things as the number of network packets lost, background noise, and the amount of "jitter" (differences in packet delay).
- Manually purge CDR and/or QoE records from the monitoring database.

1.4.5.1 Associating a Monitoring Store with a Front End Pool

Associating a Monitoring Store with a Front End Pool

Microsoft Lync Server 2013 > Deployment > Deploying Monitoring >

Topic Last Modified: *2012-06-19*

In Microsoft Lync Server 2013 monitoring data can only be collected on Front End pools that have been associated with a monitoring store, a task typically carried out you define a Front End pool in Topology Builder. To associate a monitoring store with a new Front End pool, make sure that you select the option **Monitoring (call detail recording and logging of quality of experience metrics)** on the **Select Features** page of the Define New Front End Pool wizard. Note that, if you select this option, you must also specify a SQL store in order to complete the wizard; however, this store does not have to exist at the time you run the wizard. That means that you can first associate a pool with a monitoring store, then later setup and configure that store.

Alternatively, you can associate an existing Front End pool with a new or different monitoring store by completing the following procedure:

1. Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013 (Preview)**, and then click **Lync Server Topology Builder**.
2. In the **Topology Builder** dialog box, select **Download Topology from existing deployment** and then click **OK**.
3. In the **Save As** dialog box, enter a file name for your current topology and then click **Save**. The saved topology can later be retrieved and re-published in case there are problems with the new topology.
4. In Topology Builder, expand **Lync Server 2013 (Preview)**, expand the name of the site containing the Front End pool, then click expand **Enterprise Edition Front End pools**.
5. Right-click the name of the pool to be associated with the monitoring store

and then click **Edit Properties**.

6. In the **Edit Properties** dialog box, on the **General** tab, select the option **Monitoring (CDR and QoE metrics)** and then select an existing SQL Server database from the **Monitoring SQL Server store** dropdown list. (Or, click **New** to associate the pool with a new database store.) If you choose to use a new database store then, in the **Define New SQL Store** dialog box, enter the fully qualified domain name of the SQL Server computer in the **Sql Server FQDN** box. If you want to use the default SQL Server instance for that store select **Default Instance**; otherwise select **Named Instance** and enter the instance name in the **Named Instance** box.
   The **Edit Properties** dialog box also gives you the option of creating a SQL mirror for your monitoring database (a SQL mirror enables you to maintain two copies of your monitoring database, one copy stored on the monitoring store computer and the other on the SQL mirror computer). To enable mirroring, select T**his SQL instance is in mirroring relation** and enter the port number for the mirror server in the **Mirroring port number** box.
7. In the **Edit Properties** dialog box, click **OK**.

After associating the monitoring store with a Front End pool you must publish the new topology before the changes take effect. To publish your new topology, complete the following steps in Topology Builder:

1. Click **Action**, point to **Topology**, and then click **Publish**.
2. In the Publish Topology wizard, on the **Publish the topology** page, click **Next**.
3. On the **Publishing wizard complete** page, click **Finish**.

After the topology has been published you can then install the monitoring database on the computer that will host the monitoring store. The monitoring database can be installed by using the Lync Server Management Shell and Windows PowerShell. To install the database locally (that is, to install the database on the same computer where you are running the Lync Server Management Shell), start the Management Shell on the appropriate computer, then type in the following command and press ENTER:

```
Install-CsDatabase -LocalDatabases
```

When you run the preceding command, Install-CsDatabase will read the current Lync Server topology, determine which databases need to be installed on the local computer, and then automatically install and configure each of those databases.

To install the database on a remote computer (that is, a computer other than the computer where the Management Shell is running) you must include at least two parameters: the ConfiguredDatabases parameter and the SqlServerFqdn parameter. These parameters tell the Install-CsDatabase cmdlet to retrieve the Lync Server topology and then install and configure the required databases on the computer specified by the SqlServerFqdn parameter. The SqlServerFqdn parameter must use a parameter value representing the fully qualified domain name of the computer where the databases are to be installed.

For example, this command installs the monitoring database on the computer atl-sql-001.litwareinc.com:

```
Install-CsDatabase -ConfiguredDatabases -SqlServerFqdn atl-sql-001.litwareinc.com
```

Alternatively, you can install the monitoring database by running the Lync Server Deployment Wizard on the computer that will host the monitoring store. To do this, log on to the appropriate computer and complete the following procedure:

1. Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013 (Preview)**, and then click **Lync Server Deployment Wizard**.
2. In the Deployment Wizard, click **Install or Update Lync Server System**.
3. On the **Deploy** page, under **Step 2: Setup or Remove Lync Server Components**, click **Run Again**.
4. In the Setup Lync Server components wizard, on the **Setup Lync Server**

components page, click **Next**.

5. On the **Specify path to MSIs** page, type the path to the file Ocscore.msi (a file included with your Lync Server installation media) and then click **Next**.
6. On the **Executing Commands** page, click **Finish**.

To ensure that all the required Lync Server services have started, click **Run** under the heading **Step 4: Start Services** on the **Deploy** page

1.4.5.2 Installing SQL Server Reporting Services

Installing SQL Server Reporting Services

Microsoft Lync Server 2013 > Deployment > Deploying Monitoring >

Topic Last Modified: *2012-06-20*

If you intend to use Microsoft Lync Server 2013 Monitoring Reports (see the next section of this documentation for more information) you must first install SQL Server Reporting Services; Reporting Services can be installed at the same time you install Microsoft SQL Server or any time after SQL Server has been installed. If you have not installed SQL Server, then follow the instructions provided earlier in this documentation. When installing SQL Server, make sure that, on the Feature Selection page, you select Reporting Services. That will install SQL Server Reporting Services.

If you have already installed SQL Server but did not install SQL Server Reporting Services you can add that feature by following the appropriate set of instructions for SQL Server 2008 R2 or SQL Server 2012, as appropriate.

To verify that the reporting Services have been successfully installed, complete the following steps:

1. If you are running Microsoft SQL Server 2008 R2, then click **Start**, click **All Programs**, click **Microsoft SQL Server 2008 R2**, click **Configuration Tools**, and then click **Reporting Services Configuration Manager**.
   If you are running Microsoft SQL Server 2012, then click **Start**, click **All Programs**, click **Microsoft SQL Server 2012**, click **Configuration Tools**, and then click **Reporting Services Configuration Manager**.
2. In the **Reporting Services Configuration Connection** dialog box, verify that the name of your server appears in the **Server Name** box and that the name of the SQL Server instance that stores your monitoring data appears in the **Report Server Instance** box. Click **Connect**.

In the Reporting Service Configuration Manager, the Report Server Status pane should show that SQL Server Reporting Services has been installed and that the Reporting Services are currently running: the Report Server Status should be shown as **Started** and the **Start** button should be grayed-out and unavailable. If the Reporting Service is not running, click **Start** in order to start the service.

If no database is listed next to the Report Server Database Name label then do the following:

1. In the Reporting Services Configuration Manager click **Database**.
2. In the Report Server Database pane click **Change Database**.
3. In the Report Server Database Configuration wizard, in the Action pane, select **Create a new report server database** and then click **Next**.
4. In the Report Server Database Configuration wizard, in the Database Server pane, verify that the information listed in the **Server Name**, **Authentication Type**, and **Username** boxes is correct. Click **Test Connection** to verify that a connection can be made to the database server and then click **Next**.
5. In the Report Server Database Configuration wizard, in the Database pane,

accept the default values for **Database Name**, **Language**, and **Report Server Mode** and then click **Next**.

6. In the Report Server Database Configuration wizard, in the Credentials pane, verify that the correct information is listed in the **Authentication Type** dropdown list and the **User name** and **Password** boxes, and then click **Next**.
7. In the Report Server Database Configuration wizard, in the Summary pane, click **Next**.
8. In the Report Server Database Configuration wizard, in the Progress and Finish pane, click **Finish**.

To verify that the Reporting Service URLs have been configured, click **Web Service URL**. You should see one or more URLs listed under the heading **Report Server Web Service URLs**. Click each of these URLs to verify that you can reach the home page for the local installation of SQL Server Reporting Services.

1.4.5.3 Associating Monitoring Reports with a Mirror Database

Associating Monitoring Reports with a Mirror Database

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Monitoring >

Topic Last Modified: *2013-02-19*

If you configure a mirror for your monitoring database, that mirror database will take over as the primary database if a failover occurs. However, if you use Lync Server Monitoring Reports and a failover occurs, you might find that your Monitoring Reports are not connecting to the mirror database. This is because, when you install Monitoring Reports, you specify only the location of the primary database; you do not specify the location of the mirror database.

To get Monitoring Reports to automatically failover to the mirror database, you must add the mirror database as a "failover partner" to the two databases that are used by Monitoring Reports (one database for Call Detail Record data, and the other for Quality of Experience (QoE) data). You can add the failover partner information by manually editing the connection string values used by these two databases. To do that, complete the following procedure:

1. Use Internet Explorer to open the **SQL Server Reporting Services** home page. The Reporting Services home page URL includes:
   - The **http:** prefix.
   - The fully qualified domain name (FQDN) of the computer where the Reporting Services are installed (for example, **atl-sql-001.litwareinc.com**).
   - The character string **/Reports_**.
   - The name of the database instance where the Monitoring Reports are installed (for example, **archinst**).

   For example, if SQL Server Reporting Services was installed on the computer atl-sql-001.litwareinc.com and the Monitoring Reports use the database instance archinst, the home page URL would look like this:
   http://atl-sql-001.litwareinc.com/Reports_archinst
2. After you have accessed the Reporting Services home page, click **LyncServerReports**, and then click **Reports_Content**. That will take you to the **Reports_Content** page for the Lync Server Monitoring Reports.
3. On the **Reports_Content** page, click the **CDRDB** data source.
4. On the **CDRDB** page, on the **Properties** tab, look for the text box labeled **Connection string**. The current connection string will look similar to this:
   Data source=(local)\archinst;initial catalog=LcsCDR
5. Edit the connection string to include the server name and database instance for the mirror database. For example, if the server is named atl-mirror-001

and the mirror database is in the archinst instance, you will need to add to specify the mirror database using this syntax:
FailoverPartner=atl-mirror-001\archinst
Your edited connection string will look like this:
Data source=(local)\archinst;FailoverPartner=atl-mirror-001\archinst;initial catalog=LcsCDR

6. After updating the connection string, click **Apply**.
7. On the **CDRDB** page, click the **Reports_Content** link. Click the **QMSDB** data source, and then edit the connection string for the QoE database. For example:
Data source=(local)\archinst;FailoverPartner=atl-mirror-001\archinst;initial catalog=QoEMetrics
8. Click **Apply**.

Concepts

Installing Lync Server 2013 Monitoring Reports
Using Monitoring Reports

1.4.5.4 Installing Lync Server 2013 Monitoring Reports

Installing Lync Server 2013 Monitoring Reports

Microsoft Lync Server 2013 > Deployment > Deploying Monitoring >

Topic Last Modified: *2013-02-18*

Microsoft Lync Server 2013 Monitoring Reports provide you with a wealth of information about the quality and quantity of the communication sessions that take place in your organization. However, Monitoring Reports are not automatically installed when you install Lync Server 2013; instead, you must install Monitoring Reports separately, and only after Lync Server has been installed on the computer.

Note:

It is recommended that you install Monitoring Reports on the same computer where the monitoring database is installed. This simplifies the process of assigning permissions for accessing the reports: installing Monitoring Reports on the computer that hosts the monitoring store means that you will not have to configure permissions that allow a database on one computer to interact with Reporting Services running on a second computer.

Lync Server Monitoring Reports include over 30 reports designed to provide detailed information about conferences, peer-to-peer IM sessions, user registrations, the Response Group application, and much more. For the 2013 version, Lync Server Monitoring Reports include a number of enhancements:

- **New voice quality reports**. These new reports include the Media Quality Comparison Report, which compares quality between different types of calls (for example, between wired calls and wireless calls); and the Conference Join Time Report, which provides information regarding the amount of time requires for users to join a conference.
- **Improved reports for analyzing and troubleshooting both video and application sharing sessions.** The Media Quality Summary Report provides a way to analyze video and application sharing calls, while the Server Performance Report details the performance of servers generating these calls. Video and application sharing metrics are also now reported by the Peer-to-Peer Session Detail Report and the Conference Detail Report.
- **Improved report performance**. This includes faster response and data retrieval time, as well as faster and easier navigation through the reports.

More information on the individual reports can be found in the Monitoring Reports documentation.

Note:
There is another new report – QoE Call Detail Subreport – included in Lync Server 2013. However, this report is primarily for internal use, and is not intended to be directly accessed.

There are two ways to install Lync Server Monitoring Reports: you can use the Lync Server Deployment Wizard or you can use a Windows PowerShell script included with the Lync Server 2013 installation files. Regardless of the method you use to install the reports you must first make sure that you:

- Have the right to add a database role to a user account in the monitoring database.
- Hold the Content Manager role in SQL Server Reporting Services. This role gives you the right to deploy reports to SQL Server Reporting Services.

To install the Monitoring Reports by using the Deployment Wizard, complete the following steps:

1. Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013 (Preview)**, and then click **Lync Server Deployment Wizard**.
2. In the Deployment Wizard, click **Deploy Monitoring Reports** in order to start the Deploy Monitoring Reports wizard.
3. In the Deploy Monitoring Reports wizard, on the **Specify Monitoring Database** page, make sure that the fully qualified domain name of the computer hosting your monitoring store appears in the **Monitoring database** dropdown list. (If you have multiple monitoring stores you will need to select the appropriate server from the dropdown list.) Verify that the correct SQL Server instance appears in the **SQL Server Reporting Services (SSRS) instance** box (for example, **atl-sql-001.litwareinc.com/archinst**) and then click **Next**.
4. On the **Specify Credentials** page, in the **User name** box, type the domain name and user name of the account to be used when accessing the Monitoring Reports (for example, **litwareinc\kenmyer**). If you do not use this format (domain\user name) an error will occur.
   Type the user account password in the **Password** box, and then click **Next**. Note that no special rights are required for this account. The account will automatically be granted the required logon and database permissions when setup completes.
5. On the **Specify Read-Only Group** page enter the name of a security group that will be granted read-only access to the SQL Server Reporting Services in the User group box. For example, to give read-only administrators access to the reports enter **RTCUniversalReadOnlyAdmins**. Click **Next**.
6. On the **Executing Commands** page, click **Finish**.

Monitoring Reports can also be installed from the Lync Server Management Shell by running the script DeployReports.ps1; this Windows PowerShell script can be found in the Lync Server installation folder ..\Setup\ReportingSetup. To install Monitoring Reports using DeployReports.ps1, type a command similar to the following at the Management Shell prompt:

```
C:\Scripts\DeployReports.ps1 -storedUserName "litwareinc\kenmyer" -storedPassword
```

The parameters used in the preceding command are described in the following table:

Parameter Name	Required	Description
storedUserName	Yes	User account (in the format domain\username) used to access the monitoring store; for example: `-storedUserName "litwareinc\kenmyer"`

		This account must have the previously-specified SQL Server and SQL Server Reporting Services permissions or the script will fail.
storedPassword	Yes	Password for the user account used to access the monitoring store.
readOnlyGroupName	No	Domain or local security group whose members will be granted read-only access to the Monitoring Reports. Note that the script will fail if the specified group does not exist. If you later decide to revoke these permissions, or if you decide to grant other users or other groups access permissions, you can do so using the SQL Service Reporting Services Report Manager.
reportSqlServerInstance	No	SQL Server instance that hosts the Reporting Service. The Reporting instance must be specified using the fully qualified domain name of the Report Server; for example: `-reportServerSqlInstance atl-sql-001.litwareinc.com` If this parameter is not included the script will assume that the reporting services are hosted by the same SQL Server instance that hosts the monitoring database.
monitoringDatabaseId	No	Service Identity for the monitoring database. You can return the Identities for your monitoring databases by running this command: `Get-CsService -MonitoringDatabase`

After the Monitoring Reports have been installed you must then use the Set-CsReportingConfiguration cmdlet to configure the URL used to access these reports. This task can be carried out from the Lync Server Management Shell by running the following Windows PowerShell command. Note that it is recommended, but not required, that you use the HTTPS protocol when configuring the reporting URL:

```
Set-CsReportingConfiguration -Identity "MonitoringDatabase:atl-sql-001.litwareinc
```

In the preceding command, the ReportingUrl property should be set to the Report Manager URL used by SQL Server 2008 R2 Reporting Services. You can determine the Report Manager URL by completing the following steps on the computer where SQL Server Reporting Services has been installed:

1. Click Start, click All Programs, click Microsoft SQL Server 2008 R2, click Configuration Tools, and then click Reporting Services Configuration Manager.
2. In the Reporting Services Configuration Connection dialog box, make sure that the name of the Reporting Services computer appears in the Server Name box. Select the SQL Server instance from the Report Server Instance dropdown list and then click Connect.
3. In Reporting Services Configuration Manager, click Report Manager URL. One or more URLs should appear in the Report Manager URL pane. Any of these URLs can be used as the Reporting URL although, again, it is recommended that the ReportingUrl use the HTTPS protocol.

If you have set up a mirror database for your monitoring database then you must also associate the Monitoring Reports with the mirror database. See the article Associating Monitoring Reports with a Mirror Database for details.

1.4.5.5 Configuring Call Detail Recording and Quality of Experience Settings

Configuring Call Detail Recording and Quality of Experience Settings

Microsoft Lync Server 2013 > Deployment > Deploying Monitoring >

Topic Last Modified: *2012-10-17*

After you have associated a monitoring store with a Front End pool, set up the monitoring store, and then installed and configured SQL Server Reporting Services and Monitoring Reports you can manage Call Detail Recording (CDR) and Quality of Experience (QoE) monitoring by using Lync Server Management Shell. Lync Server Management Shell cmdlets allow you to enable and disable CDR and/or QoE monitoring for a particular site or for your entire Lync Server deployment; that can be done with a command as simple as this:

```
Set-CsQoEConfiguration -Identity "global" -EnableQoE $False
```

When you install Microsoft Lync Server 2013, you will also install a predefined collection of global configuration settings for both CDR and QoE. Default values for some of the more commonly-used settings used by Call Detail Recording are shown in the following table:

Property	Description	Default Value
EnableCDR	Indicates whether or not CDR is enabled. If True, all CDR records will be collected and written to the monitoring database.	True
EnablePurging	Indicates whether or not CDR records will periodically be deleted from the database. If True, records will be deleted after the time period specified by the properties KeepCallDetailForDays (for CDR records) and KeepErrorReportForDays (for CDR errors). If False, CDR records will be maintained indefinitely.	True
KeepCallDetailForDays	Indicates the number of days that CDR records will be kept in the database; any records older than the specified number of days will automatically be deleted. However, this will occur only if purging has been enabled. KeepCallDetailForDays can be set to any integer value between 1 and 2562 days (approximately 7 years).	60 days
KeepErrorReportForDays	Indicates the number of days that CDR error reports are kept; any reports older than	60 days

	the specified number of days will automatically be deleted. CDR error reports are diagnostic reports uploaded by client applications such as Microsoft Lync 2013. You can set this property to any integer value between 1 and 2562 days.	

Similarly, default values for selected QoE settings are shown in this table:

Property	**Description**	**Default Value**
EnableQoE	Indicates whether or not QoE monitoring is enabled. If True, all QoE records will be collected and written to the monitoring database.	True
EnablePurging	Indicates whether or not QoE records will periodically be deleted from the database. If True, records will be deleted after the time period specified by the KeepQoEDataForDays property. If False, QoE records will be maintained indefinitely.	True
KeepQoEDataForDays	Indicates the number of days that QoE records will be kept in the database; any records older than the specified number of days will automatically be deleted. However, this will occur only if purging has been enabled. KeepCallDetailForDays can be set to any integer value between 1 and 2562 days.	60 days

If you need to modify these global settings you can do so by using the Set-CsCdrConfiguration and the Set-CsQoEConfiguration cmdlets. For example, this command (run from within the Lync Server Management Shell) disables CDR monitoring at the global scope; that's done by setting the EnableCDR property to False ($False):

```
Set-CsCdrConfiguration -Identity "global" -EnableCDR $False
```

Note that disabling monitoring does not dissociate the monitoring store from the Front End pool, nor does it uninstall or otherwise affect the backend monitoring database. When you use Lync Server Management Shell to disable either CDR or QoE monitoring all you really do is temporarily stop Lync Server from collecting and archiving monitoring data. If you want to resume, in this case, the collection and archiving of CDR data, all you need to do is set the EnableCDR property back to True ($True):

```
Set-CsCdrConfiguration -Identity "global" -EnableCDR $True
```

Similarly, this command disables the purging of QoE records at the global scope:

```
Set-CsQoEConfiguration -Identity "global" -EnablePurging $False
```

In addition to the global settings, CDR and QoE configurations settings can be assigned to the site scope. This provides additional management flexibility when it comes to monitoring; for example, an administrator can enable CDR monitoring for the Redmond site but disable CDR monitoring for the Dublin site. To create new CDR configuration settings at the site scope, use a command similar to this:

```
New-CsCdrConfiguration -Identity "site:Redmond" -EnableCDR $False
```

Keep in mind that settings configured at the site scope take precedence over settings configured at the global scope. For example, suppose CDR monitoring is enabled at the global scope, but disabled at the site scope (for the Redmond site). That means that call detail recording information will not be archived for users in the Redmond site. However, users in other sites (that is, users managed by the global settings instead of the Redmond site settings) will have their call detail recording information archived.

New QoE configuration settings can be created at the site scope by using a command like this one:

```
New-CsQoEConfiguration -Identity "site:Redmond" -KeepQoEDataForDays 15
```

For more information, type the following commands from within the Lync Server Management Shell:

```
Get-Help New-CsCdrConfiguration | more
Get-Help Set-CsCdrConfiguration | more
Get-Help New-CsQoEConfiguration | more

Get-Help Set-CsQoEConfiguration | more
```

1.4.5.6 Manually Purging the Call Detail Recording and Quality of Experience Databases

Manually Purging the Call Detail Recording and Quality of Experience Databases

Microsoft Lync Server 2013 > Deployment > Deploying Monitoring >

Topic Last Modified: *2012-11-01*

Administrators can configure the Call Detail Recording (CDR) and/or the Quality of Experience (QoE) databases to automatically purge old records from the database; this occurs if purging has been enabled for the specified database (CDR or QoE) and if there are any records that have been in the database longer than the specified amount of time. For example, every day at 1:00 AM administrators might configure the system so that QoE records more than 60 days old will be deleted from the QoE database.

In addition to that automatic purging, two new cmdlets -- Invoke-CsCdrDatabasePurge and Invoke-CsQoEDatbasePurge -- have been added to Microsoft Lync Server 2013; these cmdlets allow administrators to manually purge records from the CDR and the QoE databases at any time. For example, to manually purge all the records more than 10 days old from the CDR database you can use a command similar to this:

```
Invoke-CsCdrDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

In the preceding command both call detail records and diagnostic data records older than 10 days are deleted from the monitoring database on atl-sql-001.litwareinc.com. (Call detail records are user/session reports. Diagnostic data records are diagnostic logs uploaded by client applications such as Lync 2013.)

As shown above, when you run the Invoke-CsCdrDatabasePurge cmdlet you must include both the PurgeCallDetaiDataOlderThanDays and the PurgeDiagnosticDataOlderThanDays parameters. However, these parameters do not have to be set to the same value. For example, it's possible to purge call detail records more than 10 days old and yet, at the same time, leave all the diagnostic data records in the database. To do that, set PurgeCallDetailDataOlderThanDays to 10 and PurgeDiagnosticDataOlderThanDays to 0. For example:

```
Invoke-CsCdrDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

By default, any time you run Invoke-CsCdrDatabasePurge you will see a prompt similar to this one for each database table that must be purged:

```
Confirm
Are you sure you want to perform this action?
Performing operation "Stored procedure: RtcCleanupDiag" on Target "Target SQL Ser
[Y] Yes  [A] Yes to All  [N] No  [L] No to All [S] Suspend  [?] Help (default is
```

You must type either Y (for Yes) or A (for Yes to All) before the database purging will actually take place. If you would prefer to suppress these confirmation prompts, add the following parameter to the end of your call to Invoke-CsCdrDatabasePurge:

```
-Confirm:$False
```

For example:

```
Invoke-CsCdrDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

If you do that, confirmation prompts will not be displayed, and database purging will immediately be performed.

To purge the QoE database, use the Invoke-CsQoEDatabasePurge cmdlet and specify the age (in days) of the records to be deleted:

```
Invoke-CsQoEDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

1.4.6 Deploying Archiving

Deploying Archiving

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-09-28*

Lync Server 2013 provides a solution for archiving instant messaging (IM) content and conferencing communications in Lync Server. You can implement archiving support by integrating archiving storage with Exchange 2013 storage, by using SQL Server databases for storage of Lync Server 2013 archiving data, or by using both Lync Server 2013 and Exchange 2013 storage. You control how data is archived using policies and archiving configurations. For details, see Planning for Archiving in the Planning documentation and How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

You can use the information in this section to set up and configure Archiving initially. After deployment, you can change Archiving settings. For details about how you implement archiving support for day-to-day management or to meet new requirements in your organization, see Managing Lync Server 2013 Archiving in the Operations documentation.

- How Archiving Works

- Deployment Checklist for Archiving
- Setting Up Systems and the Infrastructure for Archiving
- Adding Archiving Databases to an Existing Lync Server 2013 Deployment
- Configuring Support for Archiving

1.4.6.1 How Archiving Works

How Archiving Works

Microsoft Lync Server 2013 > Planning > Planning for Archiving >

Topic Last Modified: *2013-01-22*

Lync Server 2013 Archiving provides options to help you meet your compliance needs. To implement and maintain it in a way that most effectively meets your organization's requirements, you should understand:

- What information can be archived.
- How to enable and disable Archiving in your deployment.
- The archiving options that you can configure to control how Archiving is implemented.

What Information Can Be Archived?

The following types of content can be archived:

- Peer-to-peer instant messages
- Conferences (meetings), which are multiparty instant messages
- Conference content, including uploaded content (for example, handouts) and event-related content (for example, joining, leaving, uploading sharing, and changes in visibility)
- Whiteboards and polls shared during a conference

The following types of content are not archived:

- Peer-to-peer file transfers
- Audio/video for peer-to-peer instant messages and conferences
- Desktop and application sharing for peer-to-peer instant messages and conferences

Lync Server also does not archive Persistent Chat conversations. To archive Persistent Chat conversations, you must enable and configure the compliance service, which is a component that can be deployed with Microsoft Lync Server 2013, Persistent Chat Server. For details, see Planning for Persistent Chat Server in the Planning documentation.

How Do I Start Using Archiving?

Archiving is automatically installed on each Front End Server when you deploy the server, but Archiving is not enabled until you configure it. How you configure it is determined by how you deploy Archiving:

- **Archiving using Microsoft Exchange integration.** If you have users who are homed on Exchange 2013 and their mailboxes have been put on In-Place Hold, you can select the option to integrate Lync Server 2013 storage with Exchange storage. If you choose the Microsoft Exchange integration option, you use Exchange 2013 policies and configurations to control the archiving of Lync Server 2013 data for those users.
- **Archiving using Lync Server Archiving databases.** If you have users who are not homed on Exchange 2013 or who have not had their mailboxes put on In-Place Hold, or if you don't want to use Microsoft Exchange integration for any or all users in your deployment, you can deploy Lync Server Archiving

databases using SQL Server to store Archiving data for those users. In this case, Lync Server 2013 Archiving policies and configurations determine whether Archiving is enabled and how it is implemented. To use Lync Server 2013, you must add the appropriate SQL Server databases to your topology and publish the topology.

Archiving Setup When Using Microsoft Exchange Integration

If your users are homed on Exchange 2013 and their mailboxes have been put on In-Place Hold, you can choose the **Microsoft Exchange integration** option (as described later in this section) to archive Lync Server 2013 for those users, and then you control archiving for those users by specifying Exchange In-Place Hold policies and settings, as well as Lync Server configurations to control the following:

- Whether to archive IM, conferencing, or both.
- Whether to implement critical mode for your Lync Server deployment.
- Selection of the Microsoft Exchange integration option to use Exchange 2013 for storage of archived data.

These Lync Server 2013 Archiving configuration options are described later in this section. For information about how to configure Exchange In-Place Hold policies and settings to support archiving, see the Exchange 2013 product documentation.

Archiving Setup When Using Lync Server Archiving Database Storage

If you want to use Lync Server Archiving databases (using SQL Server databases) to archive data for any users in your deployment, you can configure Lync Server Archiving policies to control whether Archiving is enabled for those users. In each Archiving policy, you can enable or disable Archiving for either or both of the following:

- Internal communications
- External communications

By default, archiving is not enabled for internal communications or external communications in any Lync Server Archiving policy. You enable and disable communications using Lync Server 2013 Control Panel or using cmdlets in the Lync Server 2013 Management Shell.

Lync Server 2013 Archiving policies include the following:

- **Global Archiving policy**. This is the default Archiving policy and applies to your entire deployment. It is created when you deploy Lync Server 2013 and, by default, disables Archiving for both internal and external communications. You cannot delete this policy. If you choose the delete option, the global policy is reset to the default settings.
- **Site Archiving policy**. Optionally, you can enable or disable Archiving for one or more specific sites by creating and configuring a site-level Archiving policy for the site. When you create a site-level Archiving policy, by default, archiving is not enabled. You can delete any site-level Archiving policy that you create. A site-level Archiving policy overrides the global policy, but only for the site specified in the policy. For example, if you enable Archiving for internal and external communications in your global policy and create a site policy in which you disable Archiving for external communications, only internal communications would be archived for that site.
- **User Archiving policy**. Optionally, you can enable or disable Archiving for one or more specific users and group of users by creating, configuring, and applying a user-level Archiving policy for the specified users and user groups. When you create a user-level Archiving policy, by default, archiving is not enabled. You can delete any user-level Archiving policy that you create, and you can change which users and group of users the Archiving policy applies to. A user-level Archiving policy overrides the global policy and any site policies, but only for the users and user groups to whom the policy is applied. For example, if you disable Archiving for internal and external communications in

your global policy, create a site-level policy in which you enable Archiving for internal and external communications, and then create a user-level policy in which you disable Archiving for external communications, the communications would be archived for both external and internal communications for all site users except that, for the users to whom you apply the user-level policy, only internal communications would be archived.

For details about how to set up initial Archiving policies when you deploy Archiving, see Configuring and Assigning Archiving Policies in the Deployment documentation. For details about using Archiving policies to enable and disable communications after deployment, see Managing the Archiving of Internal and External Communications in the Operations documentation.

Note:

If you implement both Lync Server 2013 Archiving databases and enable Microsoft Exchange integration, Exchange 2013 policies override Lync Server Archiving policies, but only for users who are homed on Exchange 2013 and have had had their mailboxes put on In-Place Hold. Lync Archiving depends on Microsoft Exchange In-Place Hold policy only.

What Options Do I Have for Configuring Archiving?

In addition to using policies and to enable and disable Archiving, you have other Archiving options that can be configure for your entire deployment and, optionally, for specific sites and pools. You control most Archiving options by using one or more Archiving configurations, which are available in Lync Server 2013 Control Panel, but also have another option that is only available for configuration using Lync Server 2013 Management Shell.

Archiving Configuration Options Available in Lync Server 2013 Control Panel

Each archiving configuration provides the following options:

The global-level configuration is created automatically when you deploy archiving and can be configured, but not deleted. If you select the option to delete the global configuration, the settings are reset to the default values. You can create multiple site and pool configurations that, together with the global configuration, control archiving settings. For the global configuration and each site and pool configuration, you have the following options:

- Disable archiving, enable archiving only for instant messaging (IM), or enable archiving of both IM and conferencing.
- Configure critical mode to block IM and conferencing sessions in the event of a Lync Server failure. Failures include the following:
  - **IM**. A problem with the Lync Server storage service. In this case, IM is blocked for users who are enabled for Archiving.
  - **Conferencing**. A failure could be an unavailable file share or a problem with the storage service. In this case, all active conferences hosted in the pool at the time of failure are switched to restricted mode and new conferences cannot be activated.

  Both IM and conferencing automatically recover after the failures are corrected.
- Specify the use of Microsoft Exchange Server 2013 integration to use Exchange 2013 for storage of archived data, instead of setting up separate SQL Server databases for storage of Lync Server 2013 archiving data.
- Configure purging options for archived data. This includes specifying when to purge archived data, which can be either of the following:
  - After a specific number of days that you specify
  - After the archiving data has been exported (which includes data that has been uploaded to Exchange, if you enable Microsoft Exchange integration).

  Note:

  If you enable Microsoft Exchange integration, purging for users homed on Exchange 2013 and with their mailboxes put on In-Place Hold is controlled by Exchange. The only qualification is for conferencing files, which are stored on

> the Lync Server file share. These files are purged from the file share only after the files have been exported (uploaded to Exchange), if you select the option to purge data after the archiving data has been exported, or after the specified maximum number of days, if you specify a maximum number of days for retention.

By default, no archiving options are enabled. You can manage Archiving configurations using Lync Server 2013 Control Panel.

You can specify the following Archiving configurations:

- **Global Archiving configuration**. This is the default Archiving configuration and applies to your entire deployment. It is created when you deploy Lync Server 2013 and, by default, does not enable archiving functionality. You can modify the global configuration, but you cannot delete it. If you choose the delete option for the configuration, the global configuration is reset to the default settings.
- **Site Archiving configuration**. Optionally, you can configure Archiving for one or more specific sites by creating and configuring a site-level Archiving configuration for an individual site. A site-level Archiving configuration exists only if you create it. You can modify or delete any site-level Archiving configuration. A site-level Archiving configuration overrides the global configuration, but only for the site specified in the site-level configuration. For example, if you enable Archiving for only IM in your global configuration and create a site configuration in which you enable Archiving for both IM and conferencing, conferencing would only be archived for the site, not for the remainder of your organization.
- **Pool Archiving configuration**. Optionally, you can specify Archiving settings for one or more specific pools by creating and configuring a pool-level configuration for the individual pool. A pool-level Archiving configuration exists only if you create it. You can modify and delete any pool-level Archiving configuration. A pool-level Archiving configuration overrides the global configuration and any site archiving configuration you may have created. For example, if you enable Archiving for only IM in your global configuration, create a site-level configuration in which you enable Archiving for both IM and conferencing for the site, and then create a pool-level configuration in which you enable Archiving only for IM, the communications would be archived for both IM and conferencing for all users of the site except the users homed in the pool specified in the pool-level configuration. For all other users in your organization, Archiving would be enabled only for IM.

For details about how to set up initial Archiving configurations when you deploy Archiving, see Configuring Archiving Options in the Deployment documentation. For details about using Archiving policies to enable and disable communications after deployment, see Managing Archiving Configuration Options for Your Organization, Sites, and Pools in the Operations documentation.

Archiving Options Available Only in Windows PowerShell

Using Lync Server 2013 Management Shell, you can use cmdlets to implement options that are not available in Lync Server 2013 Control Panel. These options include the following:

- **Archive duplicate messages**. For details, see New-CsArchivingConfiguration and Set-CsArchivingConfiguration in the Operations documentation.
- **Export archived data**. For details, see Export-CsArchivingData

How Do I Access Archived Data?

Access to archived data is dependent on where the data is stored:

- **Microsoft Exchange storage**. If you choose the SharePoint integration option, Lync Server deposits the archiving content in the Exchange 2013 store for all users who are homed on Exchange 2013, and who have had their mailboxes put on In-Place Hold. Archived data is stored in user mailboxes Recoverable items folder, which is generally invisible to users, and can only be searched by users with an Exchange **Discovery Management** role. Exchange enables federated search and discovery, along with SharePoint, if it is deployed. For more details about storage, retention, and discovery of data stored in Exchange, see the Exchange 2013 and SharePoint documentation.

- **Lync Server storage**. If you set up Lync Server 2013 Archiving databases for storage of Lync Server data, Lync Server deposits archiving content in the Lync Server Archiving databases (SQL Server databases) for any users not homed on Exchange 2013, and who have not had their mailboxes put on In-Place Hold. This data is not searchable, but it can be exported to formats that are searchable using other tools. For details about exporting data stored in Archiving databases, see Exporting Archived Data in the Operations documentation.

For more details about how Lync Server 2013 and Exchange 2013 work together, see Exchange Server and SharePoint Integration Support in the Supportability documentation.

1.4.6.2 Deployment Checklist for Archiving

Deployment Checklist for Archiving

Microsoft Lync Server 2013 > Planning > Planning for Archiving >

Topic Last Modified: *2012-10-18*

Archiving is automatically installed on each Front End Server in your Lync Server 2013 deployment, but you still need to set it up before you can use it. The steps required to set it up, as summarized in this section, constitute the deployment of Archiving.

Deployment Sequence

How you set up Archiving depends on which storage option you choose:

- If you use Microsoft Exchange integration for all users in your deployment, you don’t need to configure Lync Server 2013 Archiving policies for your users. Instead, configure your Exchange In-Place Hold policies to support archiving for users homed on Exchange 2013, with their mailboxes put on In-Place Hold. For details about configuring these policies, see the Exchange 2013 product documentation.
- If you do not use Microsoft Exchange integration for all users in your deployment, you need to add Lync Server Archiving databases (SQL Server databases) to your topology and then publish it, as well as configure policies and settings for your users, before you can archive data for those users. You can deploy Archiving databases at the same time that you deploy your initial topology or after you have deployed at least one Front End pool or Standard Edition server. This document describes how to deploy Archiving databases by adding them to an existing deployment.

If you enable archiving in one Front End pool or Standard Edition server, you should enable it for all other Front End pools and Standard Edition servers in your deployment. This is because users whose communications are required to be archived can be invited to a group IM conversation or meetings hosted on a different pool. If archiving is not enabled on the pool where the conversation or meeting is hosted, the complete session may not be archived. In these cases, IMs with archiving-enabled users still can be archived, but not for conferencing content files, and conference join or leave events.

Important:

If archiving is critical in your organization for compliance reasons, be sure to deploy Archiving, configure policies and other options at the appropriate level, and enable it for all appropriate users, before you enable those users for Lync Server 2013.

Archiving Deployment Process

The following table provides an overview of the steps required to deploy archiving in an existing topology.

Phase	Steps	Roles and group memberships	Documentation
Install prerequisite hardware and software	• To use Microsoft Exchange integration (using Exchange 2013 for archiving storage for some or all users), you need an existing Exchange 2013 deployment. • To use separate Archiving databases (using SQL Server databases) for archiving storage for some or all users, SQL Server on the server that will store archiving data. **Note:** Archiving runs on Front End Servers of an Enterprise pool and Standard Edition servers. It has no additional hardware or software requirements beyond what is required to install those servers.	Domain user who is a member of the local administrators group.	Supported Hardware in the Supportability documentation. Server Software and Infrastructure Support in the Supportability documentation. Technical Requirements for Archiving in the Planning documentation. Setting Up Systems and the Infrastructure for Archiving in the Deployment documentation. Exchange Server and SharePoint Integration Support in the Supportability documentation.
Create the appropriate internal topology to support archiving (only if not using Microsoft Exchange integration for all users in your deployment)	Run Topology Builder to add Lync Server 2013 Archiving databases (SQL Server databases) to the topology, and then publish the topology.	To define a topology to incorporate Archiving databases, an account that is a member of the local users group. To publish the topology, an account that is a member of the domain admins group and RTCUniversalServerAdmins group,	Adding Archiving Databases to an Existing Lync Server 2013 Deployment in the Deployment documentation.

		and that has full control permissions (read/write/modify) on the file share to be used for the Lync Server 2013 file store (so that Topology Builder can configure the required DACLs).	
Configure server-to-server authentication (only if using Microsoft Exchange integration)	Configure servers to enable authentication between Lync Server 2013 and Exchange 2013. We recommend running **Test-CsExchangeStorageConnectivity testuser_sipUri –Folder Dumpster** to validate Exchange Archiving storage connectivity before enabling archiving.	An account with the appropriate permissions for managing certificates on the servers.	Managing Server-to-Server Authentication (Oauth) and Partner Applications in the Deployment documentation or the Operations documentation.
Configure archiving policies and configurations	Configure archiving, including whether to use Microsoft Exchange integration, the global policy and any site and user policies (when not using Microsoft Exchange integration for all data storage), and specific archiving options, such as critical mode and data export and purging. If using Microsoft Exchange integration, configure Exchange In-Place Hold policies as appropriate.	RTCUniversalServerAdmins group (Windows PowerShell only) or assign users to the CSArchivingAdministrator or CSAdministrator role.	Configuring Support for Archiving in the Deployment documentation. Exchange product documentation (if using Microsoft Exchange integration).

Deploying Lync Server and Microsoft Exchange in Different Forests

If Microsoft Exchange Server is not deployed in the same forest as Lync Server, you must make sure that the following Exchange Active Directory attributes are synchronized to the forest where Lync Server is deployed:

1. msExchUserHoldPolicies
2. proxyAddresses

This is a multi-value attribute. When synchronizing this attribute, you need to merge the values, not replace them to ensure the existing values are not lost.

1.4.6.3 Setting Up Systems and the Infrastructure for Archiving

Setting Up Systems and the Infrastructure for Archiving

Microsoft Lync Server 2013 > Deployment > Deploying Archiving >

Topic Last Modified: *2012-06-23*

Before you deploy archiving, you need to deploy the appropriate hardware and software to support archiving and verify that your infrastructure supports your Archiving deployment.

- Setting Up System Platforms for Archiving
- Setting Up the Infrastructure for Archiving
- Setting Up Storage for Archiving
- Setting Up Permissions for Archiving

1.4.6.3.1 Setting Up System Platforms for Archiving

Setting Up System Platforms for Archiving

Deployment > Deploying Archiving > Setting Up Systems and the Infrastructure for Archiving >

Topic Last Modified: *2012-10-09*

Before starting the deployment of Archiving, you must install the required operating system and any other prerequisite software on hardware that meets system requirements:

- **Lync Server 2013 platform** Lync Server 2013 deployments do not have Archiving Servers. Instead, Unified Data Collection Agents run on Front End Servers and Standard Edition servers to capture data for archiving, so no separate system platform is required to host Archiving.
- **Data storage platform** In Lync Server 2013, you can store data by using either of the following:
  - **Microsoft Exchange integration** If you want to store Lync Server 2013 Archiving data by using your Exchange 2013 deployment, instead of or in addition to setting up a separate database for storage of Archiving data, your Exchange deployment must be running Exchange 2013. For details about setting up system platforms for Exchange 2013, see the Exchange product documentation.
  - **SQL Server** If you want to use a separate SQL Server database for storage of archiving data, instead of or in addition to using Microsoft Exchange integration, you must set up the system platform for the database prior to deployment of Archiving. The specific system platform requirements depend on whether you use Microsoft SQL Server 2008 R2 or Microsoft SQL Server 2012 for the Archiving database. For details about setting up system platforms for these databases, see the Microsoft SQL Server 2008 R2 and Microsoft SQL Server 2012 product documentation.
- **File server platform** Lync Server 2013 stores Lync Server archiving files in the same location that you specify for file storage when you set up your Front End Servers or Standard Edition servers. You cannot specify a separate location for archiving file storage, so no separate system platform is required for Archiving file storage. If you use Microsoft Exchange integration, Exchange 2013 the files for archived Lync communications are stored on Exchange 2013 servers for users homed on those Exchange servers.

1.4.6.3.2 Setting Up the Infrastructure for Archiving

Setting Up the Infrastructure for Archiving

Deployment > Deploying Archiving > Setting Up Systems and the Infrastructure for Archiving >

Topic Last Modified: *2012-10-01*

The infrastructure requirements for Archiving are the same as for your Lync Server deployment, except for storage. No additional infrastructure setup is required, except for setting up storage using Exchange 2013 storage, Archiving databases, or both. For details about infrastructure requirements for Lync Server 2013, see Determining Your Infrastructure Requirements in the Planning documentation and Preparing the Infrastructure and Systems in the Deployment documentation. For details about storage requirements for Archiving, see Technical Requirements for Archiving in the Planning documentation, Setting Up System Platforms for Archiving in the Deployment documentation, and Setting Up Storage for Archiving in the Deployment documentation.

1.4.6.3.3 Setting Up Storage for Archiving

Setting Up Storage for Archiving

Deployment > Deploying Archiving > Setting Up Systems and the Infrastructure for Archiving >

Topic Last Modified: *2012-10-01*

Archiving storage for Lync Server 2013 includes the following:

- **Data storage** Data storage is required to store IM content.
- **File storage** File storage is required to store conferencing (meeting) content data storage and file storage.

Setting Up Data Storage

Requirements for setting up data storage for Archiving in Lync Server 2013 depend on how you want to store archiving data:

- Integrate Lync Server 2013 Archiving with your Exchange deployment to store Archiving data using Exchange storage.
- Set up separate SQL Server database servers to store Archiving data.

Setting Up Exchange Storage for Archiving Data

Setting up Exchange for storage of Archiving data requires that your Exchange deployment is running Exchange 2013. Additionally, user mailboxes must be homed on the Exchange 2013 server and their mailboxes must be put on In-Place Hold. For details about configuring Exchange 2013, see the Exchange product documentation.

Setting Up SQL Server Database Servers for Storage of Archiving Data

Archiving in Lync Server 2013 requires the SQL Server database software to store the archived data, unless you integrate your deployment with Exchange.

For SQL Server archiving databases, you must install SQL Server on the computer that will host the Archiving database. You can use the same SQL instance that you use for the back-end database of a Front End pool. For best performance, you should deploy the Archiving database on a computer that is separate from the Central Management store. For details about collocating Lync Server 2013 components, see Supported Server Collocation in the Supportability documentation.

Each database server must be running a supported version of SQL Server. For details about the supported versions, see Technical Requirements for Archiving in the Planning documentation.

You must set up the SQL Server platforms prior to deploying and enabling Archiving. If the account to be used to publish the topology has the appropriate administrator rights and permissions, you can create the Archiving database (LcsLog) when you publish your topology. You can also create the database later, including as part of the installation procedure. For details about SQL Server, see the SQL Server TechCenter at http://go.microsoft.com/fwlink/p/?linkID=129045.

Setting Up File Storage

Archiving uses the Lync Server 2013 file share that you specified when you set up your Front End pool or Standard Edition server. You cannot change the file share used for Archiving. For details about supported file storage systems, see File Storage Support in the Supportability documentation.

1.4.6.3.4 Setting Up Permissions for Archiving

Setting Up Permissions for Archiving

Deployment > Deploying Archiving > Setting Up Systems and the Infrastructure for Archiving >

Topic Last Modified: *2012-10-01*

In Lync Server 2013, specific tasks still require that users who perform those tasks be members of one or more specific groups. However, you can also use role-based access control (RBAC) to grant privileges by assigning users to predefined Lync Server administrative roles.Before you deploy Archiving, be sure that the appropriate user rights and permissions are in place, and that any users who you want to assign to a specific RBAC role have been assigned to that role. For details about the user rights, permissions, and roles for deploying support for Archiving, see Deployment Checklist for Archiving, which is available in the Planning documentation and the Deployment documentation. For details about RBAC, see Planning for Role-Based Access Control in the Planning documentation.

1.4.6.4 Adding Archiving Databases to an Existing Lync Server 2013 Deployment

Adding Archiving Databases to an Existing Lync Server 2013 Deployment

Microsoft Lync Server 2013 > Deployment > Deploying Archiving >

Topic Last Modified: *2012-06-23*

After you set up the system platforms and infrastructure for Archiving, you must use Topology Builder to add Archiving to your topology, and then publish the topology.

- Adding Archiving Databases to the Lync Server 2013 Topology
- Publishing the Updated Topology to Add Archiving Databases

1.4.6.4.1 Adding Archiving Databases to the Lync Server 2013 Topology

Adding Archiving Databases to the Lync Server 2013 Topology

Deployment > Deploying Archiving > Adding Archiving Databases to an Existing Lync Server 2013 Deployment >

Topic Last Modified: *2012-10-10*

You must incorporate archiving into your topology before you can configure your deployment to support archiving. The information in this topic explains how to use Topology Builder to add archiving to your existing topology.

Note:

If you want to use Microsoft Exchange integration to store archiving data and files on Exchange 2013 servers for all your users in your deployment, do not specify **Archiving SQL Server store** or **Use SQL Server Store mirroring** information.

⊟To add Archiving database support to your topology

1. On a computer that is running Lync Server 2013, or on which the Lync Server administrative tools are installed, log on by using an account that is a member of the local Users group (or an account with equivalent user rights).

   Note:

   You can define a topology by using an account that is a member of the local Users group, but to publish a topology, which is required to add a server to the topology, you must use an account that is a member of the **Domain Admins** group and the **RTCUniversalServerAdmins** group, and that has full control permissions (that is, read, write, and modify) on the file share that you are using for the Lync Server 2013 file store (that is, so that Topology Builder can configure the required discretionary access control list (DACLs), or an account with equivalent rights.
2. Start Topology Builder.
3. In the console tree, navigate to the Front End pool in which you want to deploy Archiving, and then click the name of the Front End pool where you want to deploy Archiving.
4. In the **Action** menu, click **Edit Properties**.
5. In the **Edit Properties** dialog box, click **General**.
6. Scroll down to **Archiving**.
7. Select the **Archiving** check box.
8. Under **Archiving SQL Server store,** do one of the following:
   - To use an existing SQL Server store, in the drop-down list box, click the name of the SQL Server store that you want to use. If all of your users are homed on Microsoft Exchange Server 2013 or above, you can archive Lync communications for all your users in Exchange. In this case, you don’t need to configure SQL Server Archiving store.
   - To specify a new SQL Server store, click **New**, and then in the **Define New SQL Server Store** dialog box, do the following:
     - In **SQL Server FQDN**, specify the FQDN of the server on which you want to create the new SQL Server store.
     - Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named instance**, and then specify the instance you want to use.
     - If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
9. If you want to use SQL Server store mirroring, select **Enable SQL Server Store mirroring**, and then do the following:

- To use an existing SQL Server store for mirroring, in the **Archiving SQL Server store mirror** drop-down list box, click the name of the SQL Server store that you want to use for mirroring.
- To specify a new SQL Server store for mirroring, click **New**, and then in the **Define New SQL Server Store** dialog box, do one of the following:
  - In **SQL Server FQDN**, specify the FQDN of the SQL Server on which you want to create the new SQL Server store.
  - Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named Instance**, and then specify the instance you want to use.
  - If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
- If you enable SQL Server mirroring and want to include a SQL Server mirroring witness (a third, separate SQL Server instance that can detect the health of the primary SQL Server server and mirror instances), select the **Use SQL Server mirroring witness to enable automatic failover** check box, and then do one of the following:
  - In **SQL Server FQDN**, specify the FQDN of the server on which you want to create the new SQL Server mirroring witness.
  - Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named Instance**, and then specify the instance you want to use for the mirroring witness.
  - If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.

10.To save the configuration, click **OK**.

1.4.6.4.2 Publishing the Updated Topology to Add Archiving Databases

Publishing the Updated Topology to Add Archiving Databases

Deployment > Deploying Archiving > Adding Archiving Databases to an Existing Lync Server 2013 Deployment >

Topic Last Modified: *2012-10-01*

After updating your topology in Topology Builder, you must publish the topology to the Central Management store before you can configure and use Archiving. Read-only copies of the data are replicated to all servers in the topology to keep all servers in sync with topology and other configuration changes.

⊟To publish your updated topology

1. On a computer that is running Lync Server 2013, or on which the Lync Server administrative tools are installed, log on using an account that is a member of the local Users group (or an account with equivalent user rights).

Note:

You can define a topology by using an account that is a member of the local Users group, but to publish a topology, which is required to add a server to the topology, you must use an account that is a member of the **Domain Admins** group and the **RTCUniversalServerAdmins** group, and that has full control permissions (that is, read, write, and modify) on the file share that you are using for the Lync Server 2013 file store (that is, so that Topology Builder can configure the required discretionary access control list (DACLs), or an account with equivalent rights.

2. Open the topology you created in the previous section using Topology Builder.
3. In the console tree, right-click **Lync Server 2013**, and then click **Publish Topology**.
4. On the **Publish the topology** page, click **Next**.
5. On the **Create databases** page, verify that the database is selected, and then click **Next**.

Note:

If you do not have the appropriate permissions to create databases, you can cancel the selection of the database and someone with appropriate permissions can create the database. For details about the required administrator rights and permissions, see Deployment Permissions for SQL Server in the Deployment documentation.

Only databases on dedicated SQL Server servers can be installed by using Topology Builder. Databases on SQL Server servers that are collocated with other server components must be installed by running local setup on that computer.

6. On the **Publishing wizard complete** page, verify that the topology was successfully published, and then click **Finish**.

Important:

After publishing the topology, you must configure options and policies for Archiving before any content can be archived. For details, see Configuring Support for Archiving in the Deployment documentation.

1.4.6.5 Configuring Support for Archiving

Configuring Support for Archiving

Microsoft Lync Server 2013 > Deployment > Deploying Archiving >

Topic Last Modified: *2012-10-01*

After adding Archiving to your topology and publishing the new topology, you need to configure options for how Archiving is initially implemented in your deployment, and then configure one or more Archiving policies to enable Archiving for your deployment and, optionally, for specific sites and users. You can use Lync Server 2013 Control Panel to do this.

Note:

After deployment, you can change Archiving settings to disable or enable Archiving. For details about how to implement archiving support for day-to-day management or to meet new requirements in your organization after deployment, see Managing Lync Server 2013 Archiving in the Operations documentation.

- Configuring Archiving Options
- Configuring and Assigning Archiving Policies
- Enable or Disable Sending an Archiving Disclaimer to Federated Partners

1.4.6.5.1 Configuring Archiving Options

Configuring Archiving Options

Deployment > Deploying Archiving > Configuring Support for Archiving >

Topic Last Modified: *2012-10-10*

In Lync Server 2013 Control Panel, you use Archiving configurations to specify how archiving is implemented. This includes the following Archiving configurations:

- A global configuration that is created by default when you deploy Lync Server 2013.
- Optional site-level and pool-level configurations that you can create and use to specify how archiving is implemented for specific sites or pools.

You initially set up Archiving configurations when you deploy Archiving, but you can change, add, and delete configurations after deployment. In Lync Server 2013 Control Panel, you can use the **Archiving Configuration** page of the **Archiving and Monitoring** group to manage configurations at the global level, site level, and pool level. For details about how Archiving configurations are implemented, including which options you can specify and the hierarchy of Archiving configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation. For details about how to manage configurations after deployment, see Managing Archiving Configuration Options for Your Organization, Sites, and Pools in the Operations documentation.

Note:

To use archiving, you must configure Archiving policies to specify whether to enable archiving for internal communications, for external communications, or for both for users homed on Lync Server 2013. By default, archiving is not enabled for either internal or external communications. Before enabling Archiving in any policies, you should specify the appropriate Archiving configurations for your deployment and, optionally, for specific sites and pools, as described in this section. For details about enabling Archiving, see Configuring and Assigning Archiving Policies in the Deployment documentation.
If you do not use Microsoft Exchange integration for all users in your deployment, you must configure Archiving policies to specify whether to enable archiving for internal communications, for external communications, or for both. By default, archiving is not enabled for either internal or external communications for archiving of data when using Lync Server 2013 Archiving databases. Prior to enabling Archiving in any policies, you should specify the appropriate Archiving configurations for your deployment and, optionally, for specific sites and pools, as described in this section. For details about enabling Archiving for use with Lync Server 2013 Archiving databases, see Configuring and Assigning Archiving Policies in the Deployment documentation.

- Configuring Archiving Options at the Global Level
- Configuring Archiving Options for a Site
- Configuring Archiving Options for a Pool

1.4.6.5.1.1 Configuring Archiving Options at the Global Level

Configuring Archiving Options at the Global Level

Deploying Archiving > Configuring Support for Archiving > Configuring Archiving Options >

Topic Last Modified: *2012-10-10*

When you add Archiving to your topology and publish the topology, Lync Server creates a global configuration for Archiving. By default, no Archiving options are enabled in the global configuration. The global configuration controls which options are enabled for your entire deployment, unless you set up site or pool configurations, which override the global configuration.

For details about how Archiving configurations work, including the hierarchy for global, site, and pool configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

You should specify all appropriate options in the Archiving configurations before enabling Archiving.

⊟To configure archiving options at the global level

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server 2013 Control Panel. For details about the different methods that you can use to start Lync Server 2013 Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. On the **Archiving Configuration** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Archiving Setting - Global**, in the **Archiving setting** drop-down list, select one of the following archiving options:
   - **Disable archiving**
   - **Archive IM sessions**
   - **Archive IM and web conferencing sessions**
6. Also on the **Edit Archiving Setting – Global** page, do the following:
   - To block activity when archiving is not available, select the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.
   - To use Microsoft Exchange Server to store archiving data, click the **Microsoft Exchange integration** check box.
   - To enable data purging, select the **Enable purging of archiving data** check box, and then do one of the following:
     - To specify purging after a specific number of days, click **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
     - To limit purging to archiving data that has been exported, click **Purge exported archiving data only**.
7. Click **Commit**.

1.4.6.5.1.2 Configuring Archiving Options for a Site

Configuring Archiving Options for a Site

Deploying Archiving > Configuring Support for Archiving > Configuring Archiving Options >

***Topic Last Modified:** 2012-10-09*

You can specify Archiving options to be applied to specific sites by creating and configuring options in an Archiving configuration for each of those sites. A site configuration overrides the global configuration, but only for the site specified in the site configuration. Pool configurations override site configurations

For details about how Archiving configurations work, including the hierarchy for global, site, and pool configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

You should specify all appropriate options in the Archiving configurations before enabling Archiving.

> **Important:**
>
> To enable archiving, you must specify archiving policies to control the archiving of internal and external communications at the global level and, if appropriate, at site and user levels. If you configure user-level policies, you must also assign the user policies to specific users. For details about creating and configuring archiving policies, see Managing the Archiving of Internal and External Communications in the Operations documentation.

To configure archiving options at the site level

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server 2013 Control Panel. For details about the different methods you can use to start Lync Server 2013 Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. On the **Archiving Configuration** page, click **New**, and then click **Site Configuration**.
5. In **Select a Site**, select the site to be configured for archiving.
6. In **New Archiving Setting**, in the **Archiving setting** drop-down list box, do one of the following:
    - To enable archiving only for instant messaging (IM) sessions, click **Archive IM sessions**.
    - To enable archiving for both IM sessions and conferences, click **Archive IM and web conferencing sessions**.
    - To disable archiving for the policy, click **Disable archiving**.
7. Also in **New Archiving Setting**, do the following:
    - To block activity when archiving is not available, select the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.
    - To use Microsoft Exchange Server to store archiving data, click the **Microsoft Exchange integration** check box.
    - To enable data purging, select the **Enable purging of archiving data** check box, and then do one of the following:
        - To specify purging after a specific number of days, click **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
        - To limit purging to archiving data that has been exported, click **Purge exported archiving data only**.
8. Click **Commit**.

1.4.6.5.1.3 Configuring Archiving Options for a Pool

Configuring Archiving Options for a Pool

Deploying Archiving > Configuring Support for Archiving > Configuring Archiving Options >

Topic Last Modified: *2012-10-10*

You can specify Archiving options to be applied to specific pools by creating and configuring options in an Archiving configuration for each of those pools. A pool configuration overrides the global configuration and site configuration, but only for the pool specified in the pool configuration.

For details about how Archiving configurations work, including the hierarchy for global, site, and pool configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

> **Note:**
>
> You should specify all appropriate options in the Archiving configurations before enabling Archiving. For details, see Configuring Archiving Options in the Deployment documentation.

⊟To configure archiving options at the pool level

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server 2013 Control Panel. For details about the different methods that you can use to start Lync Server 2013 Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. On the **Archiving Configuration** page, click **New**, and then click **Pool Configuration**.
5. In **Select a Service**, select the pool to be configured for archiving.
6. In **New Archiving Setting**, in the **Archiving setting** drop-down list, select one of the following archiving options:
   - **Disable archiving**
   - **Archive IM sessions**
   - **Archive IM and web conferencing sessions**
7. Also in **New Archiving Setting** page, do the following:
   - To block activity when archiving is not available, select the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.
   - To use Microsoft Exchange Server to store archiving data, click the **Microsoft Exchange integration** check box.
   - To enable data purging, select the **Enable purging of archiving data** check box, and then do one of the following:
     - To specify purging after a specific number of days, click **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
     - To limit purging to archiving data that has been exported, click **Purge exported archiving data only**.
8. Click **Commit**.

1.4.6.5.2 Configuring and Assigning Archiving Policies

Configuring and Assigning Archiving Policies

Deployment > Deploying Archiving > Configuring Support for Archiving >

Topic Last Modified: *2012-10-01*

In Lync Server 2013, you use policies to enable and disable archiving for internal communications and external communications for users who are homed on Lync Server 2013. This includes the following Archiving policies:

- A global policy that is created by default when you deploy Lync Server 2013.
- Optional site-level and user-level policies that you can create and use to specify how archiving is implemented for specific sites or users.

You initially set up Archiving policies when you deploy Archiving, but you can change, add, and delete policies after deployment. In Lync Server 2013 Control Panel, you can use the **Archiving Policy** page of the **Archiving and Monitoring** group to manage policies at the global level, site level, and user level.

Note:

To control the implementation of Archiving, you must specify options in Archiving configurations, such as whether to archive IM or conferencing, the use of critical mode, and purging options. By default no options are enabled in the global Archiving configuration or any site or pool Archiving configuration. You should specify all appropriate options in the Archiving configurations before enabling Archiving for internal or external communications in the Archiving policies. For details, see Managing Archiving Configuration Options for Your Organization, Sites, and Pools in the Operations documentation.

If you integrate your Lync Server storage with Exchange 2013 storage, the Exchange user policies take precedence over the Lync Server 2013 archiving policies but only for those users who are homed on Exchange 2013 who have had their mailboxes put on In-Place Hold.

For details about how policies are implemented, including the hierarchy of policies, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation. For details about how to manage policies after deployment, see Managing the Archiving of Internal and External Communications in the Operations documentation.

- Configuring the Global Policy for Archiving
- Setting Up Site Policies for Archiving
- Setting Up Archiving Policies for Users

1.4.6.5.2.1 Configuring the Global Policy for Archiving

Configuring the Global Policy for Archiving

Deploying Archiving > Configuring Support for Archiving > Configuring and Assigning Archiving Policies >

Topic Last Modified: *2012-10-09*

When you deploy your Front End Servers, Lync Server creates a global policy for Archiving. By default, Archiving is disabled in the global policy. The global policy controls whether archiving is enabled for internal and external communications for your entire deployment, unless you set up site or user policies, which override the global policy, or if you use Microsoft Exchange integration for some or all of your users. If you use Microsoft Exchange integration, the global policy does not apply to any users who are homed on Exchange 2013 and have the mailboxes put on In-Place Hold.

For details about how Archiving policies work, including the hierarchy for global, site, and user policies, see How Archiving Works Planning documentation, Deployment documentation, or Operations documentation.

Note:

If you enable Microsoft Exchange integration for your deployment, Exchange In-Place Hold policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.

You should specify all appropriate options in the Archiving configurations before enabling Archiving. For details, see Configuring Archiving Options in the Deployment documentation.

⊟To configure the global policy for archiving when using Lync Server Archiving databases

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server 2013 Control Panel. For details about the different methods you can use to start Lync Server 2013 Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. On the **Archiving Policy** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Archiving Policy - Global**, do the following:
   - In **Name**, if you do not want to use the default name of Global, specify a new name for the global policy.
   - In **Description**, provide information about what the policy is (for example, Global policy for *divisionName*).
   - To control archiving of internal communications for all sites and users not specifically controlled through a site policy or user policy, select or clear the **Archive internal communications** check box.
   - To control archiving of external communications for all sites and users not specifically controlled through a site policy or user policy, select or clear the **Archive external communications** check box.
6. Click **Commit**.

1.4.6.5.2.2 Setting Up Site Policies for Archiving

Setting Up Site Policies for Archiving

Deploying Archiving > Configuring Support for Archiving > Configuring and Assigning Archiving Policies >

Topic Last Modified: *2012-10-09*

You can enable or disable Archiving for specific sites by creating and configuring an Archiving policy for each of those sites. A site policy overrides the global policy, but user policies override site policies. Archiving policies only apply if you do not use Microsoft Exchange integration or, if you do use Microsoft Exchange integration, but have some users who are not homed on Exchange 2013 and have their mailboxes put on In-Place Hold.

For details about how Archiving policies work, including the hierarchy for global, site, and user policies, see How Archiving Works Planning documentation, Deployment documentation, or Operations documentation.

Note:

If you enable Microsoft Exchange integration for your deployment, Exchange In-Place Hold policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.

You should specify all appropriate options in the Archiving configurations before enabling Archiving of internal or external communications in the Archiving policies. For details, see Configuring Archiving Options in the Deployment documentation.

⊟To create an archiving policy for a site

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server 2013 Control Panel.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.

   For details about how Archiving policies work, including the hierarchy for global, site, and user policies, see How Archiving Works Planning documentation, Deployment documentation, or Operations documentation.
4. Click **New**, and then click **Site policy**.
5. In **Select a site**, click the site to which the policy is to be applied.
6. In **New Archiving Policy**, do the following:
   - In **Name**, specify the name for the site policy.
   - In **Description**, provide information about what the site policy is (for example, site policy for Redmond).
   - To control archiving of internal communications for the specified site, select or clear the **Archive internal communications** check box.
   - To control archiving of external communications for the specified site, select or clear the **Archive external communications** check box.
7. Click **Commit**.

1.4.6.5.2.3 Setting Up Archiving Policies for Users

Setting Up Archiving Policies for Users

Deploying Archiving > Configuring Support for Archiving > Configuring and Assigning Archiving Policies >

Topic Last Modified: *2012-10-09*

You can enable or disable Archiving for specific users by creating and configuring an Archiving policy for users, and then applying the policy to specific users or user groups. User policies override any global policy or site policies. Archiving policies only apply if you do not use Microsoft Exchange integration or, if you do use Microsoft Exchange integration, but have some users who are not homed on Exchange 2013 and have their mailboxes put on In-Place Hold.

For details about how Archiving policies work, including the hierarchy for global, site, and user policies, see How Archiving Works Planning documentation, Deployment documentation, or Operations documentation.

Note:

If you enable Microsoft Exchange integration for your deployment, Exchange In-Place Hold policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.
You should specify all appropriate options in the Archiving configurations before enabling Archiving of internal or external communications in the Archiving policies. For details, see Configuring Archiving Options in the Deployment documentation.

- Setting Up User Policies for Archiving in Lync Server
- Setting Up Policies for Archiving When Using Exchange Server Integration

Setting Up User Policies for Archiving in Lync Server

Configuring Support for Archiving > Configuring and Assigning Archiving Policies > Setting Up Archiving Policies for Users >

Topic Last Modified: *2012-10-10*

Enabling or disabling Archiving for specific users homed on Lync Server 2013 requires creating and configuring one or more user policies, and then applying the appropriate policy to specific users or user groups. User policies override site and global policies, but only for users homed on Lync Server 2013.

Users are always homed in Lync Server. If Microsoft Exchange integration is enabled, users whose mailboxes are in Microsoft Exchange Server 2013 don't need to have their Archiving policies in Lync Server managed. These users with Archiving will be managed by Exchange In-Place Hold.

For details about how Archiving policies work, including the hierarchy for global, site, and user policies, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

If you enabled Microsoft Exchange integration for your deployment, Exchange In-Place Hold policies control whether archiving is enabled for the users who are homed on Exchange 2013. Archiving for these users requires that they have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.

You should specify all appropriate options in the Archiving configurations before enabling Archiving. For details, see Configuring Archiving Options in the Deployment documentation.

- Creating and Configuring User Policies for Archiving in Lync Server
- Applying a Lync Server Archiving Policy to a User

Creating and Configuring User Policies for Archiving in Lync Server

Configuring and Assigning Archiving Policies > Setting Up Archiving Policies for Users > Setting Up User Policies for Archiving in Lync Server >

Topic Last Modified: *2012-10-09*

To enable or disable Archiving for specific users homed on Lync Server, you must first create a user policy and then apply the policy to one or more users or user groups. For details about applying user policies to specific users and user groups, see Applying a Lync Server Archiving Policy to a User in the Deployment documentation.

For details about how Archiving policies work, including the hierarchy for global, site, and user policies, see How Archiving Works in the Planning documentation, in the Deployment documentation, or in the Operations documentation.

Note:

If you enabled Microsoft Exchange integration for your deployment, Exchange In-Place Hold policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.

You should specify all appropriate options in the Archiving configurations before enabling

Archiving. For details, see Configuring Archiving Options in the Deployment documentation.

⊟To configure an archiving policy for users homed on Lync Server

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server 2013 Control Panel. For details about the different methods that you can use to start Lync Server 2013 Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. Click **New**, and then click **User policy**.
5. In **New Archiving Policy**, do the following:
   - In **Name**, specify the name for the user policy.
   - In **Description**, provide information about what the user policy is (for example, user policy for legal department).
   - To control archiving of internal communications for the user policy, select or clear the **Archive internal communications** check box.
   - To control archiving of external communications for the user policy, select or clear the **Archive external communications** check box.
6. Click **Commit**.

A user policy applies only to users to whom you assign the policy. For details about applying a user policy to specific users, see Applying a Lync Server Archiving Policy to a User in the Deployment documentation.

Applying a Lync Server Archiving Policy to a User

Configuring and Assigning Archiving Policies > Setting Up Archiving Policies for Users > Setting Up User Policies for Archiving in Lync Server >

Topic Last Modified: *2012-10-10*

After creating a Lync Server user policy, you must apply it to specific the users or user groups that are homed on Lync Server 2013 before it can take effect. For details about creating user policies for specific users, see Creating and Configuring User Policies for Archiving in Lync Server in the Deployment documentation.

For details about how Archiving policies work, including the hierarchy for global, site, and user policies, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

In order to configure and use archiving, you must first deploy archiving. For details, see Deploying Archiving in the Deployment documentation.

If you enabled Microsoft Exchange integration for your deployment, Exchange In-Place Hold policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.

You should specify all appropriate options in the Archiving configurations before enabling Archiving. For details, see Configuring Archiving Options in the Deployment documentation.

⊟To apply a Lync Server archiving policy to a user

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server 2013 Control Panel. For details about the different methods you can use to start Lync Server 2013 Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**, and then search for the user account that you want to configure.
4. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
5. In **Edit Lync Server user** under **Archiving policy**, select the archiving user policy that you want to apply.

   Note:
   The **<Automatic>** settings apply the default server installation settings. These settings are applied automatically by the server.

6. Click **Commit**.

Setting Up Policies for Archiving When Using Exchange Server Integration

Configuring Support for Archiving > Configuring and Assigning Archiving Policies > Setting Up Archiving Policies for Users >

Topic Last Modified: *2012-10-09*

If users homed on Exchange 2013 have their mailboxes put on In-Place Hold, Exchange In-Place Hold policies control archiving for those users. If you use Microsoft Exchange integration for your deployment, Exchange 2013 policies override Lync Server Archiving policies for users who are homed on Exchange 2013. For information about configuring Exchange Archiving policies, see the Exchange 2013 documentation. For details about setting up user policies for users homed on Lync Server 2013, see Setting Up User Policies for Archiving in Lync Server in the Deployment documentation. For details about how policies work, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:
If you deploy Exchange 2013 and Lync Server 2013 in the same forest, your Exchange 2013 In-Place Hold policies control archiving. If you deploy Exchange 2013 and Lync Server 2013 in separate forests, see “Deploying Lync Server and Microsoft Exchange in Different Forests” in Deployment Checklist for Archiving.

1.4.6.5.3 Enable or Disable Sending an Archiving Disclaimer to Federated Partners

Enable or Disable Sending an Archiving Disclaimer to Federated Partners

Deployment > Deploying Archiving > Configuring Support for Archiving >

Topic Last Modified: *2013-02-23*

At the time you deployed your Edge Servers and enabled federation for your organization, you should have specified whether to automatically send the archiving disclaimer to federated partners. If you archive external communications, you should enable the sending of an archiving disclaimer. Use the procedure in this topic to change that configuration.

Note:

The following procedure assumes that you have already enabled federation for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation.

To enable or disable sending of an archiving disclaimer to federated partners

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, click **Access Edge Configuration**.
4. On the **Access Edge Configuration** tab, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, under **Enable communications with federated users**, select or clear the **Send archiving disclaimer to federated partners** check box to enable or disable automatically sending the archiving disclaimer.
6. Click **Commit**.

To enable federated users to collaborate with users in your Lync Server 2013 deployment, you must have also configured at least one external access policy to support federated user access. For details, see Manage XMPP Federated Partners for Your Organization in the Deployment documentation or the Operations documentation. For details about controlling access for specific federated domains, see Configure Support for Allowed External Domains in the Deployment documentation or Operations documentation.

Enabling or Disabling the Archiving Disclaimer by Using Windows PowerShell Cmdlets

The use of the archiving disclaimer can be managed by using Windows PowerShell and the Set-CsAccessEdgeConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable the archiving disclaimer

- To enable the archiving disclaimer, set the value of the **EnableArchivingDisclaimer** property to True ($True):

```
Set-CsAccessEdgeConfiguration -EnableArchivingDisclaimer $True
```

To disable the archiving disclaimer

- To disable the archiving disclaimer, set the value of the **EnableArchivingDisclaimer** property to False ($False):

```
Set-CsAccessEdgeConfiguration -EnableArchivingDisclaimer $False
```

1.4.7 Configuring Video

Configuring Video

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-10-02*

Lync Server 2013 introduces the following new video features:

- **HD video** Users can experience resolutions up to full high definition (HD) (that is, 1920 x 1080) in two-party calls and multiparty conferences.
- **Gallery View** In video conferences that have more than two people, users can see videos of participants in the conference. If the conference has more than five participants, video of only the most active participants appears in the top row, and a photo appears for the other participants.
- **H.264 video** The H.264 video codec is now the default for encoding video on Lync 2013 clients. H.264 video supports a greater range of resolutions and frame rates, and improves video scalability.

> **Note:**
> Lync Server 2013 still supports the VC1 codec for interoperability with previous versions of Lync. For details and background information about the new video codec, see Jeff Schertz's Blog article, "Video Interoperability in Lync 2013," at http://blog.schertz.name/2012/07/video-interoperability-in-lync-2013/.

This section describes how to manage bandwidth for video in Lync Server 2013 and how to configure video features.

- Configuring Video Bandwidth in Lync Server 2013
- Configuring Gallery View
- Configuring Video Example Scenarios
- Interoperability Considerations for Video Conferencing

1.4.7.1 Configuring Video Bandwidth in Lync Server 2013

Configuring Video Bandwidth in Lync Server 2013

Microsoft Lync Server 2013 > Deployment > Configuring Video >

Topic Last Modified: *2012-10-02*

Lync Server 2013 includes several settings for managing video for two-party calls and multiparty conferences. When you deploy Lync Server 2013, you should evaluate whether the default settings are appropriate for your organization, and modify them as necessary.

The parameters described in this section apply to both two-party calls and multiparty conferencing. View or modify these settings by using one of the following cmdlets:

- **Get-CsConferencingPolicy**
- **Set-CsConferencingPolicy**
- **New-CsConferencingPolicy**

Verify the following settings in your conferencing policy:

- **VideoBitRateKb** This setting specifies the maximum video bit rate in kilobits per second (kbps) used for video sent by a user. The default value is 50000 kbps. Valid values are 0 to 50000.
  This setting applies separately to main video and panoramic video.
  Example: if you specify 2000 kbps, then Lync Server can send 2000 kbps for the main video stream and 2000 kbps for the panoramic video stream.

Note:
The maximum video network bandwidth for a Lync 2013 endpoint is 8000 kbps for the main video and 2500 kbps for panoramic video. These maximum values are reached only if multiple videos are received or sent. For details, see the "Media Traffic Network Usage" section in Network Bandwidth Requirements for Media Traffic. This section lists the maximum and typical video stream bandwidth for all supported resolutions.

- **TotalReceiveVideoBitRateKb** This setting, which is new in Lync Server 2013, specifies the maximum allowed bitrate (in kilobits per second) for all the video streams received by a client. That is, it specifies the combined total for all the video streams, except for panoramic video streams, that a client can receive. For example, if you specify 1500 kbps, then a client can receive up to 1500 kbps of video, which may consist of multiple video streams or a single video stream. This setting applies only to Lync Server 2013 clients.
  The default value for **TotalReceiveVideoBitRateKb** is 50000 kbps. If the **EnableMultiviewJoin** setting for Gallery View is set to True, **TotalReceiveVideoBitRateKb** must not be set below 420 kbps. If the **EnableMultiviewJoin** setting for Gallery View is set to False, **TotalReceiveVideoBitRateKb** must not be set below 100 kbps. If **EnableMultiviewJoin** is set to True and you set the value below 420 kbps, the values will default to the threshold value. This threshold helps prevent accidental misconfiguration that might result in poor user experience.

  Note:
  For details about the **EnableMultiviewJoin** setting, see Configuring Gallery View.

- **MaxVideoConferencingResolution** This parameter is no longer used for Lync Server 2013 clients in Lync Server 2013 conferences. Lync Server 2013 conferences use the bit rate controls described earlier in this section. This setting is still used for legacy clients joining a Lync Server 2013 conference. This parameter determines the maximum resolution allowed for legacy clients in conferences organized by users who are homed on Lync Server 2013. That is, legacy clients are treated the same as they were in previous versions of Lync Server or Office Communications Server.

In addition to conferencing policy settings that apply to users, evaluate media configuration settings. View or modify these settings by using one of the following cmdlets:

- **Get-CsMediaConfiguration**
- **Set- CsMediaConfiguration**
- **New- CsMediaConfiguration**

Verify the following setting:

- **MaxVideoRateAllowed** This per-pool setting specifies the maximum rate at which video signals will be transferred at the client endpoints. It applies only to previous versions of Lync Server clients.

  Note:
  Lync Server 2013 clients ignore this setting and use the TotalReceiveVideoBitRateKb setting in conferencing policy instead.

  The default value is HD720P. Valid values are HD720p15M, VGA600K, and CIF250K.
  Example: If you specify 1500 kbps, then all the legacy clients in the pool can receive up to 1500 kbps of video in two-party or multiparty conferences.

The following procedures are examples of using Lync Server Management Shell to modify the settings described in this section.

⊟To modify conferencing policy for video settings

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. At the command line, run the following cmdlet to edit conferencing policy:

```
Set-CsConferencingPolicy -Identity Pool01ConferencingPolicy -VideoBitR
```

To modify media configuration for legacy clients

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. At the command line, run the following cmdlet to edit the media configuration:

```
Set-CsMediaConfiguration -Identity site:Redmond01 -MaxVideoRateAllowed
```

1.4.7.2 Configuring Gallery View

Configuring Gallery View

Microsoft Lync Server 2013 > Deployment > Configuring Video >

Topic Last Modified: *2012-10-30*

In Lync Server 2013, you configure Gallery View video conferencing in conferencing policy. Gallery View is turned on by default. If you do not want to allow Gallery View, or want to allow it for only some users, you need to turn off the feature in conferencing policy.

When a conference participant's video is not available, the users' Gallery View experience can be enhanced if you deploy high-resolution photos, a new feature in Lync Server 2013. High-resolution photos provide an alternative to the smaller, limited resolution contact photos stored in Active Directory Domain Services (AD DS). High-resolution photos are stored in a user's Exchange 2013 mailbox, and, therefore, require you to integrate Lync Server 2013 with Exchange 2013. For details, see the NextHop blog article, "Integrating Exchange 2013 and Lync Server 2013," at http://go.microsoft.com/fwlink/p/?LinkId=260987.

Note:

The content of each blog and its URL are subject to change without notice.

You can view or modify the Gallery View parameters by using Lync Server 2013 Control Panel or by using one of the following cmdlets:

- **Get-CsConferencingPolicy**
- **Set-CsConferencingPolicy**
- **New-CsConferencingPolicy**

Configure Gallery View with the following conferencing policy settings:

- **AllowMultiview** This parameter controls whether a user is allowed to organize Gallery View video conferences. This parameter applies to scheduled and ad-hoc meetings created by the user.
  Examples:
  - This parameter is set to True for User A, who is homed on a Lync Server 2013 pool. Meetings organized by User A enable users to join and receive multiple video streams.
  - This parameter is set to False for User B, who is homed on a Lync Server 2013 pool. Meetings organized by User B have a single video stream that is similar to the video conference experience provided by Lync Server 2010.

  This parameter determines who can organize meetings that allow multiple video streams. Participants in meetings that allow multiple video streams may or may not be allowed to receive multiple video streams, based on their individual permissions (see the description for the EnableMultiviewJoin parameter).

- **EnableMultiviewJoin** This parameter controls whether a participant in a meeting receives the Gallery View video experience in meetings that allow it. This parameter controls the user's experience in any meeting in which he or she participates.
  Examples:
  - This parameter is set to True for User C. User C can receive multiple video streams when participating in a meeting organized or started by User A. User C receives a single video stream that is similar to the video conference experience provided by Lync Server 2010 when participating in a meeting organized or started by User B.
  - This parameter is set to False for User D. User D receives single video stream that is similar to the video conference experience provided by Lync Server 2010 when participating in any meeting organized by User A or User B.

The following procedure is an example of using Lync Server Management Shell to enable Gallery View video conferencing.

⊟To modify conferencing policy for Gallery View video conferencing

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. At the command line, run the following cmdlet to edit conferencing policy:

```
Set-CsConferencingPolicy -Identity Pool01ConferencingPolicy -AllowMult
```

1.4.7.3 Configuring Video Example Scenarios

Configuring Video Example Scenarios

Microsoft Lync Server 2013 > Deployment > Configuring Video >

Topic Last Modified: *2012-10-02*

Lync 2013 adds new video features to support 1920 x 1080 full high definition (HD) video and Gallery View video. Measurements based on customer data show that the typical video bandwidth increased only slightly compared to Lync 2010, but the maximum video stream bandwidth has increased due to full HD support (for details, see the "Media Traffic Network Usage" section in Network Bandwidth Requirements for Media Traffic). Therefore, administrators may want to restrict video bandwidth for certain users (such as users in a branch office that has less network capacity) and help to ensure the best possible video quality for other users (such as executives).

The following table provides a list of recommended settings for configuring video for different network capacities. These settings will restrict some user scenarios from sending and receiving higher resolution videos (see rightmost column). The minimum setting will result in Gallery Video being unavailable, due to the low maximum receive network bandwidth.

Recommended Video Settings

-	AllowMultiView	EnableMultiViewJoin	VideoBitRate KB	TotalReceiveVideoBitRate KB	Expected video resolution for good quality video
Best	True	True	8000	8000	Peer-to-peer: Up to 1920 x

					1080 video resolution Gallery View: Up to two 1920 x 1080 videos or multiple smaller resolution videos
Good	True	True	2500	2500	Peer-to-peer: Up to 1280 x 720 video resolution Gallery View: Up to five 640 x 360 resolution videos
Medium	True	True	1000	1000	Peer-to-peer: Up to 960 x 540 video resolution Gallery View: Up to five 424 x 240 resolution videos
Minimum	True	False	350	350	Peer-to-peer: Up to 424 x 240 video resolution Gallery View: Unavailable

You can use the information in the preceding table to deploy the new HD video and Gallery View video conferencing features for some users in your organization, while allowing different video resolutions for others.

In the following example, the administrator rolls out the new video features with the highest video quality available only to executives. For employees in a remote branch office that has low network capacity, only the minimum setting from the preceding table is deployed. For all other employees, the "Good" setting from the preceding table is deployed.

To roll out the new features to the executives, the administrator creates a conferencing policy named ExecutiveVideo. This conferencing policy has the following settings:

- VideoBitRateKB is set to 8000 Kbps
- TotalReceiveVideoBitRateKB is set to 8000 Kbps
- AllowMultiview is set to True
- EnableMultiviewJoin is set to True

For employees in the branch office, the administrator creates a conferencing policy named

BranchOfficeVideo. This conferencing policy has the following settings:

- VideoBitRateKB is set to 350 Kbps
- TotalReceiveVideoBitRateKB is set to 350 Kbps
- AllowMultiview is set to True
- EnableMultiviewJoin is set to False

For all other employees, the administrator creates a conferencing policy named StandardVideo. This conferencing policy has the following settings:

- VideoBitRateKB is set to 2500 Kbps
- TotalReceiveVideoBitRateKB is set to 2500 Kbps
- AllowMultiview is set to True
- EnableMultiviewJoin is set to True

The administrator assigns conferencing policy to users as follows:

- The ExecutiveVideo conferencing policy is assigned to the executives.
- The BranchOfficeVideo conferencing policy is assigned to all employees in the branch office.
- The StandardVideo conferencing policy is assigned to all other employees.

These conferencing policy assignments result in the following user experience:

- All conferences organized by any user support Gallery View, but employees in the branch office cannot experience Gallery View.
- For any two-party or multiparty conferences, executives can send 1920 x 1080 full HD video, if their hardware and network link supports it, and can receive 1920 x 1080 full HD video where the other participant clients support it.
- Employees who are not executives experience lower resolutions than the executives in their two-party or multiparty conferences, but still get good resolution.
- Employees who are in the branch office will get good video quality in two-party calls when Lync displays the default video window size; however, if the Lync window is maximized to full screen, the video resolution will not increase. For multiparty conferences, the employees in the branch office will see only one active video.

1.4.7.4 Interoperability Considerations for Video Conferencing

Interoperability Considerations for Video Conferencing

Microsoft Lync Server 2013 > Deployment > Configuring Video >

Topic Last Modified: *2012-10-02*

This section describes the user experience during the coexistence phase of migration, when there is interoperability between legacy clients and a Lync Server 2013 pool or Lync Server 2013 clients and a legacy pool.

Lync Server 2013 Pools

Users will experience the following behavior when a legacy client is used in a Lync Server 2013 pool:

- For two-party calls, video resolution is the same as in the legacy pool.
- For multiparty conferences, video resolution and video conferencing features are the same as in the legacy pool. Gallery View and high resolution are not available.

Legacy Pools

Users will experience the following behavior when a Lync Server 2013 client is used in a legacy pool:

- For two-party calls, Lync Server 2013 clients can use new features as follows:
  - H.264 is available if both participants are using Lync Server 2013 clients.
  - The Lync Server 2013 client uses the default value for TotalReceiveVideoBitRateKb, since the legacy server doesn't send this information with in-band provisioning.
- For multiparty conferences, video resolution and video conferencing features are the same as experienced by a legacy client in the legacy pool.

Note:

When a legacy server hosts a Lync Server 2013 client, it's possible to configure video conferencing bandwidth so that all users on the pool receive only low-resolution video, but send high-resolution video. An example of this is when MaxVideoRateAllowed is set to CIF-250K in the media configuration and VideoBitRateKb is set to 2000 kbps in conferencing policy. The net effect in this situation is that high resolution is not possible for users on the pool.

Because MaxVideoRateAllowed is no longer used for Lync Server 2013 clients, it cannot prevent Lync Server 2013 clients from requesting high-resolution video. Instead, set VideoBitRateKb in conferencing policy for all users on the pool to the same value as MaxVideoRateAllowed (that is, CIF is set to 250 kbps, or VGA is set to 600 kbps, or HD is set to 1500 kbps).

1.4.8 Deploying Branch Sites

Deploying Branch Sites

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-09-21*

Branch site users get most of their Lync Server 2013 functionality from the server at the central site that the branch site is associated with. Each branch site is associated with exactly one central site. To provide calls to and from the public switched telephone network (PSTN), a branch site might contain any of the following:

- A PSTN gateway and possibly a Meditation Server
- A SIP trunk
- An existing voice infrastructure with a private branch exchange (PBX)
- A Survivable Branch Appliance
- A Survivable Branch Server

Branch sites with a Survivable Branch Appliance or a Survivable Branch Server are more resilient in times of wide-area network or central site failures than branch sites without one of these solutions. For example, in a site with a Survivable Branch Appliance or a Survivable Branch Server deployed, users can still make and receive PSTN calls if the network connecting the branch site to the central site is down. Another way to achieve branch-site resiliency is by using a PSTN gateway or a SIP trunk with a full-scale Lync Server deployment at the branch site.

For details about which branch site deployment is right for your organization, including prerequisites and other planning considerations, see Planning for PSTN Connectivity and Planning for Branch-Site Voice Resiliency in the Planning documentation.

- Providing PSTN Connectivity at a Branch Site
- Deploying a Survivable Branch Appliance or Server

1.4.8.1 Providing PSTN Connectivity at a Branch Site

Providing PSTN Connectivity at a Branch Site

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Branch Sites >

Topic Last Modified: *2012-10-05*

We recommend using the Microsoft Lync Server 2013, Planning Tool to add branch sites to your topology and to set up your voice infrastructure in branch sites.

If you are not using the Planning Tool, use the procedures in the topics in this section—first, to add the branch sites, and then, to set up your voice infrastructure by defining the IP/public switched telephone network (PSTN) gateway and/or by configuring the SIP trunk (with or without media bypass). Connecting a private branch exchange (PBX) to the branch site is another option.

Note:
If you want to provide branch-site resiliency, you must deploy a Survivable Branch Appliance, a Survivable Branch Server, or Standard Edition server at the branch site. For details, see Deploying a Survivable Branch Appliance or Server or Deploying Lync Server 2013, as appropriate, in the Deployment documentation.

- Add Branch Sites to Your Topology
- Define a PSTN Gateway for a Branch Site
- Configure a Trunk with Media Bypass
- Configure a Trunk without Media Bypass

⊟See Also

Other Resources

Planning for Media Bypass
Planning for PSTN Connectivity

1.4.8.1.1 Add Branch Sites to Your Topology

Add Branch Sites to Your Topology

Deployment > Deploying Branch Sites > Providing PSTN Connectivity at a Branch Site >

Topic Last Modified: *2012-10-05*

Branch sites represent physical branch offices that are connected to your main offices over a WAN link. To add a branch site to your Lync topology, perform this procedure at the central site.

⊟To add branch sites to your topology

1. Click **Start**, click **All Programs**, click **Microsoft Lync Server**, and then click **Lync Server Topology Builder**.
2. In the console tree, expand the central site, right-click **Branch Sites**, and then click **New Branch Site**.
3. In the **Define New Branch Site** dialog box, click **Name**, and then type the name of the branch site.
4. (Optional) Click **Description**, and then type a meaningful description for the branch site.
5. Click **Next**.
6. (Optional) In the next **Define New Branch Site** dialog box, do any of the following:

- Click **City**, and then type the name of the city in which the branch site is located.
- Click **State/Region**, and then type the name of the state or region in which the branch site is located.
- Click **Country Code**, and then type the two-digit calling code for the country/region in which the branch site is located.

7. Click **Next**, and then do one of the following:
   - If you are using a Survivable Branch Appliance or Server at this site, be sure that the **Open the New Survivable Wizard when this wizard closes** check box is selected, click **Finish**, and then follow the directions in the wizard that opens. For information about wizard items, see Define a Survivable Branch Appliance or Server.
   - If you are not using a Survivable Branch Appliance or Server at this site, clear the **Open the New Survivable Wizard when this wizard closes** check box, and then click **Finish**.
8. Repeat the previous steps for each branch site that you want to add to the topology.

Next step:

For Survivable Branch Appliances or Servers: Define a Survivable Branch Appliance or Server

For non-resilient PSTN connectivity: Define a PSTN Gateway for a Branch Site, Configure a Trunk with Media Bypass, or Configure a Trunk without Media Bypass

1.4.8.1.2 Define a PSTN Gateway for a Branch Site

Define a PSTN Gateway for a Branch Site

See Also

Deployment > Deploying Branch Sites > Providing PSTN Connectivity at a Branch Site >

Topic Last Modified: *2012-09-21*

Perform this procedure at the central site, which contains at least one Front End pool or Standard Edition server.

◆**Important:**
Before you perform the procedure, the following conditions must be in place: • Lync Server 2013 communications software must be set up at the central site. • Mediation Server must be deployed at the central site.

⊟To define a PSTN gateway

1. Click **Start**, click **All Programs**, click **Microsoft Lync Server**, and then click **Lync Server Topology Builder**.
2. In the console tree, expand the central site, expand **Branch Office Sites**, expand name of the branch site that you want to define a public switched telephone network (PSTN) gateway for, and then expand **Shared Components**.
3. Right-click **PSTN gateways**, and then click **New IP/PSTN Gateway**.
4. In the **Define New IP/PSTN Gateway** dialog box, click **Gateway FQDN or IP Address**, and then type the fully qualified domain name (FQDN) or IP address of the gateway that you are deploying at the branch site.
5. Click **Listening Port for IP/PSTN Gateway**, and then accept the default values.
6. In the **SIP Transport Protocol** list, click the transport protocol the gateway

uses, and then click **OK**.

> **Note:**
> For security reasons, we strongly recommend that you use a PSTN gateway that supports Transport Layer Security (TLS).

> **Tip:**
> Use the cmdlet **Set-CsPstnGateway** to modify properties of a PSTN gateway. For details, see Set-CsPstnGateway, in the Lync Server Management Shell Help.

Next step for branch-site resiliency: Configuring Users for Branch Site Resiliency

Concepts

PSTN Gateway Deployment Options

1.4.8.1.3 Configure a Trunk with Media Bypass

Configure a Trunk with Media Bypass

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2013-02-24*

Follow these steps to configure a trunk with media bypass enabled. To configure a trunk with media bypass disabled, see Configure a Trunk without Media Bypass.

We strongly recommend that you enable media bypass. However, before you enable media bypass on a SIP trunk, confirm that your qualified SIP trunk provider supports media bypass and is able to accommodate the requirements for successfully enabling the scenario. Specifically, the provider must have the IP addresses of servers in your organization’s internal network. If the provider cannot support this scenario, media bypass will not succeed. For details, see Planning for Media Bypass in the Planning documentation.

> **Note:**
> Media bypass will not interoperate with every public switched telephone network (PSTN) gateway, IP-PBX, and Session Border Controller (SBC). Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions that are listed on Unified Communications Open Interoperability Program – Lync Server at http://go.microsoft.com/fwlink/p/?linkId=214406.

A trunk configuration as described below groups a set of parameters that are applied to trunks assigned this trunk configuration. A particular trunk configuration can be scoped globally (to all trunks that do not have more specific site or pool configuration), or to a site, or to a pool. The pool-level trunk configuration is used to scope a specific trunk configuration to a single trunk.

⊟To configure a trunk with media bypass

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Trunk**

Configuration.

4. On the **Trunk Configuration** page, use one of the following methods to configure a trunk:
   - Double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
   - Click **New**, and then select a scope for the new trunk configuration:
     - **Site trunk:** Choose the site for this trunk configuration from **Select a Site**, and then click **OK**. Note that if a trunk configuration has already been created for a site, the site does not appear in **Select a Site**. This trunk configuration will be applied to all trunks in the site.
     - **Pool trunk:** Choose the name of the trunk that this trunk configuration applies to. This trunk can be the root trunk or any additional trunks defined in Topology Builder. From **Select a Service**, click **OK**. Note that if a trunk configuration has already been created for a specific trunk, the trunk does not appear in **Select a Service**.

   Note:

   After you select the scope of the trunk configuration, it cannot be changed. The **Name** field is prepopulated with the name of the trunk configuration's associated site or service and cannot be changed.

5. Specify a value in **Maximum early dialogs supported**. This is the maximum number of forked responses a public switched telephone network (PSTN) gateway, IP-PBX, or ITSP Session Border Controller (SBC) can receive to an INVITE that it sent to the Mediation Server. The default value is 20.

   Note:

   Before you change this value, consult your service provider or equipment manufacturer for details about the capabilities of your system.

6. Select one of the following **Encryption support level** options:
   - **Required:** Secure real-time transport protocol (SRTP) encryption must be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
   - **Optional:** SRTP encryption will be used if the service provider or equipment manufacturer supports it.
   - **Not Supported:** SRTP encryption is not supported by the service provider or equipment manufacturer and therefore will not be used.
7. Select the **Enable media bypass** check box if you want media to bypass the Mediation Server for processing by the trunk peer.

   Important:

   For media bypass to work successfully, the PSTN gateway, IP-PBX, or ITSP Session Border Controller must support certain capabilities. For details, see Planning for Media Bypass in the Planning documentation.

8. Select the **Centralized media processing** check box if there is a well-known media termination point (for example, a PSTN gateway where the media termination has the same IP as the signaling termination). Clear this check box if the trunk does not have a well-known media termination point.
9. If the trunk peer supports receiving SIP REFER requests from the Mediation Server, select the **Enable sending refer to the gateway** check box.

   Note:

   If you disable this option while the **Enable media bypass** option is selected, additional settings are required. If the trunk peer does not support receiving SIP REFER requests from the Mediation Server and media bypass is enabled, you must also run the **Set-CsTrunkConfiguration** cmdlet to disable RTCP for active and held calls in order to support proper conditions for media bypass. For details, see the Lync Server Management Shell documentation. Alternatively, you can select **Enable refer using third-party-call control** if you want transferred calls to be media bypassed, and the gateway does not support SIP REFER requests.

10.(Optional) To enable inter-trunk routing, associate and configure PSTN usage records to this trunk configuration. The PSTN usages associated to this trunk configuration will be applied for all incoming calls through the trunk that is not originating from a Lync endpoint. To manage PSTN usage records associated to a trunk configuration, use one of the following methods:

- To select one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records you want to associate with this trunk configuration and then click **OK**.
- To remove a PSTN usage record from this trunk configuration, select the record and click **Remove**.
- To define a new PSTN usage record and associate it with this trunk configuration, do the following:
  - Click **New**.
  - In the **Name** field, specify a descriptive name for the record that is unique.

    Note:
    The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

  - Use one of the following methods to associate and configure routes for this PSTN usage record:
    - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
    - To remove a route from the PSTN usage record, select the route, and click **Remove**.
    - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
    - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
  - Click **OK**.
- To edit a PSTN usage record that is already associated with this trunk configuration, do the following:
  - Select the PSTN usage record you want to edit, and click **Show details**.
  - Use one of the following methods to associate and configure routes for this PSTN usage record:
    - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
    - To remove a route from the PSTN usage record, select the route, and click **Remove**.
    - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
    - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
  - Click **OK**.

Important:
It important to associate PSTN usage records according to the Mediation Server peer that is associated to the trunk being configured. If the Mediation Server peer is a PSTN gateway or a Session Border Controller (SBC), it is strongly recommended that the trunk configuration is not associated to a PSTN usage record that routes to a PSTN destination or any other downstream systems connected via Lync Server.

11.Arrange the PSTN usage records for optimum performance. To change a record’s position in the list, select the PSTN usage record, and click the up or down arrows.

Important:

The order in which PSTN usage records are listed in the trunk configuration is significant. Lync Server traverses the list from top to down.

12. **Enable RTP Latching** should be selected to enable bypass media for clients behind a network address translation (NAT) or firewall and an SBC that supports latching.
13. **Enable forward call history** should be selected to enable sending of call history information to the gateway peer of the Mediation Server.
14. **Enable forward P-Asserted-Identity data** should be selected to enable the P-Asserted-Identity (PAI) call originator information to be forwarded between the Mediation Server side and gateway side (and vice versa), when present.
15. **Enable outbound routing failover timer** should be selected to enable fast failover. The gateway associated with this trunk can give notification within 10 seconds that it is processing an outbound call. Rerouting to another trunk will occur if this notification is not received by the Mediation Server. On networks where latency may delay the response time or the gateway takes longer than 10 seconds to respond, the fast failover should be disabled.
16. (Optional) Associate and configure **calling number translation rules** for the trunk. These translation rules apply to the calling number for outbound calls
    - To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
    - To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
    - To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
    - To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
    - To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

Warning:

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

17. (Optional) Associate and configure **called number translation rules** for the trunk. The translation rules apply to the called number in an outbound call.
    - To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
    - To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
    - To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
    - To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
    - To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

Warning:

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

18. Make sure that the trunk's translation rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name and then click the up or down arrow.

Important:

Lync Server 2013 traverses the translation rule list from the top down and uses the first rule that matches the dialed number. If you configure a trunk so that a dialed number can match more than one translation rule, be sure that the more restrictive rules are sorted above the less restrictive rules. For example, if you have included a translation rule that matches any 11-digit number and a translation rule that matches only 11-digit numbers that start with +1425, be sure that the rule that matches any 11-digit number is sorted *below* the more restrictive rule.

19. When you are finished configuring the trunk, click **OK**.
20. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

Note:

Whenever you create or modify a trunk configuration, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

After you have configured the trunk, continue configuring media bypass by choosing between global media bypass options, as described in Global Media Bypass Options in the Deployment documentation.

Tasks

Configure a Trunk without Media Bypass

Concepts

Configure Media Bypass
Global Media Bypass Options

Other Resources

Defining Translation Rules

1.4.8.1.4 Configure a Trunk without Media Bypass

Configure a Trunk without Media Bypass

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

***Topic Last Modified:** 2013-02-24*

If you want to configure a trunk with media bypass disabled, follow these steps. If you want to configure a trunk with media bypass enabled, see Configure a Trunk with Media Bypass.

A trunk configuration, as described below, groups a set of parameters that are applied to trunks assigned this trunk configuration. A particular trunk configuration can be scoped globally (to all trunks that do not have more specific site or pool configuration), or to a site, or to a pool. The pool-level trunk configuration is used to scope a specific trunk configuration to a single trunk.

⊟To configure a trunk without media bypass

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
4. On the **Trunk Configuration** page, use one of the following methods to configure a trunk:
   - Double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
   - Click **New**, and then select a scope for the new trunk configuration:
     - **Site trunk:** Choose the site for this trunk configuration in **Select a Site** , and then click **OK**. Note that if a trunk configuration has already been created for a site, the site does not appear in **Select a Site**. This trunk configuration will be applied to all trunks in the site.
     - **Pool trunk:** Choose the name of the trunk that this trunk configuration applies to in **Select a Service** and click **OK**. This trunk can be the root trunk, or any additional trunks defined in Topology Builder. Note that if a trunk configuration has already been created for a specific trunk, the trunk does not appear in **Select a Service**.

   Note:

   After you select the scope of the trunk configuration, it cannot be changed. The **Name** field is prepopulated with the name of the trunk configuration's associated site or service and cannot be changed.
5. Select one of the following **Encryption support level** options:
   - **Required:** Secure real-time transport protocol (SRTP) encryption must be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
   - **Optional:** SRTP encryption will be used if the service provider or equipment manufacturer supports it.
   - **Not Supported:** SRTP encryption is not supported by the service provider or equipment manufacturer and therefore will not be used.
6. Be sure that the **Enable media bypass** check box is cleared.
7. Select the **Centralized media processing** check box if there is a well-known media termination point (for example, a public switched telephone network (PSTN) gateway where the media termination has the same IP as the signaling termination). Clear this check box if the trunk does not have a well-known media termination point.
8. If the trunk peer supports receiving SIP REFER requests from the Mediation Server, select the **Enable sending refer to the gateway** check box.
9. (Optional) To enable inter-trunk routing, associate and configure PSTN usage records to this trunk configuration. The PSTN usages associated to this trunk configuration will be applied for all incoming calls through the trunk that is not originating from a Lync endpoint. To manage PSTN usage records associated to a trunk configuration, use one of the following methods:
   - To select one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records you want to associate with this trunk configuration and then click **OK**.
   - To remove a PSTN usage record from this trunk configuration, select the record and click **Remove**.
   - To define a new PSTN usage record and associate it with this trunk configuration, do the following:
     - Click **New**.
     - In the **Name** field, specify a descriptive name for the record that is

unique.

> **Note:**
> The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

- Use one of the following methods to associate and configure routes for this PSTN usage record:
  - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
  - To remove a route from the PSTN usage record, select the route, and click **Remove**.
  - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
- Click **OK**.

- To edit a PSTN usage record that is already associated with this trunk configuration, do the following:
  - Select the PSTN usage record you want to edit, and click **Show details**.
  - Use one of the following methods to associate and configure routes for this PSTN usage record:
    - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
    - To remove a route from the PSTN usage record, select the route, and click **Remove**.
    - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
    - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
  - Click **OK**.

> **Important:**
> It important to associate PSTN usage records according to the Mediation Server peer that is associated to the trunk being configured. If the Mediation Server peer is a PSTN gateway or a Session Border Controller (SBC), it is strongly recommended that the trunk configuration is not associated to a PSTN usage record that routes to a PSTN destination or any other downstream systems connected via Lync Server.

10. Arrange the PSTN usage records for optimum performance. To change a record’s position in the list, select the PSTN usage record, and click the up or down arrows.

> **Important:**
> The order in which PSTN usage records are listed in the trunk configuration is significant. Lync Server traverses the list from top to down.

11. **Enable RTP Latching** should be selected to enable bypass media for clients behind a NAT or firewall and an SBC that supports latching.
12. **Enable forward call history** should be selected to enable sending of call history information to the gateway peer of the Mediation Server.
13. **Enable forward P-Asserted-Identity data** should be selected to enable PAI call originator information to be forwarded between the Mediation Server side and gateway side (and vice versa), when present.
14. **Enable outbound routing failover timer** should be selected to enable fast failover. The gateway associated with this trunk can give notification within 10 seconds that it is processing an outbound call. Rerouting to another trunk will occur if this notification is not received by the Mediation Server. On

networks where latency may delay the response time or the gateway takes longer than 10 seconds to respond, the fast failover should be disabled.

15.(Optional) Associate and configure **calling number translation rules** for the trunk. These translation rules apply to the calling number for outbound calls

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

Security Note:

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

16.(Optional) Associate and configure **called number translation rules** for the trunk. The translation rules apply to the called number in an outbound call.

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

Caution:

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

17.Make sure that the trunk's translation rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name, and then click the up or down arrow.

Important:

Lync Server traverses the translation rule list from the top down and uses the first rule that matches the dialed number. If you configure a trunk so that a dialed number can match more than one translation rule, be sure that the more restrictive rules are sorted above the less restrictive rules. For example, if you have included a translation rule that matches any 11-digit number and a translation rule that matches only 11-digit numbers that start with +1425, be sure that the rule that matches any 11-digit number is sorted *below* the more restrictive rule.

18. When you are finished configuring the trunk, click **OK**.
19. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

> **Note:**
> Whenever you create or modify a trunk configuration, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Configure a Trunk with Media Bypass

Other Resources

Defining Translation Rules

1.4.8.2 Deploying a Survivable Branch Appliance or Server

Deploying a Survivable Branch Appliance or Server

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Branch Sites >

Topic Last Modified: *2012-10-10*

Resilient Enterprise Voice refers to branch-site resiliency, that is, the ability to provide continuous Enterprise Voice service to branch site users in the event that the link to the central site becomes unavailable.

For small and medium-sized branch sites (branch sites with 25 to 1,000 users), we recommend deploying a Survivable Branch Appliance, which will terminate public switched telephone network (PSTN) calls by using its built-in PSTN gateway or a SIP trunk to a telephone service provider. A Survivable Branch Appliance is a third-party device that includes a blade server running the Windows Server 2008 R2 operating system, Lync Server 2013 Registrar, Mediation Server software, and a PSTN gateway, all in a single appliance chassis.

For branch sites with 1,000 to 5,000 users and no resilient WAN, we recommend a Survivable Branch Server connected to either a PSTN gateway or a SIP trunk to a telephone service provider. A Survivable Branch Server is a Windows Server-based computer that has Registrar and Mediation Server software installed on it.

> **Note:**
> For branch sites with more than 5,000 users and dedicated Lync Server administrators, we recommend a full Lync Server 2013 deployment, separate from that of the central site. For details about choosing the best resiliency solution for the branch sites in your organization, including prerequisites and planning considerations, see Branch-Site Resiliency Requirements in the Planning documentation.

- Deploying a Survivable Branch Appliance or Server - Central Site Tasks
- Deploy a Survivable Branch Appliance or Server - Branch Site Task
- Configuring Users for Branch Site Resiliency
- Home Users on a Survivable Branch Appliance or Server
- Appendices: Survivable Branch Appliances and Servers

See Also

Other Resources

Deploying Lync Server 2013

1.4.8.2.1 Deploying a Survivable Branch Appliance or Server - Central Site Tasks

Deploying a Survivable Branch Appliance or Server - Central Site Tasks

Deployment > Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server >

Topic Last Modified: *2012-10-18*

Complete the tasks in this section at the central site. If you're deploying a Survivable Branch Server, skip the first task.

Important:

Before you perform the tasks in this section, the following conditions must be in place:

- Lync Server must be set up at the central site.
- An installation technician at the branch site must be added to the RTCUniversalSBATechnicians group.

In addition, we recommend that you do the following:

- Deploy a DHCP server at each branch site to enable clients to obtain IP addresses.
- As an alternative to deploying a DHCP server at each branch site, enable Lync Server DHCP on the Survivable Branch Appliance or Survivable Branch Server by using the Lync Server Management Shell cmdlet **Set-CsRegistrarConfiguration –EnableDHCPServer $true**. For details, see the "Hardware and Software Requirements" section of Branch-Site Resiliency Requirements in the Planning documentation.

- Add a Survivable Branch Appliance to Active Directory
- Add Branch Sites to Your Topology
- Define a Survivable Branch Appliance or Server

1.4.8.2.1.1 Add a Survivable Branch Appliance to Active Directory

Add a Survivable Branch Appliance to Active Directory

Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server > Deploying a Survivable Branch Appliance or Server - Central Site Tasks >

Topic Last Modified: *2012-09-23*

If you plan to deploy a Survivable Branch Appliance, you must add the Survivable Branch Appliance to Active Directory Domain Services. Perform this procedure at the central site.

Important:

Perform this procedure only if you are deploying a Survivable Branch Appliance. Do not perform it if you are deploying a Survivable Branch Server.

To add an Survivable Branch Appliance to Active Directory Domain Services

1. Log on to a member server as a member of the Enterprise Admins group.
2. Click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. On the **Actions** menu, click **New** and then click **Computer**.
4. In the **New Object-Computer** dialog box, type in a name for the Survivable Branch Appliance computer object (for example, BranchOffice1), and then click **Change**.
5. In the **Select User or Group** dialog box, add the RTCUniversalSBATechnicians group and then click **OK**.

Note:
A member of the RTCUniversalSBATechnicians group at the branch site will add this device to the domain later.

6. Click **OK** to save the Survivable Branch Appliance computer object.
7. Click **Start**, click **Administrative Tools**, and then click **ADSI Edit**.
8. In **ADSI Edit**, right-click the computer object that you created in the previous steps, and then click **Properties**.
9. In the attribute list, click **servicePrincipalName**, and then click **Edit**.
10. In the **Value to add** field, type HOST/<SBA FQDN> where <SBA FQDN> is the fully qualified domain name (FQDN) of your Survivable Branch Appliance. For example, type **HOST/BranchOffice1.contoso.com**.
11. Click **OK** to save the **servicePrincipalName** attribute setting, and then click **OK** to save the computer object properties.
12. In **Active Directory Users and Computers**, right-click **Users**, click **New**, and then click **User**.
13. Enter information into the wizard to create a domain user account for a Survivable Branch Appliance technician.
14. In **Active Directory Users and Computers**, click **Users**, right-click the user object, and then click **Add to a group**.
15. In **Enter the object names to select**, type **RTCUniversalSBATechnicians**, and then click **OK**.
16. Repeat Steps 12-15 for each branch site technician.

Next step: Add Branch Sites to Your Topology

1.4.8.2.1.2 Add Branch Sites to Your Topology

Add Branch Sites to Your Topology

Deployment > Deploying Branch Sites > Providing PSTN Connectivity at a Branch Site >

Topic Last Modified: *2012-10-05*

Branch sites represent physical branch offices that are connected to your main offices over a WAN link. To add a branch site to your Lync topology, perform this procedure at the central site.

⊟To add branch sites to your topology

1. Click **Start**, click **All Programs**, click **Microsoft Lync Server**, and then click **Lync Server Topology Builder**.
2. In the console tree, expand the central site, right-click **Branch Sites**, and then click **New Branch Site**.
3. In the **Define New Branch Site** dialog box, click **Name**, and then type the name of the branch site.
4. (Optional) Click **Description**, and then type a meaningful description for the branch site.
5. Click **Next**.
6. (Optional) In the next **Define New Branch Site** dialog box, do any of the following:
   - Click **City**, and then type the name of the city in which the branch site is located.
   - Click **State/Region**, and then type the name of the state or region in which the branch site is located.
   - Click **Country Code**, and then type the two-digit calling code for the

country/region in which the branch site is located.

7. Click **Next**, and then do one of the following:
    - If you are using a Survivable Branch Appliance or Server at this site, be sure that the **Open the New Survivable Wizard when this wizard closes** check box is selected, click **Finish**, and then follow the directions in the wizard that opens. For information about wizard items, see Define a Survivable Branch Appliance or Server.
    - If you are not using a Survivable Branch Appliance or Server at this site, clear the **Open the New Survivable Wizard when this wizard closes** check box, and then click **Finish**.
8. Repeat the previous steps for each branch site that you want to add to the topology.

Next step:

For Survivable Branch Appliances or Servers: Define a Survivable Branch Appliance or Server

For non-resilient PSTN connectivity: Define a PSTN Gateway for a Branch Site, Configure a Trunk with Media Bypass, or Configure a Trunk without Media Bypass

1.4.8.2.1.3 Define a Survivable Branch Appliance or Server

Define a Survivable Branch Appliance or Server

Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server > Deploying a Survivable Branch Appliance or Server - Central Site Tasks >

Topic Last Modified: *2012-10-07*

Perform this procedure at the central site if you did not define the Survivable Branch Appliance or Server when you added it to your topology.

⊟To define a Survivable Branch Appliance or Survivable Branch Server

1. Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In the console tree, expand the central site, expand **Branch sites**, and then expand the name of the branch site where you plan to deploy the Survivable Branch Appliance or Survivable Branch Server.
3. Right-click **Survivable Branch Appliances**, and then click **New Survivable Branch Appliance**.

    Important:

    Survivable Branch Appliances is where you define Survivable Branch Servers and Survivable Branch Appliances.

4. In the **Define Survivable Branch Appliance** dialog box, click **FQDN**, type the fully qualified domain name (FQDN) of the Survivable Branch Appliance or Survivable Branch Server you will deploy at this branch site, and then click **Next**.

    Important:

    If you are defining a Survivable Branch Appliance, the name you enter in **FQDN** must be the same as the Survivable Branch Appliance FQDN you assigned to the **servicePrincipalName** attribute. For details, see Add a Survivable Branch Appliance to Active Directory.

5. Click **Front End pool**, click the Front End Server (User Services pool) at the central site that this Survivable Branch Appliance or Survivable Branch Server will connect to, and then click **Next**.

6. Click **Edge Server**, click the Edge pool that this Survivable Branch Appliance or Survivable Branch Server will connect to provide PSTN connectivity to remote users of the branch site, and then click **Next**.
7. Click **Gateway FQDN or IP Address**, and then type the FQDN or IP address of the gateway peer that the Survivable Branch Appliance or Survivable Branch Server is associated with for routing inbound or outbound PSTN calls.

   Important:

   If you are defining a Survivable Branch Appliance, this is the gateway to which the Mediation Server inside the Survivable Branch Appliance will connect for PSTN connectivity.

8. Click **Listening Port for IP/PSTN Gateway**, and then accept the default port.
9. In **Sip Transport Protocol**, click the transport protocol the Survivable Branch Appliance or Survivable Branch Server will use, and then click **Finish**.

   Note:

   For security reasons, we strongly recommend that you use Transport Layer Security (TLS). If you are defining a Survivable Branch Appliance, refer to your Survivable Branch Appliance vendor documentation to verify that your Survivable Branch Appliance supports the TLS protocol.

10. In the console tree, right-click the new Survivable Branch Appliance or Server, click **Topology**, and then click **Publish**.

Next step: Deploy a Survivable Branch Appliance or Server - Branch Site Task

1.4.8.2.2 Deploy a Survivable Branch Appliance or Server - Branch Site Task

Deploy a Survivable Branch Appliance or Server - Branch Site Task

See Also

Deployment > Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server >

Topic Last Modified: *2012-09-22*

Perform one of the two procedures described in this topic at the branch site, after successfully completing the tasks in Deploying a Survivable Branch Appliance or Server - Central Site Tasks.

Important:

To perform this procedure, you must be a member of the RTCUniversalSBATechnicians group.

⊟To deploy the Survivable Branch Appliance

- Survivable Branch Appliance deployment is enabled by the Survivable Branch Appliance vendor through a web user interface (UI). For information about deploying the Survivable Branch Appliance, see your Survivable Branch Appliance vendor documentation.

⊟To deploy the Survivable Branch Server

- Install Microsoft Lync Server 2010 on a computer running Windows Server 2008 or Windows Server 2008 R2, just as you would install any other Lync Server 2013 server role.

  Note:

  For information about installing Lync Server, see Deploying Lync Server 2013 in the Deployment documentation.

Next step: Configuring Users for Branch Site Resiliency

Tasks

Appendix A: Using Cmdlets to Deploy a Survivable Branch Appliance

1.4.8.2.3 Configuring Users for Branch Site Resiliency

Configuring Users for Branch Site Resiliency

Deployment > Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server >

Topic Last Modified: *2012-10-11*

After successfully completing the tasks in Deploy a Survivable Branch Appliance or Server - Branch Site Task, perform the following procedures to enable users for Enterprise Voice, assign them a voice policy and voice mail settings. Then in Home Users on a Survivable Branch Appliance or Server, you will home these users on the Survivable Branch Appliance or Server.

- Enable Users for Enterprise Voice
- Create the VoIP Routing Policy for Branch Users
- Configure Voice Mail Rerouting Settings

1.4.8.2.3.1 Enable Users for Enterprise Voice

Enable Users for Enterprise Voice

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-11-01*

After you install files for one or more Mediation Servers, configure outbound call routing, and optionally deploy one or more advanced Enterprise Voice features, you can use the following procedures to enable a user to make calls by using Enterprise Voice:

Note:
Of the following procedures, only the first can be performed by using Lync Server Control Panel. For the remaining procedures, you can use only Lync Server Management Shell.

- Enable the user account for Enterprise Voice.
- (Optional) Assign the user account a user-specific voice policy.
- (Optional) Assign the user account a user-specific dial plan.

To enable a user account for Enterprise Voice

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to enable, and then click **Find**.
5. In the table, click the user account that you want to enable for Enterprise Voice.

6. On the **Edit** menu, click **Show details**.
7. On the **Edit Lync Server User** page, under **Telephony**, click **Enterprise Voice**.
8. Click **Line URI**, and then type a unique, normalized phone number (for example, tel:+14255550200).
9. Click **Commit**.

To finish enabling a user for Enterprise Voice, be sure that the user is assigned a voice policy and a dial plan, whether global (assigned by default) or user-specific.

By default, all users are assigned a global voice policy and dial plan. If a voice policy or dial plan exists at the site level for the site on which the user account is homed, those site policies will automatically apply to the user. To apply a per-user voice policy or dial plan to a user, you must run the **Grant-CsVoicePolicy** and **Grant-CsDialPlan** cmdlets. For details, see the Lync Server Management Shell documentation.

Voice Policy Assignment

Global and site-level voice policies are automatically assigned to all user accounts that are enabled for Enterprise Voice. You can also create voice policies that apply to specific users or groups. These per-user policies must be explicitly assigned to the users or groups. If you want to use the global or site voice policy for all users who are enabled for Enterprise Voice, you can skip this section and continue to Dial Plan Assignment section later in this topic.

To assign a user-specific voice policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. To assign an existing user voice policy to a user, run the following at the command prompt:

```
Grant-CsVoicePolicy -Identity <UserIdParameter> -PolicyName <String>
```

   For example:

```
Grant-CsVoicePolicy -Identity "Bob Kelly" -PolicyName VoicePolicyJapar
```

   In this example, the user with the display name Bob Kelly is assigned the voice policy with the name **VoicePolicyJapan**.

For details about assigning a user-specific voice policy or about running the **Grant-CsVoicePolicy** cmdlet, see the Lync Server Management Shell documentation.

Dial Plan Assignment

To complete user account configuration for either users of Enterprise Voice or users of dial-in conferencing, the user must be assigned a dial plan. User accounts will automatically use the global dial plan or, if one exists, the site-level dial plan, when you do not explicitly assign an existing per-user dial plan. If you want to use the global or site dial plan for all users who are enabled for Enterprise Voice, you can skip this section.

To assign a dial plan

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management**

Shell.

3. To assign a user-specific dial plan, run the following at the command prompt:

```
Grant-CsDialPlan -Identity <UserIdParameter> -PolicyName <String>
```

For example:

```
Grant-CsDialPlan -Identity "Bob Kelly" -PolicyName DialPlanJapan
```

In this example, the user with the display name Bob Kelly is assigned the user dial plan with the name **DialPlanJapan**.

For details about assigning a user dial plan or about running the **Grant-CsDialPlan** cmdlet, see the Lync Server Management Shell documentation.

⊟See Also

Tasks

Disable a User for Enterprise Voice

1.4.8.2.3.2 Create the VoIP Routing Policy for Branch Users

Create the VoIP Routing Policy for Branch Users

Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server > Configuring Users for Branch Site Resiliency >

Topic Last Modified: *2012-09-23*

We recommend creating a separate voice over IP (VoIP) policy for users at branch sites. This policy should contain routes to egress from the Survivable Branch Appliance gateway or the Survivable Branch Server external gateway and backup routes to egress from a gateway at the central site. Regardless of where the user is registered, either on the Registrar on the Survivable Branch Appliance or Survivable Branch Server or on the backup Registrar cluster at the central site, the user’s VoIP policy is always in effect.

⊟To configure the VoIP routing policy for branch users

1. Create a user-level dial plan and assign it to branch users. (See Create a Dial Plan in the Operations documentation.)
2. Assign normalization rules corresponding to the dialing habits of users at that site. If the Survivable Branch Appliance or Survivable Branch Server user fails over to the backup Registrar pool at the central site, the same dial plan will be in effect. (See Create a Dial Plan in the Operations documentation.)
3. Configure a voice route that egresses from the Survivable Branch Appliance gateway or the Survivable Branch Server external gateway. (See Create a Voice Route in the Operations documentation.)
4. Set a backup call route on the Survivable Branch Appliance or Survivable Branch Server gateway to point to the backup Registrar pool (collocated with Mediation Server) at the central site. (See your Survivable Branch Appliance or Survivable Branch Server vendor documentation.)

> **Note:**
>
> This backup call route setup helps ensure that inbound calls to the branch user will work when the Survivable Branch Appliance or Survivable Branch Server is not available (for example, if it is down for maintenance). If the Registrar and Mediation Server on the Survivable Branch Appliance or Survivable Branch Server are not available, and the user is registered with the backup Registrar pool at the central site, inbound calls can still be routed to the user.

Next step: Configure Voice Mail Rerouting Settings

1.4.8.2.3.3 Configure Voice Mail Rerouting Settings

Configure Voice Mail Rerouting Settings

Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server > Configuring Users for Branch Site Resiliency >

Topic Last Modified: *2012-10-18*

Survivable Branch Appliances and Survivable Branch Servers can provide voice mail survivability for branch users during a WAN outage, if Exchange Unified Messaging (UM) is installed at the central site and an Exchange UM Message Auto Attendant (AA) is deployed. We recommend that your Exchange administrator configure the AA to accept messages only, which disables other generic functionality, such as transfer to a user or transfer to an operator. Alternatively, you might use a generic AA or an AA customized to route the call.

For details, see the “Preparing for Voice Mail Survivability” section of Branch-Site Resiliency Requirements in the Planning documentation.

⊟To configure voice mail survivability

1. Ask your Exchange administrator to configure the AA to accept messages only (in the Exchange Shell use the following cmdlet: **Set-UMAutoAttendant <AA name> -CallSomeoneEnabled $false**. The parameter that specifies to allow leaving messages (*SendVoiceMsgEnabled*) is true by default.
2. In the Lync Server Management Shell, use the **New-CSVoiceMailReroutingConfiguration** cmdlet to set the AA phone number as the Exchange UM Auto Attendant phone number in the voice mail rerouting configuration on the Survivable Branch Appliance or Survivable Branch Server.

   Note:
   If you need to modify the voice mail rerouting setting later, use the **Set-CsVoiceMailReRoutingConfiguration** cmdlet to do so. For details, about **New-** and **Set-CSVoiceMailReroutingConfiguration**, in the Shell Help topics.

3. Set the Exchange UM subscriber access number that corresponds to the branch user’s Exchange UM dial plan as the Exchange UM subscriber access number in the voice mail rerouting configuration on the Survivable Branch Appliance or Survivable Branch Server.

   Note:
   Configure the Exchange UM users’ dial plan so that there is only one dial plan associated with all branch users who need access to the Get Voice Mail functionality during a WAN outage.

Next step for Survivable Branch Appliances or Survivable Branch Servers: Home Users on a Survivable Branch Appliance or Server.

1.4.8.2.4 Home Users on a Survivable Branch Appliance or Server

Home Users on a Survivable Branch Appliance or Server

See Also

Deployment > Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server >

***Topic Last Modified:** 2012-09-21*

The process of homing users on a Survivable Branch Appliance or a Survivable Branch Server is similar to the process of homing users on a Front End pool. Perform the Survivable Branch Appliance or Survivable Branch Server procedure at the central site.

⊟To home users on Survivable Branch Appliance or Survivable Branch Server

1. Before moving users to the Survivable Branch Server or Survivable Branch Server, open the Lync Server Management Shell, and then do all of the following:
   - Run the cmdlet **Test-CsPstnOutboundCall** to verify that the Survivable Branch Server is running and that the public switched telephone network (PSTN) connectivity is configured. If you need to modify PSTN gateway properties, use the cmdlet **Set-CsPstnGateway**.
   - Run the cmdlet **Get-CsVoicePolicy** to verify that the users who will be homed on the Survivable Branch Server have the appropriate VoIP routing policy. If you need to modify the VoIP policy, use the cmdlet **Set-CsVoicePolicy**.
   - Run the cmdlet **Get-CsVoicemailReroutingConfiguration** to verify that the voice mail rerouting settings are configured. If you need to modify the voice mail rerouting settings, use the cmdlet **Set-CsVoicemailReroutingConfiguration**.
2. In the Lync Server Management Shell, run the cmdlet **Move-CsUser** to move home users.

Note:
You can also use Lync Server Control Panel to verify prerequisites and home users.

Other Resources

Test-CsPstnOutboundCall
Get-CsVoicePolicy
Get-CsVoicemailReroutingConfiguration
Move-CsUser

1.4.8.2.5 Connecting Survivable Branch Appliance to Lync Server 2013 Front End pool

Connecting Survivable Branch Appliance to Lync Server 2013 Front End pool

Deployment > Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server >

***Topic Last Modified:** 2012-10-05*

Every Survivable Branch Appliance (SBA) is associated with a Front End pool, which serves as a backup Registrar for the SBA. When the Front End pool is upgraded to Lync Server 2013, the SBA must be disassociated from the Front End pool while the Front End pool is upgraded. After the Front End pool is upgraded, the SBA can be reassociated with the Front End pool. This involves deleting the SBA from the topology in Topology Builder and then adding the SBA, again, to Topology Builder. Users homed on the SBA must be moved to another Front End pool before removing the SBA from the topology. After the SBA is added back to the topology, those users can be moved back to the SBA.

These steps are summarized below:

1. Move branch users homed on SBA to another Front End pool.
2. Remove SBA from your topology to disassociate the existing Front End pool as the backup Registrar.

3. Upgrade Front End pool to Microsoft Lync Server 2013.
4. Add SBA back into your topology.
5. Associate the new Front End pool to the SBA as a backup Registrar.
6. Move branch users back to the SBA.

- Add Lync Server 2013 Survivable Branch Appliance branch site to your Topology
- Add Lync Server 2010 Survivable Branch Appliance branch site to your Topology

1.4.8.2.5.1 Add Lync Server 2013 Survivable Branch Appliance branch site to your Topology

Add Lync Server 2013 Survivable Branch Appliance branch site to your Topology

See Also

Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server > Connecting Survivable Branch Appliance to Lync Server 2013 Front End pool >

Topic Last Modified: *2012-10-07*

Microsoft Lync Server 2013 Survivable Branch Appliances (SBA) cannot be associated to a Microsoft Lync Server 2010 Front End pool as a backup Registrar. The SBA must be associated with a Microsoft Lync Server 2013 Front End pool. These steps assume a Microsoft Lync Server 2013 SBA. Perform this procedure at the central site.

⊟To add branch sites with Microsoft Lync Server 2013 SBA to your topology

1. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
2. In the console tree, expand the central site, expand **Branch Sites**, and then click **New Branch Site**.
3. In the **Define New Branch Site** dialog box, click **Name**, and then type a name for the new branch site.
4. (Optional) Click **Description**, and then type a meaningful description for the branch site.
5. Click **Next**.
6. (Optional) In the next **Define New Branch Site** dialog box, do any of the following:
   - Click **City**, and then type the name of the city in which the branch site is located.
   - Click **State/Region**, and then type the name of the state or region in which the branch site is located.
   - Click **Country Code**, and then type the two-digit calling code for the country/region in which the branch site is located.
7. Click **Next**, and then do one of the following:
   - If you are using a Survivable Branch Appliance or Survivable Branch Server at this site, be sure that the **Open the New Survivable Wizard when this wizard closes** check box is selected.
   - If you are not using a Survivable Branch Appliance or Survivable Branch Server at this site, clear the **Open the New Survivable Wizard when this wizard closes** check box.
   - Click **Finish**, and then follow the directions in the wizard that opens. For information about wizard items, see Define a Survivable Branch Appliance or Server.
8. Repeat the previous steps for each branch site that you want to add to the topology.

Tasks

Define a Survivable Branch Appliance or Server

Define a PSTN Gateway for a Branch Site
Configure a Trunk with Media Bypass
Configure a Trunk without Media Bypass

1.4.8.2.5.2 Add Lync Server 2010 Survivable Branch Appliance branch site to your Topology

Add Lync Server 2010 Survivable Branch Appliance branch site to your Topology

See Also

Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server > Connecting Survivable Branch Appliance to Lync Server 2013 Front End pool >

Topic Last Modified: *2012-10-07*

Microsoft Lync Server 2010 Survivable Branch Appliances (SBA) can be associated to a Microsoft Lync Server 2013 Front End pool as a backup Registrar. Refer to the Migration section, Connect a Survivable Branch Appliance, for detailed procedures on how to connect your Microsoft Lync Server 2010 SBA to a Microsoft Lync Server 2013 Front End pool.

Tasks

Define a Survivable Branch Appliance or Server
Define a PSTN Gateway for a Branch Site
Configure a Trunk with Media Bypass
Configure a Trunk without Media Bypass

Concepts

Connect a Survivable Branch Appliance

1.4.8.2.6 Appendices: Survivable Branch Appliances and Servers

Appendices: Survivable Branch Appliances and Servers

Deployment > Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server >

Topic Last Modified: *2012-06-28*

The section provides additional information about Survivable Branch Appliances and Survivable Branch Servers.

- Appendix A: Using Cmdlets to Deploy a Survivable Branch Appliance
- Appendix B: Managing a Survivable Branch Appliance

1.4.8.2.6.1 Appendix A: Using Cmdlets to Deploy a Survivable Branch Appliance

Appendix A: Using Cmdlets to Deploy a Survivable Branch Appliance

Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server > Appendices: Survivable Branch Appliances and Servers >

Topic Last Modified: *2012-10-07*

This topic describes how to deploy a Survivable Branch Appliance using the Lync Server Management Shell. Perform this procedure at the central site.

To deploy a Survivable Branch Appliance remotely

1. Follow the procedure in Add Branch Sites to Your Topology to add a new branch site.
2. Join the branch site to the domain.
3. Add the RTCUniversalSBATechnicians group to the local Administrators group.
4. Restart the server, and log on to it as a member of the RTCUniversalSBATechnicians group.
5. In the Lync Server Management Shell, type the following commands, replacing the placeholders with the correct information for your organization:

```
Export-CsConfiguration -FileName C:\CSConfig.zip
Import-CsConfiguration -LocalStore -FileName C:\CSConfig.zip -Verbose
Enable-CSReplica -Verbose
Enable-CsComputer -Verbose
Request-CsCertificate -New -Type default -CA <YourCA> -Verbose
Set-CsCertificate -Type Default -Thumbprint <YourCertThumbprint>
Start-cswindowsservice -verbose
```

1.4.8.2.6.2 Appendix B: Managing a Survivable Branch Appliance

Appendix B: Managing a Survivable Branch Appliance

Deploying Branch Sites > Deploying a Survivable Branch Appliance or Server > Appendices: Survivable Branch Appliances and Servers >

Topic Last Modified: *2012-10-18*

This topic describes the procedures for managing a Survivable Branch Appliance. Specifically, how to replace and rename a Survivable Branch Appliance, and how to change the Lync Server 2013 Front End pool that the Survivable Branch Appliance is associated with.

To Replace a Survivable Branch Appliance

1. Stop all Lync Server 2013 services on the Survivable Branch Appliance. (See the Survivable Branch Appliance vendor documentation.)
2. (Recommended) Remove the Survivable Branch Appliance from the domain.
3. Delete the Survivable Branch Appliance computer object in Active Directory Domain Services (AD DS), by following these steps:
    - Log on to a member server as a member of the Enterprise Admins group.
    - Click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**.
    - Right-click the Survivable Branch Appliance object, and click **Delete**.
4. Add the Survivable Branch Appliance computer object again. (See Add a Survivable Branch Appliance to Active Directory.)
5. Wait for Active Directory replication to take place.
6. Open the Lync Server Management Shell, and type **Enable-CSTopology**.
7. Connect the new Survivable Branch Appliance to the network, and follow the steps in Deploying a Survivable Branch Appliance or Server - Central Site Tasks and Deploy a Survivable Branch Appliance or Server - Branch Site Task.

To Rename a Survivable Branch Appliance

1. Move users to the central site. For details, see Move Users to Another Pool.
2. Stop all Lync Server 2013 services on the Survivable Branch Appliance. (See the Survivable Branch Appliance vendor documentation.)
3. Remove the Survivable Branch Appliance from the topology, by following these steps:
    - Click **Start**, click **All Programs**, click **Microsoft Lync Server**, and then click

Lync Server Topology Builder.
- In the console tree, expand **Branch Sites**, click the Survivable Branch Appliance, and then click **Delete** on the Action pane.

4. Remove the Survivable Branch Appliance from the domain.
5. Delete the Survivable Branch Appliance computer object in Active Directory, by following these steps:
   - Log on to a domain controller as a member of the Enterprise Admins group.
   - Click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**.
   - Right-click the Survivable Branch Appliance object, and click **Delete**.
6. Restore the Survivable Branch Appliance to factory defaults. (See the Survivable Branch Appliance vendor documentation.)
7. Follow the steps in Deploying a Survivable Branch Appliance or Server - Central Site Tasks and Deploy a Survivable Branch Appliance or Server - Branch Site Task.
8. Move users to the renamed Survivable Branch Appliance. For details, see Move Users to Another Pool.

⊟To Change the Lync Server Front End Pool that the Survivable Branch Appliance Is Associated With

1. Move users from the Survivable Branch Appliance to the Lync Server Front End pool at the central site. For details, see Move Users to Another Pool.
2. Stop all Lync Server services on the Survivable Branch Appliance. (See the Survivable Branch Appliance vendor documentation).
3. Update the Lync Server Front End pool that the Survivable Branch Appliance is associated with, by following these steps:
   - Click **Start**, click **All Programs**, click **Microsoft Lync Server**, and then click **Lync Server Topology Builder**.
   - Expand **Branch Sites**.
   - Right-click the Survivable Branch Appliance object to modify, and click **Edit Properties**
   - Under Resiliency, select the new Front End pool the Survivable Branch Appliance is to be associated to, and then click **Next**.
   - In the console tree, right-click the new Survivable Branch Appliance, click **Topology**, and then click **Publish**.
4. Restart all Lync Server Services on the Survivable Branch Appliance.
5. Test the Survivable Branch Appliance. For details, see Home Users on a Survivable Branch Appliance or Server.
6. Move users from the Lync Server Front End pool at the central site to the Survivable Branch Appliance.

1.4.9 Deploying Persistent Chat Server

Deploying Persistent Chat Server

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-10-11*

Lync Server 2013, Persistent Chat Server is part of the Lync Server 2013 infrastructure.

Deploying Persistent Chat Server requires that you:
- Use Topology Builder to define, or import, and subsequently publish your topology and the components that you want to deploy.
- Prepare your environment for deploying Persistent Chat Server components.
- Install and configure Persistent Chat Server components for your deployment.

Persistent Chat Server is available with Lync Server 2013 Enterprise Edition as a separate pool (not collocated with the Enterprise Edition Front End Servers). Persistent Chat Server requires a SQL Server Back End Server in your Enterprise Edition pool to store the chat room content and other relevant metadata. We recommend that you install the **PersistentChatStore** on a dedicated SQL Server Back End Server, although collocating Lync Server 2013 Back End Server and **PersistentChatStore** on the same SQL Server instance is supported.

Persistent Chat Server can also be deployed with Lync Server 2013 Standard Edition. In this case, the **PersistentChatService** Front End Server is collocated on the Standard Edition computer, and the **PersistentChatStore** Back End Server can be deployed on the local SQL Server Express instance.

Important:
We do not support high availability for Persistent Chat Server Standard Edition. Performance and scale will be limited. Furthermore, we support only new Persistent Chat Server Standard Edition server. We do not support upgrading Lync Server 2010, Group Chat Server to a Lync Server 2013 Persistent Chat Server Standard Edition.

If your organization requires compliance support, you can install the Persistent Chat Server Compliance service on the Persistent Chat Server Front End Server. A separate database is required for compliance.

At a minimum, each topology requires a server with Lync Server 2013 installed and a server with SQL Server database software installed.

Use Topology Builder to add Persistent Chat Server to your Lync Server 2013 deployments. You can choose to add one or more Persistent Chat Server pools using Topology Builder. Follow the same deployment instructions for deploying multiple Persistent Chat Server pools as you would for any pool. For details, see Deploying Lync Server 2013 in the Deployment documentation.

For details about available topologies and the technical and software requirements for installing Persistent Chat Server, see Planning for Persistent Chat Server in the Planning documentation, How Persistent Chat Server Works in the Planning documentation, Deployment documentation, or Operations documentation, and Supported Hardware in the Supportability documentation.

For details about acquiring certificates, creating the SQL Server database, and creating file stores, see Deploying Lync Server 2013 in the Deployment documentation.

A single Persistent Chat Server Front End Server can support 20,000 active users. You can have a Persistent Chat Server pool with up to 4 active Front End Servers supporting a total of 80,000 concurrent users.

Persistent Chat Server is also supported on a virtual server. The virtual server can support up to 20,000 concurrent users if it matches the specifications of the physical server. We recommend four-core processors and 8 GB of memory.

Important:
Persistent Chat Server must be installed on an NTFS file system to help enforce file system security. FAT32 is not a supported file system for Persistent Chat Server.

In This Section

- How Persistent Chat Server Works
- Deployment Checklist for Persistent Chat Server
- Technical Requirements for Persistent Chat Server
- Setting Up Systems and the Infrastructure for Persistent Chat Server

- Adding Persistent Chat Server to Your Deployment
- Installing Persistent Chat Server
- Adding a Persistent Chat Administrator
- Configuring Persistent Chat Server
- Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets
- Troubleshooting Persistent Chat Server Configuration using Windows PowerShell Cmdlets
- Configuring Persistent Chat Server for High Availability and Disaster Recovery
- Failing Over and Failing Back Persistent Chat Server

1.4.9.1 How Persistent Chat Server Works

How Persistent Chat Server Works

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

***Topic Last Modified:** 2012-11-21*

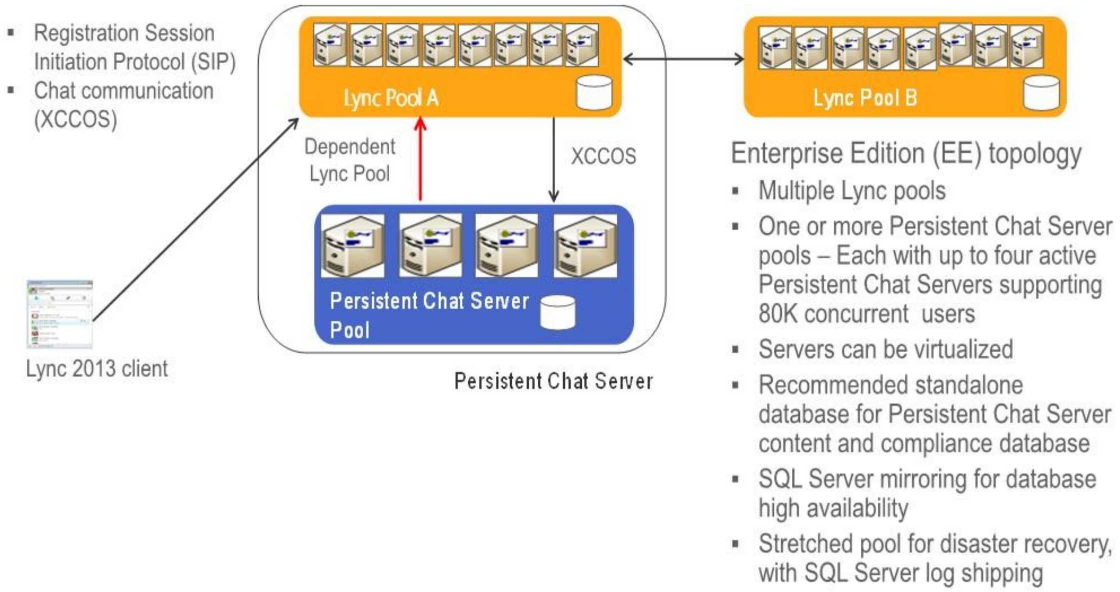
Lync Server 2013, Persistent Chat Server enables you to participate in multiparty, topic-based conversations that persist over time. Persistent Chat Server can help your organization do the following:

- Improve communication between geographically dispersed and cross-functional teams
- Broaden information awareness and participation
- Improve communication with your extended organization
- Reduce information overload
- Improve information awareness
- Increase dispersion of important knowledge and information

You can deploy Persistent Chat Server as an optional role with Lync Server 2013. Persistent Chat services run on a dedicated pool, and a Persistent Chat Server pool depends on a Lync Server pool to route messages to it. Clients use eXtensible Chat Communication Over SIP (XCCOS). The Lync Server Front End Servers are configured to route the traffic to a Persistent Chat Server pool.

High-Level Architecture

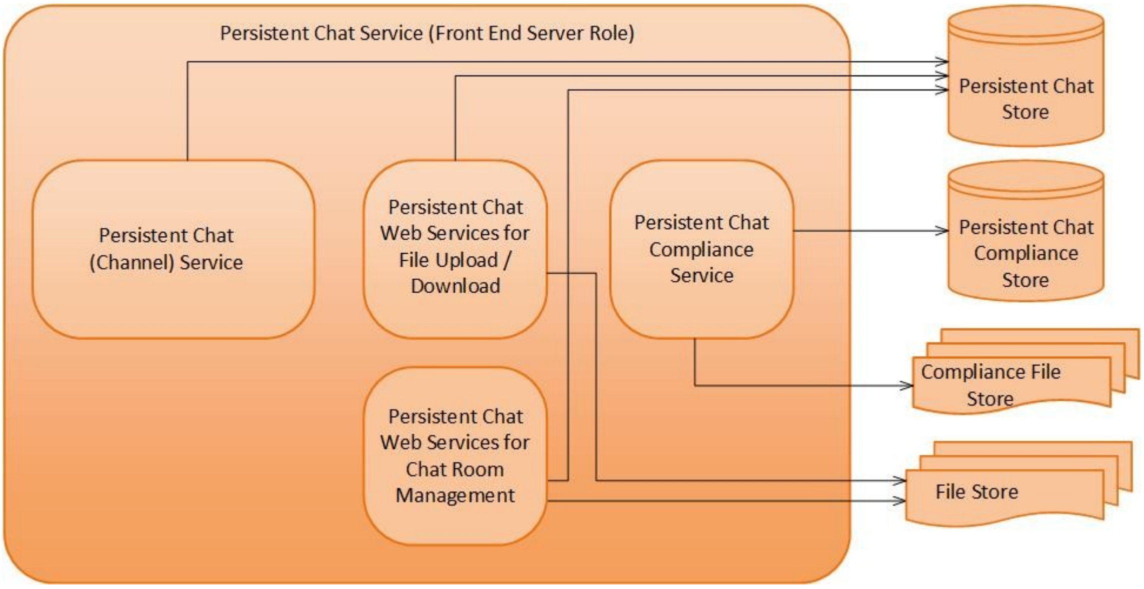
The following diagrams provide high-level perspectives of the Persistent Chat Server architecture and services.



- Registration Session Initiation Protocol (SIP)
- Chat communication (XCCOS)

Enterprise Edition (EE) topology

- Multiple Lync pools
- One or more Persistent Chat Server pools – Each with up to four active Persistent Chat Servers supporting 80K concurrent users
- Servers can be virtualized
- Recommended standalone database for Persistent Chat Server content and compliance database
- SQL Server mirroring for database high availability
- Stretched pool for disaster recovery, with SQL Server log shipping



Persistent Chat Service (Front End Server Role)
Persistent Chat (Channel) Service
Persistent Chat Web Services for File Upload / Download
Persistent Chat Compliance Service
Persistent Chat Web Services for Chat Room Management
Persistent Chat Store
Persistent Chat Compliance Store
Compliance File Store
File Store

Two services run on the Persistent Chat Server Front End Servers:

- Persistent Chat (Channel)
- Compliance

Persistent Chat (Channel) Service

The Persistent Chat (Channel) service is the core service responsible for Persistent Chat Server. This service provides the following functions:

- Accepts incoming messages
- Registers and lists online participants within a Persistent Chat room
- Retransmits messages to other channel subscribers
- Implements logic for channel management, chat room invitation, search, and new content notifications

The Persistent Chat (Channel) service stores and accesses chat room content and other system metadata (authorization rules, and so on) by using the Persistent Chat Store. This service stores files that are uploaded into chat rooms in the Persistent Chat File Store.

Compliance Service

The Compliance service is an optional component of Persistent Chat Server and is responsible for archiving chat content and events to the Persistent Chat Compliance Store. If your organization has regulations that require Persistent Chat activity to be archived, you can deploy the optional Persistent Chat Compliance service. The Compliance service is installed on each Persistent Chat Server in a Persistent Chat pool. When configured, Persistent Chat Server compliance records user activity such as joining and leaving rooms, and posting and reading of messages. The Compliance service stores files that need to be archived in the Persistent Chat Compliance File Store.

Persistent Chat Web Services

On the Lync Server Front End Servers, two services run that depend on Internet Information Services (IIS), and are implemented as web components:

- **Persistent Chat Web Services for File Upload/Download** Responsible for posting and retrieving files from chat rooms.
- **Persistent Chat Web Services for Chat Room Management** Responsible for providing users the ability to manage their chat rooms, and create new chat rooms.

How Do I Start Using Persistent Chat Server?

Persistent Chat Server is an optional server role within the Lync Server 2013 infrastructure. If you install the Persistent Chat Server role, any users who have been enabled through policy by an administrator can use Persistent Chat with the Lync 2013 client.

For details about how to deploy Persistent Chat Server and enable users to leverage the capabilities by policy, see Deploying Persistent Chat Server.

For details about how to configure settings on your Persistent Chat Server deployment, see Deploying Persistent Chat Server and Managing Lync Server 2013, Persistent Chat Server.

For details about how to enable users by policy such that they can leverage Persistent Chat functionality in Lync 2013 client, see Deploying Persistent Chat Server and Managing Lync Server 2013, Persistent Chat Server.

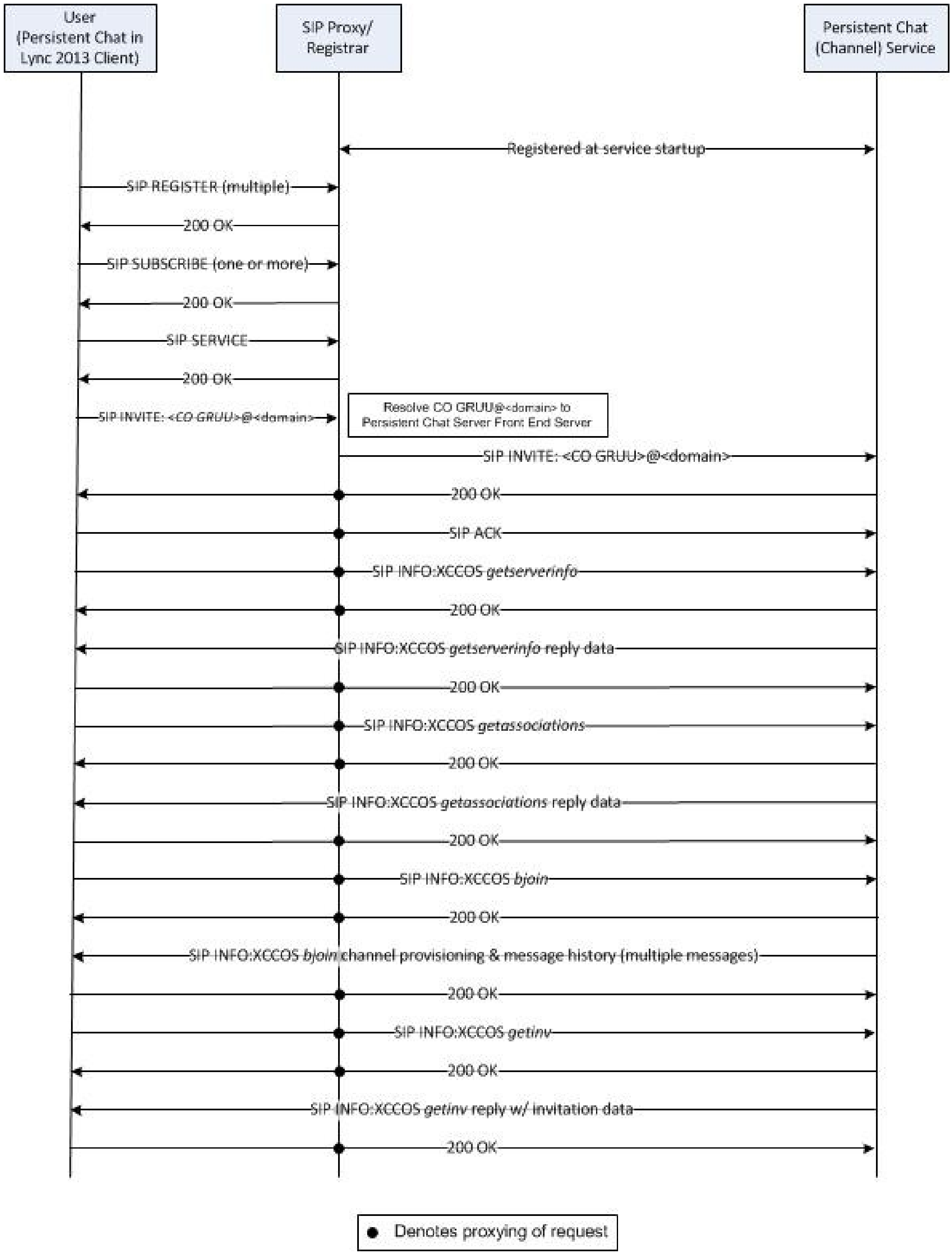
If you deployed Persistent Chat compliance, see Managing Lync Server 2013, Persistent Chat Server for details about how to configure settings for compliance.

Persistent Chat Call Flows

The Persistent Chat client communicates with the Persistent Chat service by using XCCOS. The following sequences describe the sign-in process and a typical room subscription and message post scenario.

Sign-in

The following call flow diagram and steps describe the sign-in process.


User (Persistent Chat in Lync 2013 Client)
SIP Proxy/ Registrar
Persistent Chat (Channel) Service
Registered at service startup
SIP REGISTER (multiple)
200 OK
SIP SUBSCRIBE (one or more)
200 OK
SIP SERVICE
200 OK
SIP INVITE: <CO GRUU>@<domain>
Resolve CO GRUU@<domain> to Persistent Chat Server Front End Server
SIP INVITE: <CO GRUU>@<domain>
200 OK
SIP ACK
SIP INFO:XCCOS getserverinfo
200 OK
SIP INFO:XCCOS getserverinfo reply data
200 OK
SIP INFO:XCCOS getassociations
200 OK
SIP INFO:XCCOS getassociations reply data
200 OK
SIP INFO:XCCOS bjoin
200 OK
SIP INFO:XCCOS bjoin channel provisioning & message history (multiple messages)
200 OK
SIP INFO:XCCOS getinv
200 OK
SIP INFO:XCCOS getinv reply w/ invitation data
200 OK
● Denotes proxying of request

1. The Persistent Chat client first sends a SIP SUBSCRIBE to retrieve the in-band provisioning document from the server. This document indicates if Persistent Chat is enabled or disabled for the user and the list of SIP URIs for the Persistent Chat Server pool.
2. The Persistent Chat client sends a SIP INVITE message to the SIP URI of the Persistent Chat Server that it obtained in the previous step. The INVITE sequence is followed by 200 OK and ACK, and the Persistent Chat client has

now opened a SIP session with a Persistent Chat Server endpoint. Consequently, the Persistent Chat client communicates with Persistent Chat Server by sending SIP INFO messages that contain either chat messages or commands requesting the server to take an action. All of these messages are acknowledged with either 200 OK or 503 Service Unavailable (that is, in the event of heavy server load). If the client receives a 503 response, it will retry the message. (This example does not include a 503 response.) If the server accepts the message or command and sends 200 OK, it provides a response to the client in the form of a separate SIP INFO message. This response includes a reference to the originating command.

3. The Persistent Chat client sends a SIP INFO message that contains the XCCOS **getserverinfo** command. Persistent Chat Server replies with a new SIP INFO message that contains information about the Persistent Chat service configuration.
4. The Persistent Chat client sends a SIP INFO message that contains the XCCOS **getassociations** command. Persistent Chat Server replies with a new SIP INFO message that contains the list of rooms of which the user is a member. The Persistent Chat client repeats the command to retrieve the list of rooms of which the user is a manager.
5. The Persistent Chat client gets the list of followed rooms from the "presence" document, where each followed room is represented by a "roomSetting" category. All followed rooms are joined by a single SIP INFO message that contains the XCCOS **bjoin** command that contains the list of room URIs. Because the list of followed rooms is kept on the server, any client on any computer has the same list of followed rooms for the specified user URI. The Persistent Chat client also keeps the list of opened rooms (if this option is enabled by the user) in the local computer registry, and joins each of these rooms at sign-in by sending a SIP INFO message that contains the XCCOS **join** command for each opened room. Because this list is kept in the registry, it can be different on two Persistent Chat clients running on different computers.
6. For each room joined, the Persistent Chat client sends a SIP INFO message that contains the XCCOS **bccontext** command. Persistent Chat Server replies with a new SIP INFO message that contains the most recent chat message in the room.
7. The Persistent Chat client sends a SIP INFO message that contains a XCCOS **getinv** (that is, get invitation) command to request any new room invitations that the client has not yet seen. In a separate SIP INFO message, Persistent Chat Server returns a list of those rooms.

Subscribe to a Room and Post a Message

The following call flow diagram and steps describe a typical room subscription and message post scenario.

1. From the Persistent Chat client, User1 clicks **Join a Chat Room**, clicks **Search**, and then enters some search criteria. The Persistent Chat client sends a SIP INFO message that contains the XCCOS **chansrch** (room search) command, along with the search criteria. Persistent Chat Server queries the back-end database and replies in a new SIP INFO message that contains a list of available rooms that meet the search criteria.
2. User1 selects the chat room that he or she wants to join, and then clicks **Follow this room**. The Persistent Chat client sends Persistent Chat Server a SIP INFO message that contains the XCCOS **join** command and the room ID of the chat room that the user selected. Persistent Chat Server replies with a SIP INFO message that contains the provisioning data.
3. The Persistent Chat client sends Persistent Chat Server a SIP INFO message that contains the XCCOS **bccontext** (backchat context) command. Persistent Chat Server retrieves the chat history, and returns it to the Persistent Chat client in a separate SIP INFO message. At this point, the user enters the chat

room and is ready to participate.

4. User1 enters a new message, and then clicks **Send**. The Persistent Chat client posts the message to the chat room in a SIP INFO XCCOS **grpchat** command. Persistent Chat Server stores a copy of this new message in the Persistent Chat back-end database.
5. Persistent Chat Server sends a separate copy of the SIP INFO XCCOS **grpchat** message to User2, who has already entered the chat room.

Persistent Chat Compliance Call Flows

Persistent Chat Server uses Message Queuing (also known as MSMQ) and an additional compliance database (mgccomp) to process compliance data. As an example of how compliance events are processed, the following sequence of events describes how a message post event is processed.

1. A user posts a message to a room.
2. Persistent Chat Server places information pertaining to the event in a private Message Queuing queue.
3. Persistent Chat Compliance server reads this event from the queue, and places it into the mgccomp database for processing later.
4. Periodically, the Persistent Chat Compliance server processes a set of events in the database, and sends them to the Persistent Chat Compliance adapter for processing.
5. If the adapter successfully processes the data, Persistent Chat Compliance server deletes the events from the mgccomp database.

1.4.9.2 Deployment Checklist for Persistent Chat Server

Deployment Checklist for Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-10-16*

Deployment of Lync Server 2013, Persistent Chat Server requires that you deploy it in the correct sequence and that you complete all required deployment steps.

Deployment Sequence

You can deploy Persistent Chat Server after you deploy your initial topology, including at least one Lync Server 2013, Front End pool or one Lync Server 2013, Standard Edition server. This topic describes how to deploy Persistent Chat Server by adding it to an existing deployment.

Deployment Process

The following table lists the basic steps to deploy Persistent Chat Server and provides links for more details.

Persistent Chat Server Deployment Process

Task	**Steps**	**Required roles and group memberships**	**Related topics**
Install prerequisite hardware and	On hardware that meets system requirements, install the following: • On the Persistent	Any user who is a member of the local	Supported Hardware in the Supportability documentation

software	Chat Server Front End Servers: • An operating system that meets system requirements • Software prerequisites for computers running Lync Server 2013 • SQL Server on the server that will host Persistent Chat Server database If Persistent Chat Server compliance is required: • SQL Server on the server that will host Persistent Chat Server compliance database	Administrators group.	Server Software and Infrastructure Support in the Supportability documentation Determining Your System Requirements Technical Requirements for Persistent Chat Server
Create the appropriate internal topology to support Persistent Chat Server (and optionally, Persistent Chat compliance)	Run Topology Builder to add a Persistent Chat Server pool to your topology: • Add Persistent Chat Server components to the topology • Create a SQL Server database for the Persistent Chat Server store (and a backup SQL Server for disaster recovery) • Define a new Lync File Store or use an existing Lync File Store for Persistent Chat Server files • Associate the Lync Server 2013 pool that can route requests to this Persistent Chat Server pool If Persistent Chat compliance is required: • Add Persistent Chat Compliance Store • Click the Persistent Chat Server pool definition check box for enabling compliance • Publish the topology If you install Persistent Chat	To define a topology, an account that is a member of the local Users group. To publish the topology, an account that is a member of the Domain Admins group and RTCUniversalServerAdmins group, and the user should also have full control permissions (read/write/modify) on the Lync File Store for Persistent Chat Server files (so that Topology Builder can configure the required DACLs).	Adding Persistent Chat Server to Your Deployment in the Deployment documentation

	Server on Standard Edition, the fully qualified domain name (FQDN) of the Persistent Chat Server pool must match the Standard Edition server, and the SQL Server databases are collocated on the SQL Server Express instance on the Standard Edition server		
Deploy Persistent Chat Server	Run the Lync Server setup on all the computers running Persistent Chat Server. The Persistent Chat Server setup is integrated into the Lync Server 2013 Deployment wizard that provides the following instructions: • Deploy local management store • Install Persistent Chat Server services • Request and assign certificates • Run and start the services	Any user who is a member of the local Administrators group.	Deploying Persistent Chat Server in the Deployment documentation
Create a Persistent Chat administrator	Add users to the CsPersistentChatAdministrator security group.	Any user who is a member of domain administrators.	Adding a Persistent Chat Administrator in the Deployment documentation
Configure Persistent Chat Server	Configure users: • User has to be enabled by policy to access Persistent Chat Server. By default, the policy is turned off for all users and can be defined at global/site/pool/user scopes. • Configure settings	User must be a member of CsPersistentChatAdministrator. To change policy, user must be in CsUserAdministrator, at a minimum.	Configuring Persistent Chat Server in the Deployment documentation

◆Important:

You can deploy one or more Persistent Chat Server pools. We support multiple Persistent Chat Server pools for regulatory reasons whereby data generated in a given region is required to stay in that region. For example, if you deploy a Persistent Chat Server pool in Chicago, and another in Zurich to comply with regulations for data in Switzerland, users can connect to rooms in both the Persistent Chat Server pools, provided they have access.

1.4.9.3 Technical Requirements for Persistent Chat Server

Technical Requirements for Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2013-01-06*

Each computer that hosts Persistent Chat Server must have access to an existing Lync Server 2013 topology with the following components:

- **Lync Server 2013, Front End Server.** The Front End Server is the foundation for Session Initiation Protocol (SIP) routing, which makes communication between computers running Persistent Chat Server and the Persistent Chat functionality possible. Before you begin to deploy Persistent Chat Server, verify the deployment of Lync Server 2013, Standard Edition, or a Lync Server Front End pool and any other internal computers running Lync Server, as appropriate to your organization.

The following sections describe the specific requirements for the Persistent Chat Server and the database that stores the Persistent Chat data.

Persistent Chat Server Requirements

For details about the recommended hardware for deploying Lync Server and the latest version of Persistent Chat Server, see Server Hardware Platforms in the Supportability documentation.

For details about the server and tools operating system support for Lync Server and Persistent Chat Server, see Server and Tools Operating System Support in the Supportability documentation.

For details about additional software required for deploying Persistent Chat Server, see the following table.

Persistent Chat Server Software Prerequisites

Software	Description
Message Queuing	Used by the Persistent Chat Server and Persistent Chat Compliance service, if deployed.

Persistent Chat Server Database Requirements

Persistent Chat Server uses the Persistent Chat database to store chat history, configuration, and user provisioning data. Optionally, it uses the Persistent Chat compliance database to store compliance data.

◆Important:

The Persistent Chat database (mgc) and the compliance database (mgccomp) can be located in the same instance of SQL Server or on different SQL Servers.

To prepare a database server platform, be sure that each computer meets the hardware requirements, and then install the prerequisite software.

The server platform for the Persistent Chat database servers requires the same hardware as the Lync Server back-end database server. For details, see Server Hardware Platforms in the Supportability documentation.

On the database server, be sure that one of the following software applications is installed:

- Microsoft SQL Server 2012. For details about how to install Microsoft SQL Server 2012, see "Install SQL Server 2012" at http://go.microsoft.com/fwlink/p/?LinkID=248559.
- Microsoft SQL Server 2008 R2. For details about how to install Microsoft SQL Server 2008 R2, see "SQL Server Installation (SQL Server 2008 R2)" at http://go.microsoft.com/fwlink/?LinkId=275702.

Persistent Chat Server Certificate Requirements

For details about acquiring certificates, creating the SQL Server database, and creating file stores, see Deploying Lync Server 2013 in the Deployment documentation.

1.4.9.4 Setting Up Systems and the Infrastructure for Persistent Chat Server

Setting Up Systems and the Infrastructure for Persistent Chat Server

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-03-23*

Before deploying Lync Server 2013, Persistent Chat Server, you need to deploy the appropriate hardware and software for all Persistent Chat Server components.

In This Section

- Set Up System Platforms
- Install Lync Server 2013 Prerequisite Software

1.4.9.4.1 Set Up System Platforms

Set Up System Platforms

See Also

Deployment > Deploying Persistent Chat Server > Setting Up Systems and the Infrastructure for Persistent Chat Server >

Topic Last Modified: *2013-02-21*

Before starting the deployment of Persistent Chat Server, you must install the required operating system on hardware that meets system requirements on servers:

For details about supported hardware for servers running Lync Server 2013, database servers, and file servers, see Supported Hardware in the Supportability documentation. For details about supported operating systems and database software, see Server Software and Infrastructure Support in the Supportability documentation. For details about Windows update requirements, see Additional Server Support and Requirements in the Supportability documentation.

The Persistent Chat Server Front End Server, **PersistentChatService**, can be deployed on one or more stand-alone computers in a Lync Server 2013 Enterprise Edition pool. They cannot be collocated on the Lync Server Enterprise Edition Front End Servers. Persistent Chat Server can be deployed by the Bootstrapper, just like other Lync Server roles. The **Persistent Chat Web Services for File Upload/Download**, and **Persistent Chat Web Services for Chat Room Management** are web components deployed on the Lync Server 2013 Front End Servers.

A single Persistent Chat Server Front End Server can support 20,000 active users. You can have a Persistent Chat Server pool with up to 4 active front ends supporting a total of 80,000 concurrent users. The Persistent Chat Back End Server, **PersistentChatStore**, stores the chat rooms and categories. We recommend that you install the **PersistentChatStore** on a dedicated SQL Server Back End Server in your Enterprise Edition pool; although we support collocating Lync Server 2013 Back End Server and **PersistentChatStore** on the same SQL Server instance.

If your organization requires compliance support, you can install it by using Topology Builder. The Persistent Chat Server Compliance service is installed on the same computer as the Persistent Chat Server Front End Server. A separate database is required for compliance. For details about compliance requirements for Persistent Chat Server, see Planning for Persistent Chat Server in the Planning documentation.

At a minimum, each topology requires a server with Lync Server 2013 installed and a server with SQL Server database software installed. Topology Builder supports multiple Persistent Chat Server pools. Follow the same deployment instructions for deploying multiple Persistent Chat Server pools as you would for any pool from Deploying Lync Server 2013 in the Deployment documentation.

You can also deploy Persistent Chat Server with Lync Server 2013 Standard Edition. In this case, the **PersistentChatService** Front End Server is collocated on the Standard Edition server, and you can deploy the **PersistentChatStore** Back End Server on the local SQL Server Express instance.

Important:
We do not support Persistent Chat Server Standard Edition for high availability. Performance and scale will be limited. Furthermore, we support only new Persistent Chat Server Standard Edition server deployments. We do not support an upgrade of Lync Server 2010, Group Chat Server to a Lync Server 2013 Persistent Chat Server Standard Edition.

Concepts

Additional Server Support and Requirements

Other Resources

Supported Hardware
Server Software and Infrastructure Support
Planning for Persistent Chat Server
Deploying Lync Server 2013

1.4.9.4.2 Install Lync Server 2013 Prerequisite Software

Install Lync Server 2013 Prerequisite Software

See Also

Deployment > Deploying Persistent Chat Server > Setting Up Systems and the Infrastructure for Persistent Chat Server >

Topic Last Modified: *2013-02-21*

The prerequisite software for Persistent Chat Server is the same as the prerequisite software for the Lync Server 2013 Front End Servers and the Lync Server 2013 Standard Edition server on which Persistent Chat Server features are installed.

The prerequisite software required for the Persistent Chat Server file store is the same as that for Lync Server 2013.

The prerequisite software for the SQL Server databases for Persistent Chat Server content and compliance is also the same as that for Lync Server 2013.

For details about all the software requirements for Lync Server 2013 servers, see Additional Server Support and Requirements in the Supportability documentation.

Concepts

Additional Server Support and Requirements

1.4.9.5 Adding Persistent Chat Server to Your Deployment

Adding Persistent Chat Server to Your Deployment

Microsoft Lync Server 2013 > Deployment > Deploying Persistent Chat Server >

Topic Last Modified: *2012-09-12*

After you install the prerequisite software on each server on which you plan to deploy Lync Server 2013, Persistent Chat Server, you must use Topology Builder to add Persistent Chat Server support to your topology, and then publish the topology.

In This Section

- Add Persistent Chat Server to the Topology
- Publish the Updated Topology

1.4.9.5.1 Add Persistent Chat Server to the Topology

Add Persistent Chat Server to the Topology

Deployment > Deploying Persistent Chat Server > Adding Persistent Chat Server to Your Deployment >

Topic Last Modified: *2012-10-06*

You must incorporate Lync Server 2013, Persistent Chat Server support in your topology before you can configure your deployment to support Persistent Chat Server. The information in this topic describes how to use Topology Builder to add Persistent Chat Server support to your existing topology.

To add Persistent Chat Server to a topology

Perform the following steps for installing a single Persistent Chat Server pool without a disaster recovery configuration. For configuring a stretched Persistent Chat Server pool for high availability and disaster recovery, see Configuring Persistent Chat Server for High Availability and Disaster Recovery in the Deployment documentation.

To deploy multiple Persistent Chat Server pools, repeat the same process for each pool.

1. On a computer that is running Lync Server 2013 or on which the Lync Server administrative tools are installed, log on using an account that is a member of the local Users group (or an account with equivalent user rights).

   Note:
   You can define a topology by using an account that is a member of the local Users group, but to publish a topology, which is required to install a Lync Server 2013 server, you must use an account that is a member of the **Domain Admins** group and the **RTCUniversalServerAdmins** group, and that has full control permissions (that is, read, write, and modify) on the file store that you are going to use for the Persistent Chat Server file store (that is, so that Topology Builder can configure the required DACLs), or an account with equivalent rights.

2. Start Topology Builder.
3. In the console tree, navigate to the **Persistent Chat Pools** node and expand it to select a Persistent Chat Server pool, or right-click the node and select **New Persistent Chat Pool**. You must define the pool's fully qualified domain name (FQDN), and indicate whether the pool will be a single-server pool or multiple-server pool deployment.
   You can choose a **Multiple Computer Pool** or a **Single Computer Pool**. Choose the former if you are planning to have more than one Persistent Chat Server Front End Server in your Persistent Chat Server pool. Make this choice now, or at a later point, because after you create a single computer pool, you cannot add additional servers to it later. If you choose a multiple computer pool, enter the names of the individual Persistent Chat Server Front End Servers that comprise the pool.

   Important:
   If the Persistent Chat Server role is being installed on a Lync Server 2013 Standard Edition server, the FQDN needs to match the FQDN of the Standard Edition server.

4. Define a simple **Display Name** for the Persistent Chat Server pool. The display name can be used by custom clients, particularly when there are multiple Persistent Chat Server pools, to differentiate rooms.
5. Define the port used by the Persistent Chat Server to communicate with Lync Server Front End Servers. The default port is 5041.
6. If your organization requires compliance support, select the **Enable compliance** check box. If chosen, the Persistent Chat Server Compliance service is installed on the same computer as the Persistent Chat Server Front End Server. You are prompted to select a SQL Server Back End Server for Persistent Chat Server Compliance later.
7. Assign site affinity for the Persistent Chat Server pool. Select the **Use this pool as default for site <SiteName>** check box or **Use this pool as default for all sites** to designate this Persistent Chat Server pool as the default pool for the current site or all sites. When the Lync 2013 client is used to create and manage rooms, the default pool associated with the user's site is used by the room creation and management experience so that it can route room creation and management operations to that pool. This only applies when you have multiple Persistent Chat Server pools deployed, and want to use the room creation and management features of Persistent Chat Server.

   Important:
   You can customize the room creation and management features using the Persistent Chat Server Software Development Kit (SDK).
   For details about how to configure SQL Server backup databases for disaster recovery, see Configuring Persistent Chat Server for High Availability and Disaster Recovery in the Deployment documentation.

8. Define the **SQL store for the Persistent Chat Server Back End (where chat**

room content is stored) by doing one of the following:

- To use an existing SQL Server database, in the drop-down list, click the name of the SQL Server database that you want to use.
- To specify a new SQL Server database, click **New**, and in **Define New SQL Store**, perform the following:
- In **SQL Server FQDN**, specify the FQDN of the SQL Server on which you want to create the new SQL Server database.
- Either select **Default Instance** to use the default instance or, to specify a different instance, select **Named Instance**, and specify the instance that you want to use.

9. Define the SQL Server compliance database if you enabled Compliance.

> **Important:**
> For details about how to configure SQL Server mirrors for high availability for the Persistent Chat Server database and the Persistent Chat Server compliance database, see Configuring Persistent Chat Server for High Availability and Disaster Recovery in the Deployment documentation.

10. Define the file store. A file store is a folder where a copy of any file uploaded to the file repository is stored (for example, storing file attachments posted to a chat room). In the case of a multiple-server Persistent Chat Server topology, this must be a Universal Naming Convention (UNC) path; and for a single-server Persistent Chat Server topology, it can be a local file path.
    To use an existing file store, perform the following steps:
    - In **File Server FQDN**, specify the FQDN of the file store on which you want to create the new file store.
    - In **File Share**, specify the file store that you want to use.

> **Important:**
> You can define the file store in Topology Builder before you create the file store, but you must create the file store in the defined location you define before you publish the topology.

11. Select the Front End Server pool to be used as a next hop for this Persistent Chat Server pool. This is the Front End Server pool that will be able to route Persistent Chat Server requests to this pool.
12. To save the configuration, click **Finish**. The Persistent Chat Server pool appears in Topology Builder accompanied by your specific pool settings.
    To now publish your updated topology to which you've Persistent Chat Server, see Publish the Updated Topology in the Deployment documentation.

> **Note:**
> With Topology Builder already open, you can proceed to step 3 in Publish the Updated Topology to begin publishing your updated topology.

1.4.9.5.2 Publish the Updated Topology

Publish the Updated Topology

Deployment > Deploying Persistent Chat Server > Adding Persistent Chat Server to Your Deployment >

Topic Last Modified: *2012-10-01*

After updating your topology in Topology Builder, you must publish the topology to the Central Management store before you can configure and use Persistent Chat Server. Read-only copies of the data are replicated to all servers in the topology to keep all servers in sync with topology and other configuration changes.

To publish an updated topology

Before you publish your topology, install the databases for Persistent Chat Server. Use Topology Builder to install databases by selecting **Action** and **Install Database**.

1. On a computer that is running Lync Server 2013 or on which the Lync Server administrative tools are installed, log on using an account that is a member of both the **Domain Admins** group and the **RTCUniversalServerAdmins** group, and that has full control permissions (that is, read, write, and modify) on the file store to be used for the Persistent Chat Server file store (so that Topology Builder can configure the required discretionary access control lists (DACLs)), or an account with equivalent user rights.
2. Start Topology Builder. Select **Download Topology from existing deployment**, or **Open Topology from a local file** if you saved it locally.
3. In the console tree, right-click **Lync Server 2013**, and then click **Publish Topology**.
4. On the **Publish the topology** page, click **Next**.
5. On the **Publishing wizard complete** page, verify that the topology was successfully published, and then click **Finish**.

Important:

After publishing the topology, you must configure support for Persistent Chat Server before any content can be archived.

1.4.9.6 Installing Persistent Chat Server

Installing Persistent Chat Server

Microsoft Lync Server 2013 > Deployment > Deploying Persistent Chat Server >

Topic Last Modified: *2012-10-01*

Installing Persistent Chat Server is integrated into Lync Server 2013 setup and uses the same Bootstrapper that Lync Server 2013 uses for installation. For installation instructions, see Deploying Lync Server 2013 in the Deployment documentation.

1.4.9.7 Adding a Persistent Chat Administrator

Adding a Persistent Chat Administrator

Microsoft Lync Server 2013 > Deployment > Deploying Persistent Chat Server >

Topic Last Modified: *2012-10-06*

In Lync Server 2013, users who perform specific tasks must be assigned as members of one or more specific groups. Role-based access control (RBAC) can also be used to grant privileges by assigning users to predefined Lync Server 2013 administrative roles.

Before configuring and administering Persistent Chat Server, be sure that the appropriate user rights and permissions are in place, and that any users to be classified as Persistent Chat administrators are added to the CsPersistentChatAdministrator security group.

1.4.9.8 Configuring Persistent Chat Server

Configuring Persistent Chat Server

Microsoft Lync Server 2013 > Deployment > Deploying Persistent Chat Server >

Topic Last Modified: *2012-04-12*

After deploying support for Lync Server 2013, Persistent Chat Server in Topology Builder, you use the Lync Server 2013 Control Panel to configure how Persistent Chat Server is implemented in your deployment.

In This Section

- Enable Persistent Chat Server Policy
- Configure Persistent Chat Server Options Globally or for Persistent Chat Server Pool
- Configure Categories
- Configure Rooms
- Configure Add-ins for Rooms

1.4.9.8.1 Enable Persistent Chat Server Policy

Enable Persistent Chat Server Policy

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server >

Topic Last Modified: *2012-10-06*

In the Lync Server 2013 Control Panel, you can use the **Persistent Chat Policy** page of the **Persistent Chat** group to manage policies at a global, pool, site, or user level, including configuring the default global policy and creating one or more additional user and site policies for your deployment. If a user is enabled for Persistent Chat Server by policy, then the Persistent Chat Server environment appears in their Lync 2013 client.

Note:

In the topology, Persistent Chat Server site policies apply globally, per user’s pool, or per user’s site, or per user.

The global policy is created automatically when you deploy Persistent Chat Server, and it can be configured, but not deleted. Because the global policy applies to all users, it doesn’t have to be set per user.

You can create and configure multiple site and user policies which, together with the global policy, enable users for Persistent Chat Server. Pool and site Persistent Chat Server policies override the global Persistent Chat Server policy, but only for users of that site. User policies override both global, pool, and site policies for the users to whom the user policy is assigned.

Note:

To configure and use Persistent Chat Server, you must first use Topology Builder to add Persistent Chat Server support to the topology, and then publish the topology. For details, see Adding Persistent Chat Server to Your Deployment in the Deployment documentation.

In This Section

- Configure the Global Policy for Persistent Chat
- Create a Site Policy for Persistent Chat
- Create a User Policy for Persistent Chat
- Apply a Persistent Chat Policy to a User or User Group

1.4.9.8.1.1 Configure the Global Policy for Persistent Chat

Configure the Global Policy for Persistent Chat

Deploying Persistent Chat Server > Configuring Persistent Chat Server > Enable Persistent Chat Server Policy >

Topic Last Modified: *2012-10-06*

You can use the default global policy by itself to enable Persistent Chat settings for all users in your deployment. You can also specify additional policies for sites and users to control whether Persistent Chat is enabled or disabled for specific users and sites.

You cannot delete the global policy. If you attempt to delete it, the configuration resets to the default values.

Note:

To configure and use Persistent Chat Server, you must first use Topology Builder to add Persistent Chat Server support to the topology, and then publish the topology. For details, see Adding Persistent Chat Server to Your Deployment in the Deployment documentation.
To configure Persistent Chat Server configuration settings, see Configure Persistent Chat Server Options Globally or for Persistent Chat Server Pool in the Deployment documentation.

To configure the Global Policy for Persistent Chat

1. From a user account that is assigned to the CsPersistentChatAdministrator, CsAdministrator, or CsUserAdministrator role, log on to any computer in your internal deployment.
2. From the **Start** menu, select the Lync Server Control Panel or open a browser window, and then enter the Admin URL. For details about the different methods that you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools in the Operations documentation.

   Important:

   You can also use Windows PowerShell cmdlets. For details, see Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets in Deployment documentation.

3. In Lync Server Control Panel, click **Persistent Chat**, and then click **Persistent Chat Policy**.
4. Click **Global** in the list of policies, click **Edit**, and then click **Show details**.
5. In **Edit Persistent Chat Policy - Global**, do the following:
   - In **Name**, specify a new name for the global policy, if you do not want to use the default of Global.
   - In **Description**, provide details about what the user policy is (for example, Global policy for *centralSiteName*).
   - To control Persistent Chat for all sites and users not specifically controlled through a site policy or user policy, select or clear the **Enable Persistent Chat** check box.

6. Click **Commit**.

Create a Site Policy for Persistent Chat

Deploying Persistent Chat Server > Configuring Persistent Chat Server > Enable Persistent Chat Server Policy >

Topic Last Modified: *2012-10-06*

For each site you have deployed, you can create a site-specific Persistent Chat policy.

The configuration in the site policy overrides the global policy, but only for the specific site covered by the site policy.

Note:

To configure and use Persistent Chat Server, you must first use Topology Builder to add Persistent Chat Server support to the topology, and then publish the topology. For details, see Adding Persistent Chat Server to Your Deployment in the Deployment documentation.
To configure Persistent Chat Server configuration settings, see Configure Persistent Chat Server Options Globally or for Persistent Chat Server Pool in the Deployment documentation.

To create a Persistent Chat policy for a site

1. From a user account that is assigned to the CsPersistentChatAdministrator, CsAdministrator, or CsUserAdministrator role, log on to any computer in your internal deployment.
2. From the **Start** menu, select the Lync Server Control Panel or open a browser window, and then enter the Admin URL. For details about the different methods that you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Persistent Chat**, and then click **Persistent Chat Policy**.

   Important:

   You can also use Windows PowerShell cmdlets. For details, see Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets in the Deployment documentation.
4. Click **New**, and then click **Site policy**.
5. In **Select a Site**, click the site to which the policy is to be applied.
6. In **New Persistent Chat Policy**, do the following:
   - In **Name**, specify a name for the new site policy (for example, Redmond).
   - In **Description**, provide details about what the site policy is (for example, chat room policy for Redmond).
   - To control Persistent Chat for all sites not specifically controlled through a site policy, select or clear the **Enable Persistent Chat** check box.
7. Click **Commit**.

1.4.9.8.1.3 Create a User Policy for Persistent Chat

Create a User Policy for Persistent Chat

Deploying Persistent Chat Server > Configuring Persistent Chat Server > Enable Persistent Chat Server Policy >

Topic Last Modified: *2012-10-06*

In the Lync Server Control Panel, you define user policies that can be assigned to users in **Users**.

The user policy overrides the global policy and site policies, but only for the specific users who are assigned the user policy.

> **Note:**
>
> To configure and use Persistent Chat Server, you must first use Topology Builder to add Persistent Chat Server support to the topology, and then publish the topology. For details, see Adding Persistent Chat Server to Your Deployment in the Deployment documentation.
> To configure Persistent Chat Server configuration settings, see Configure Persistent Chat Server Options Globally or for Persistent Chat Server Pool in the Deployment documentation.

To create a user policy for Persistent Chat

1. From a user account that is assigned to the CsPersistentChatAdministrator, CsAdministrator, or CsUserAdministrator role, log on to any computer in your internal deployment.
2. From the **Start** menu, select the Lync Server Control Panel or open a browser window, and then enter the Admin URL. For details about the different methods that you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

   > **Important:**
   >
   > You can also use Windows PowerShell cmdlets. See Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets in the Deployment documentation.

3. In the left navigation bar, click **Persistent Chat**, and then click **Persistent Chat Policy**.
4. Click **New**, and then click **User policy**.
5. In **New Persistent Chat Policy**, do the following:
   - In **Name**, specify a name for the new user policy.
   - In **Description**, provide details about what the user policy is (for example, Persistent Chat policy for specific user).
   - To control Persistent Chat for all users who are not specifically controlled through a user policy, select or clear the **Enable Persistent Chat** check box.

6. Click **Commit**.

1.4.9.8.1.4 Apply a Persistent Chat Policy to a User or User Group

Apply a Persistent Chat Policy to a User or User Group

Deploying Persistent Chat Server > Configuring Persistent Chat Server > Enable Persistent Chat Server Policy >

Topic Last Modified: *2012-10-06*

If a user has been enabled for Lync Server 2013, you can apply appropriate policies to specific users to enable or disable them for Persistent Chat Server.

Note:

To configure and use Persistent Chat Server, you must first use Topology Builder to add Persistent Chat Server support to the topology, and then publish the topology. For details, see Adding Persistent Chat Server to Your Deployment in the Deployment documentation.
To configure Persistent Chat Server configuration settings, see Configure Persistent Chat Server Options Globally or for Persistent Chat Server Pool in the Deployment documentation.

Use the procedure in this topic to apply a previously created Persistent Chat user policy to one or more user accounts or user groups.

To apply a Persistent Chat user policy to a user account

1. From a user account that is assigned to the CsPersistentChatAdministrator, CsAdministrator, or CsUserAdministrator role, log on to any computer in your internal deployment.
2. From the **Start** menu, select the Lync Server Control Panel or open a browser window, and then enter the Admin URL. For details about the different methods that you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**, and then search on the user account that you want to configure.
4. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
5. In **Edit Lync Server User** under **Persistent Chat policy**, select the Persistent Chat user policy that you want to apply.

   Note:

   The **<Automatic>** settings apply the default effective policy. These settings are applied automatically by the server.

6. Click **Commit**.

1.4.9.8.2 Configure Persistent Chat Server Options Globally or for Persistent Chat Server Pool

Configure Persistent Chat Server Options Globally or for Persistent Chat Server Pool

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server >

Topic Last Modified: *2012-10-06*

In Lync Server 2013 Control Panel, you can use the **Persistent Chat Configuration** section of the **Persistent Chat** page to configure Persistent Chat settings globally where it applies to all Persistent Chat Server pools, or for a specific Persistent Chat Server pool.

Note:

To configure and use Persistent Chat Server, you must first use Topology Builder to add

> Persistent Chat Server support to the topology, and then publish the topology. For details, see Adding Persistent Chat Server to Your Deployment in the Deployment documentation.

To configure Persistent Chat options globally

1. From a user account that is assigned to the CsPersistentChatAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. From the **Start** menu, select the Lync Server Control Panel or open a browser window, and then enter the Admin URL. For details about the different methods that you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

   > **Important:**
   >
   > You can also use Windows PowerShell cmdlets. For details, see Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets in the Deployment documentation.

3. In the left navigation bar, click **Persistent Chat**, and then click **Persistent Chat Configuration**.
4. On the **Persistent Chat Configuration** page, click **New,** and then click **Site configuration**.

   > **Important:**
   >
   > Choose this option if you want the configuration to be applied to all Persistent Chat Server pools deployed in the site. Click **Pool Configuration** if you want the configuration to be applied to a specific Persistent Chat Server pool.

5. In **Select a Site**, select the site to be configured for the Persistent Chat Server site configuration.
6. In **New Persistent Chat Configuration**, do the following:
   - In **Name**, specify a name for the new configuration settings. By default, the site name already exists.
   - In **Default chat history**, define the number of chat messages that will be processed for each room upon first request. By default, the number is 30. This is the global default, and administrators can disable chat history per category.

     > **Important:**
     >
     > Persistent Chat Server will cache these messages in memory, so if you increase this number, more messages will be cached. You can always access historical content by search. The default number simply determines the maximum number of messages that you initially see when connecting to a chat room.

   - In **Maximum file size (KB)**, select the maximum file size of each chat history. By default, the number is 20 MB (20,000 KB). This is the maximum size for a file that can be uploaded to any chat room in the system (for which file uploads are enabled by its corresponding **Category** setting).

     > **Important:**
     >
     > This setting is enforced on the server because custom applications or previous Group Chat clients using Office Communications Server 2007 R2 Group Chat Server or Lync Server 2010, Group Chat can post files to a room. The Lync 2013 client does not have file upload/download capability, so if you have a pure Lync 2013 deployment or Lync 2013 client, it is not possible to post files in a Persistent Chat Server chat room.

   - In **Participant update limit**, select the limit for participant updates.

Persistent Chat Server sends roster information (who is connected to a chat room) to all participants until the number of connected users reaches this number. By default, the number is 75. This limit indicates the maximum number of participants in a given room beyond which Persistent Chat Server stops sending roster updates to connected clients about who is present in the room.

- (Optional.) In **Room management URL**, select the room management URL. This is the URL for a web-based custom room management. If you don't need to customize room management, and you simply use the default setting, leave this option blank. After the URL is set, it is applied as both the internal and external room management URL.

  If you want to customize your room creation experience and include your specific business workflow, you can build a custom room management solution by using the Persistent Chat Server Software Development Kit (SDK), host it somewhere, and put the URL here. This URL is sent down to the client, so that when a user tries to view or create a room, he or she is directed to your custom room management solution.

7. Click **Commit**.

To configure Persistent Chat options for a specific Persistent Chat Server pool

1. From a user account that is assigned to the CsPersistentChatAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. From the **Start** menu, select the Lync Server Control Panel, or open a browser window, and then enter the Admin URL. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

> **Important:**
> You can also use Windows PowerShell cmdlets. For details, see Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets in the Deployment documentation.

3. In the left navigation bar, click **Persistent Chat**, and then click **Persistent Chat Configuration**.
4. On the **Persistent Chat Configuration** page, click **New**, and then click **Pool configuration**.
5. In **Select a Service**, select the service associated with the Persistent Chat Server pool to be configured.
6. In **New Persistent Chat Configuration**, do the following:

- In **Name**, specify a name for the new configuration settings. By default, the site pool name already exists.
- In **Default chat history**, define the number of chat messages that will be processed for each room upon first request. By default, the number is 30. This is the global default, and administrators can disable chat history per category.

> **Important:**
> Persistent Chat Server will cache these messages in memory, so if you increase this number, more messages will be cached. You can always access historical content by search. The default number simply determines the maximum number of messages that you initially see when connecting to a chat room.

- In **Maximum file size (KB)**, select the maximum file size of each chat history. By default, the number is 20 MB (20,000 KB). This is the maximum size for a file that can be uploaded to any chat room in the system (for which file uploads are enabled by its corresponding **Category** setting).

Important:
This setting is enforced on the server because custom applications or previous Group Chat clients (Office Communications Server 2007 R2 Group Chat Server or Lync Server 2010, Group Chat) can post files to a room. The Lync 2013 client does not have file upload/download capability, so if you have a pure Lync 2013 deployment or Lync 2013 client, it is not possible to post files in a Persistent Chat Server chat room.

- In **Participant update limit**, select the limit for participant updates. Persistent Chat Server sends roster information (who is connected to a chat room) to all participants until the number of connected users reaches this number. By default, the number is 75. This limit indicates the maximum number of participants in a given room beyond which Persistent Chat Server stops sending roster updates to connected clients about who is present in the room.
- In **Room management URL**, select the room management URL. This is the URL for a web-based room management deployment. If you don’t need to customize room management, and you simply use the default setting, leave this option blank.

  If you want to customize your room creation experience and include your specific business workflow, you can build a custom room management solution by using the Persistent Chat Server Software Development Kit (SDK), host it somewhere, and put the URL here. This URL is sent down to the client so that when a user tries to view/create a room, he or she is directed to your custom room management solution.

7. Click **Commit**.

1.4.9.8.3 Configure Categories

Configure Categories

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server >

Topic Last Modified: *2012-10-06*

In Lync Server 2013 Control Panel, you can use the **Category** section of the **Persistent Chat** page to configure categories. A Persistent Chat room category is a logical structure for organizing chat rooms. A category defines a default set of access control lists (ACLs) for controlling the users and user groups who may create or join the chat rooms. You can use categories enforce ethical walls between different subdivisions within their organizations.

Chat room categories may contain chat rooms, but not other categories. Each category describes its contents with metadata, such as *Name* and *Description*. In addition, the category has properties which can be set to control the behavior of the chat rooms belonging to it, such as if the chat rooms allow *Invitations* or *File Uploads*, or contain *Chat History*.

To configure categories for chat rooms

1. From a user account that is assigned to the CsPersistentChatAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. From the **Start** menu, select the Lync Server Control Panel or open a browser window, and then enter the Admin URL. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

Important:
You can also use Windows PowerShell cmdlets. For details, see Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets in the Deployment documentation.

3. In the left navigation bar, click **Persistent Chat**, and then click **Category**. For multiple Persistent Chat Server pool deployments, select the appropriate pool from the drop-down list.
4. On the **Category** page, click **New** or **Edit**.
5. In **Select a Service**, select the service corresponding to the Persistent Chat Server pool on which the category needs to be created. The service is the Persistent Chat Server pool that the Persistent Chat (client) uses to identify which pool the category belongs to. A category can belong to only one Persistent Chat Server pool, and cannot be moved to another one, or shared with another pool.
6. In **New Category**, do the following:
   6.a. In **Name**, specify a name for the new room category.
   6.b. In **Description**, provide a detailed description for the room category (for example, a room category for Contoso).
   6.c. To control whether invitations can be enabled for chat rooms that belong to this category, select or clear the **Enable invitations** check box. If selected, rooms in this category may have invitations on or off; if cleared, the rooms in this category are not allowed to have invitations. If a room has invitations on, when a new member is added to a room, he or she gets a notification of the new room in their Persistent Chat client.
   6.d. To control file uploads in chat rooms belonging to this category, select or clear the **Enable file upload** check box. If selected, the rooms of this category can enable or disable file uploads; if cleared, the rooms of this category are not allowed to have file uploads.

   Important:
   This setting is enforced on the server because custom applications or previous Group Chat clients that use Office Communications Server 2007 R2 Group Chat Server or Lync Server 2010, Group Chat can post files to a room. The Lync 2013 client does not have file upload/download capability, so if you have a pure Lync 2013 deployment or Lync 2013 client, it is not possible to post files in a Persistent Chat Server chat room.

   6.e. To control chat history, select or clear the **Enable chat history** check box. If selected, room chats become persistent; otherwise, chat messages are not persisted. If compliance is enabled, room chats will be saved in compliance, but users will not be able to access older messages. This option can be used for rooms designated for real-time, ad hoc collaborations that don't need chat history to be persisted.
7. In **Edit Category**, do the following:
   7.a. In **Membership**, in the **Allowed members** section, add or remove users and other Active Directory Domain Services (AD DS) principals (users, distribution groups, organizational units, and so on) that are permitted to be added as members of chat rooms belonging to the category. Principals permitted by a category can search for the rooms in the category (unless the room is hidden, in which case only members of the room can search for it in the directory).
   7.b. In **Membership**, in the **Denied members** section, add or remove users and other Active Directory principals associated with members being denied from the room.
   7.c. In **Membership**, in the **Creators** section, add or remove users and other Active Directory principals associated with creators for the category. A creator is a user who has permissions to create chat rooms and assign chat room managers and members.

8. Click **Commit**.

1.4.9.8.4 Configure Rooms

Configure Rooms

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server >

Topic Last Modified: *2012-10-06*

Configuring Persistent Chat rooms is commonly handled by users or other central teams by using Windows PowerShell command-line interface; an administrator typically does not manage chat rooms. However, if you have to create and manage chat rooms, you can use the Windows PowerShell command-line interface, or add yourself as a member to a chat room and use the Lync 2013 client.

For details about configuring chat rooms by using the Windows PowerShell command-line interface, see "Room Management" in Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets.

Managing Data in Chat Rooms

Persistent Chat Server lets users collaborate by posting messages into Persistent Chat rooms. The data is persisted on the server, and members of the room can have access to the data, including historical data. However, users with different roles have different access to the persisted data, as outlined in the following list.

- Administrators can delete earlier content (for example, content that was posted before a certain date) from any chat room to keep the database from growing too large. Or, they can remove or replace messages that are considered inappropriate for a particular chat room.
- End users, including message authors, cannot delete content from any chat room.
- Chat room managers can disable rooms, but cannot delete rooms. Only administrators can delete a chat room after it has been created.

When a message is deleted, you cannot undo the action. However, deleted messages can be restored if there is a backup. If a Persistent Chat Compliance server is enabled, old messages are persisted in the compliance database.

> **Note:**
>
> This chat room data usage applies to the Lync Server 2013, Persistent Chat Server API application, except for the case when the administrator role is involved. The Persistent Chat Server API cannot be used to do any of the administrator’s operations. You must perform these operations in the Lync Server Management Shell.

1.4.9.8.5 Configure Add-ins for Rooms

Configure Add-ins for Rooms

See Also

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server >

Topic Last Modified: *2013-02-21*

In Lync Server 2013 Control Panel, you can use the **Add-in** section of the **Persistent Chat** page to associate URLs with Persistent Chat rooms. These URLs appear in the Lync 2013 client in the chat room in the conversation extensibility pane. An administrator must add Add-ins to the list of registered add-ins, and chat room managers/Creators have to associate rooms with one of the registered add-ins before users can see this upgrade in their Lync 2013 client.

Add-ins are used to extend the in-room experience. A typical add-in might include a URL pointing to a Silverlight application that intercepts when a stock ticker is posted to a chat room, and shows the stock history in the extensibility pane. Other examples include embedding a OneNote 2013 URL in the chat room as an add-in to include some shared context, such as "Top of mind" or "Topic of the day."

To configure Add-ins for chat rooms

1. From a user account that is assigned to the CsPersistentChatAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. From the **Start** menu, select the Lync Server Control Panel or open a browser window, and then enter the Admin URL. For details about the different methods that you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

Important:
You can also use Windows PowerShell cmdlets. For details, see Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets in the Deployment documentation.

3. In the left navigation bar, click **Persistent Chat**, and then click **Add-in**. For multiple Persistent Chat Server pool deployments, select the appropriate pool from the drop-down list.
4. On the **Add-in** page, click **New**.
5. In **Select a Service**, select the service corresponding to the Persistent Chat Server pool where you need to create the Add-in. Add-ins cannot be moved from one pool to another or shared between different pools.
6. In **New Add-in**, do the following:
   - In **Name**, specify a name for the new add-in.
   - In **URL**, specify the URL to be associated with the add-in. URLs are limited to http and https protocols.
7. Click **Commit**.

⊟See Also

Tasks

Open Lync Server Administrative Tools

Concepts

Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets

1.4.9.9 Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets

Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets

Microsoft Lync Server 2013 > Deployment > Deploying Persistent Chat Server >

Topic Last Modified: *2012-10-06*

Use the following Windows PowerShell cmdlets to configure management within Lync Server 2013, Persistent Chat Server.

In This Section

- Manage Categories
- Manage Rooms

- Manage Add-ins
- Remove a Message
- Test Persistent Chat Server with a Synthetic Transaction
- Run Backward Compatibility for Persistent Chat Server
- Run, Grant, Get, Remove, or Set Persistent Chat Policy
- Configure Persistent Chat Server
- Get Persistent Chat Server Pool Availability
- Persistent Chat Compliance

1.4.9.9.1 Manage Categories

Manage Categories

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets >

Topic Last Modified: *2012-10-06*

To create a new Persistent Chat Server Category

```
New-CsPersistentChatCategory -Name Foo -PersistentChatPoolFqdn client.contoso1b11
```

◆Important:

PersistentChatPoolFqdn is needed only if there is more than one Persistent Chat Server pool.

To make changes to existing Persistent Chat Server Category

```
Set-CsPersistentChatCategory -Identity testCat -AllowedMembers @{Add="sip:user1@c
Set-CsPersistentChatCategory -Identity testCat -Creators @{Add="sip:user1@contoso
```

Windows PowerShell: AllowedMembers, DeniedMembers, and Creators can be set simultaneously. Creators should be the subset of AllowedMembers minus DeniedMembers. You can also set the properties of a category at the same time as the members and creators.

Create, Get, Set, or Remove a Category

To create a new Category

```
New-CsPersistentChatCategory -Name <String> [-PersistentChatPoolFqdn <String>] [-
```

To get a Category

```
Get-CsPersistentChatCategory -Identity <String>
```

or

```
Get-CsPersistentChatCategory -PersistentChatPoolFqdn <String>
```

To set a Category

```
Set-CsPersistentChatCategory -Instance <CategoryObject> [-WhatIf] [-Confirm] [<Co
```

or

```
Set-CsPersistentChatCategory [-Identity] <string> [-Name <string>] [-Description
```

To remove a Category

```
Remove-CsPersistentChatCategory -Instance <CategoryObject> [-Force <Switch Parame
```

or

```
Remove-CsPersistentChatCategory -Identity <String> [-Force <Switch Parameter>] [-
```

1.4.9.9.2 Manage Rooms

Manage Rooms

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets >

Topic Last Modified: *2013-02-21*

To create a new Persistent Chat Server room

```
New-CsPersistentChatRoom -Name Foo1 -PersistentChatPoolFqdn client.contoso.com -C
```

Important:

-PersistentChatPoolFqdn is not needed if one of the following is true:

- There is only one Persistent Chat Server pool.
- You provide a pool FQDN to the category.
- You provide a pool FQDN to adding the room.

To make changes to an existing Persistent Chat Server room

```
Set-CsPersistentChatRoom -Identity testCat -Members @{Add="sip:user1@contoso.com"
Set-CsPersistentChatRoom -Identity testCat -Managers @{Add="sip:user2@contoso.com
Set-CsPersistentChatRoom -Identity testCat -Presenters @{Add="sip:user1@contoso.c
```

Windows PowerShell: Members, Managers and Presenters can be set simultaneously. They all should be the subset of AllowedMembers minus DeniedMembers of the host Category. A room that is type=normal cannot include Presenters.

Create, Get, Set, Clear, or Remove a Room

To create a new room

```
New-CsPersistentChatRoom -Name <String> [-PersistentChatPoolFqdn <String>]-Catego
```

To set a room

```
Set-CsPersistentChatRoom -Identity <String> [-Name <String>] [-Category <String>]
```

To get a room

```
Get-CsPersistentChatRoom -Identity <String>
```

or

```
Get-CsPersistentChatRoom -filter <String> [-PersistentChatPoolFqdn <String>] [-Se
```

where –filter supports only Name and Description and helps you find rooms whose Name/ Description matches the keyword string. PoolFqdn searches in a given Persistent Chat Server pool.

To clear a room and clear messages from a room

```
Clear-CsPersistentChatRoom [-Identity] <string> -EndDate <DateTime> [-WhatIf] [-C
```

or

```
Clear-CsPersistentChatRoom [-Instance] <ChatRoomObject> -EndDate <DateTime> [-Wha
```

To remove a room

```
Remove-CsPersistentChatRoom [-Identity] <string> [-Force] [-WhatIf] [-Confirm]  [
```

or

```
Remove-CsPersistentChatRoom [-Instance] <ChatRoomObject> [-Force] [-WhatIf] [-Con
```

1.4.9.9.3 Manage Add-ins

Manage Add-ins

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets >

Topic Last Modified: *2012-10-06*

To create a new Persistent Chat Server Add-in

```
New-CsPersistentChatAddin -Name Contoso -PersistentChatPoolFqdn client.contoso.co
```

Create, Get, Set, or Remove an Add-in

To create a new Add-in

```
New-CsPersistentChatAddin -PersistentChatPoolFqdn <String> -Name <String> -Url<St
```

Important:

PersistentChatPoolFqdn <String> is required only if there is more than one Persistent Chat Server pool.

To get an Add-in

```
Get-CsPersistentChatAddin -Identity <String>]
```

or

```
Get-CsPersistentChatAddin -PersistentChatPoolFqdn <String>
```

To set an Add-in

```
Set-CsPersistentChatAddIn -Instance <AddinObject> [-Force <Switch Parameter>] [-C
```

or

```
Set-CsPersistentChatAddIn -Identity <String> [-Name <String>] [-Url<String>] [-Fo
```

To remove an Add-in

```
Remove-CsPersistentChatAddIn -Instance <AddinObject> [-Force <Switch Parameter>]
```

or

```
Remove-CsPersistentChatAddIn -Identity <String> [-Force <Switch Parameter>] [-Con
```

1.4.9.9.4 Remove a Message

Remove a Message

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets >

Topic Last Modified: *2012-04-04*

To remove a message

```
Remove-CsPersistentChatMessage -Identity <string> [-UserUri <string>] [-StartDate
```

1.4.9.9.5 Test Persistent Chat Server with a Synthetic Transaction

Test Persistent Chat Server with a Synthetic Transaction

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets >

Topic Last Modified: *2012-09-21*

To test Persistent Chat Server for sending and receiving messages in a chat room between two users

```
Test-CsPersistentChatMessage [-Authentication <TrustedServer | Negotiate | Client
    LiveID>] [-ReceiverSipAddress <String>] [-RegistrarPort <Int32>] [-SenderSipA
    [-OutVerboseVariable <String>] [<CommonParameters>]
```

or

```
Test-CsPersistentChatMessage [-Authentication <TrustedServer | Negotiate | Client
    LiveID>] -ReceiverCredential <PSCredential> -ReceiverSipAddress <String> [-Re
    <Int32>] -SenderCredential <PSCredential> -SenderSipAddress <String> [-Target
```

or

```
Test-CsPersistentChatMessage [-Authentication <TrustedServer | Negotiate | Client
    LiveID>] [-Force <SwitchParameter>] [-OutLoggerVariable <String>] [-OutVerbos
    <String>] [<CommonParameters>]
```

1.4.9.9.6 Run Backward Compatibility for Persistent Chat Server

Run Backward Compatibility for Persistent Chat Server

See Also

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets >

Topic Last Modified: *2013-02-21*

The Lync Server 2013, Persistent Chat Server endpoint provides a way to create a simple URL that points to a Persistent Chat Server pool. This is useful for legacy clients (Microsoft Office Communications Server 2007 R2 Group Chat Server or Lync Server 2010, Group Chat) because users can enter a simple URL in the manual configuration when trying to point the legacy client to a computer running Lync 2013, Persistent Chat. This endpoint isn’t used by Persistent Chat, and is required for legacy clients only. This is useful for the interim period where rooms may be migrated, but the Lync 2013 clients have not been deployed throughout the organization. Users running Lync 2010 Group Chat (client) can then still connect to the Persistent Chat Server Back End Server.

You don’t need to create multiple Persistent Chat Server endpoints; you just need one for each Persistent Chat Server pool. Administrators can create multiple endpoints (one per pool), but legacy clients can be configured to connect to only one pool at a time. In the usual or mainstream scenario, the legacy deployment is one pool only. A new deployment generally migrates that pool to a new Lync Server 2013 and might add some new additional Persistent Chat Server pools.

This mainstream scenario generally follows this pattern:

- You administer users with one Lync Server 2010, Group Chat pool, and your Lync 2010 Group Chat clients connect to that pool by using some well-known user (either default sip:ocschat@<*domainName*>.com, or a similar one). The users are SIP-enabled Active Directory Domain Services (AD DS), and the Lookup service registers with them to receive incoming requests.
- Subsequently, you install a Lync Server 2013 Persistent Chat Server and Persistent Chat Server pool.
- During a time when users are generally offline (for example, a weekend):
  - Turn off Lync Server 2010, Group Chat.
  - Migrate data from the Lync Server 2010, Group Chat pool to the Lync Server 2013 Persistent Chat Server pool.
  - Delete the well-known user from the Active Directory Domain Services (AD DS).
  - Create a new *legacy endpoint* with the same SIP URI as the previously deleted well-known user.
  - Start the Lync Server 2013, Persistent Chat Servers.
- Users log back on by using their Lync 2010 Group Chat (client) and connect to their data without needing to change any configuration.
- At a later time, you can decommission the Lync Server 2010, Group Chat. Subsequently, you can deploy Lync Server 2013, Persistent Chat Server, and install new Lync Server 2013 Persistent Chat Server pools.

For details about migrating from Lync Server 2010, Group Chat to Lync Server 2013, Persistent Chat Server, see Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server.

To run backward compatibility (to create a Persistent Chat Server endpoint that points to a Persistent Chat Server pool, which can be used by legacy Group Chat pool clients):

```
New-CsPersistentChatEndpoint -SipAddress <CO name, ex. persistentchat@contoso.com
```

Next, configure Persistent Chat clients to use that SIP address as their contact object. The SIP address is created with the **New-CsPersistentChatEndpoint** cmdlet for a specific Persistent Chat Server pool.

To add the Persistent Chat Server endpoint by using Windows PowerShell command-line interface, consider the following example. In this case, you are configuring the contact object to be named "persistentchat" on the "contoso.com" topology, where the pool fully qualified domain name (FQDN) is "pcpool.contoso.com":

```
New-CsPersistentChatEndpoint -SipAddress sip:persistentchat@contoso.com -Persiste
```

Concepts

Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server

1.4.9.9.7 Run, Grant, Get, Remove, or Set Persistent Chat Policy

Run, Grant, Get, Remove, or Set Persistent Chat Policy

[Deployment](#) > [Deploying Persistent Chat Server](#) > [Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets](#) >

Topic Last Modified: *2012-10-01*

To create a new Persistent Chat policy

```
New-CsPersistentChatPolicy -Identity <XdsIdentity> [-Enable <Switch Parameter>] [
```

To grant Persistent Chat policy

```
Grant-CsPersistentChatPolicy -Identity <UserIdParameter> -PolicyName <String> [-C
```

To get Persistent Chat policy

```
Get-CsPersistentChatPolicy [-Identity <XdsIdentity>] [-Filter <String>] [-LocalSt
```

To remove Persistent Chat policy

```
Remove-CsPersistentChatPolicy -Identity <XdsIdentity> [-Confirm <Switch Parameter
```

To set Persistent Chat policy

```
Set-CsPersistentChatPolicy [-Identity <XdsIdentity>] [-Instance < PSObject>]
```

1.4.9.9.8 Configure Persistent Chat Server

Configure Persistent Chat Server

[Deployment](#) > [Deploying Persistent Chat Server](#) > [Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets](#) >

Topic Last Modified: *2012-10-06*

To create a new Persistent Chat configuration

```
New-CsPersistentChatConfiguration -Identity <XdsIdentity> [-DefaultChatHistory <I
```

To get Persistent Chat configuration

```
Get-CsPersistentChatConfiguration [-LocalStore <Switch Parameter>] [-Identity <Xd
```

To remove Persistent Chat configuration

```
Remove-CsPersistentChatConfiguration -Identity <XdsIdentity>
```

To set Persistent Chat configuration

```
Set-CsPersistentChatConfiguration [-DefaultChatHistory <Integer>] [-MaxChatConten
```

For Lync Server 2013, all web service traffic is supported on the Lync Server 2013, Front End Servers. Therefore, the gcweb01 address on Persistent Chat Server is not necessary. We still support internal web service access because we provide the File Upload/ Download Web service to the *internal* website only (not to the *external* website for remote users).

1.4.9.9.9 Get Persistent Chat Server Pool Availability

Get Persistent Chat Server Pool Availability

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets >

Topic Last Modified: *2012-03-23*

To get Persistent Chat Server pool availability

```
Get-CsService -PersistentChatServer
```

1.4.9.9.10 Persistent Chat Compliance

Persistent Chat Compliance

Deployment > Deploying Persistent Chat Server > Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets >

Topic Last Modified: *2012-10-06*

To create a new Persistent Chat compliance configuration

```
New-CsPersistentChatComplianceConfiguration -Identity <XdsIdentity> [-AdapterName
```

To get Persistent Chat compliance configuration

```
Get-CsPersistentChatComplianceConfiguration [-Identity <XdsIdentity>] [-LocalStor
```

To set Persistent Chat compliance configuration

```
Set-CsPersistentChatComplianceConfiguration -Identity <XdsIdentity> [-AdapterName
```

To remove Persistent Chat compliance configuration

```
Remove-CsPersistentChatComplianceConfiguration -Identity <XdsIdentity> [-Confirm
```

1.4.9.10 Troubleshooting Persistent Chat Server Configuration using Windows PowerShell Cmdlets

Troubleshooting Persistent Chat Server Configuration using Windows PowerShell Cmdlets

Microsoft Lync Server 2013 > Deployment > Deploying Persistent Chat Server >

Topic Last Modified: *2012-10-06*

Use the following workarounds to resolve Persistent Chat Server configuration issues with Windows PowerShell command-line interface cmdlets.

- If the "principal not provisioned" error message appears, the principal that you tried to add is not available.

  > **Tip:**
  >
  > Workaround — No workaround. This error message means that the principal is not available.

1.4.9.11 Configuring Persistent Chat Server for High Availability and Disaster Recovery

Configuring Persistent Chat Server for High Availability and Disaster Recovery

Microsoft Lync Server 2013 > Planning > Planning for High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-01*

The Lync Server 2013, Persistent Chat Server services use a *stretched pool* configuration for disaster recovery. A stretched pool is a pool that has computers that are distributed between two physical data centers, but are within a single logical Lync Server site.

In This Section

1.4.9.11.1 Required Resources

Required Resources

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-01*

High availability and disaster recovery for Persistent Chat Server requires additional resources beyond what is typically needed for full operation. Before configuring Persistent Chat Server for high availability and disaster recovery, ensure that you have the following resources in addition to what is required for standard Persistent Chat Server operation. For additional configuration information, see Configuring Persistent Chat Server.

- One dedicated database instance located in the same physical data center in which the home front end of the Persistent Chat Server service is located. This database will serve as the SQL Server mirror for the primary Persistent Chat database. Optionally, designate an additional SQL Server to serve as the mirroring witness if you want an automated failover to the mirror database.
- One dedicated database instance located in the other physical data center. This database will serve as the SQL Server Log Shipping secondary database for the database in the primary data center.
- One dedicated database instance to serve as the SQL Server mirror for the secondary database. Optionally, designate an additional SQL Server to server as the mirroring witness. Both of these must be located in the same physical data center as the secondary database.
- If Persistent Chat Server compliance is enabled, an additional three dedicated database instances are required. Their distribution is the same as those previously outlined for the Persistent Chat database. While it is possible for the compliance database to share the same SQL Server instance as the Persistent Chat database, we recommend standalone instances for high availability and disaster recovery.
- A file share must also be created and designated for the SQL Server Log Shipping transaction logs. This share must have read/write privileges to all the

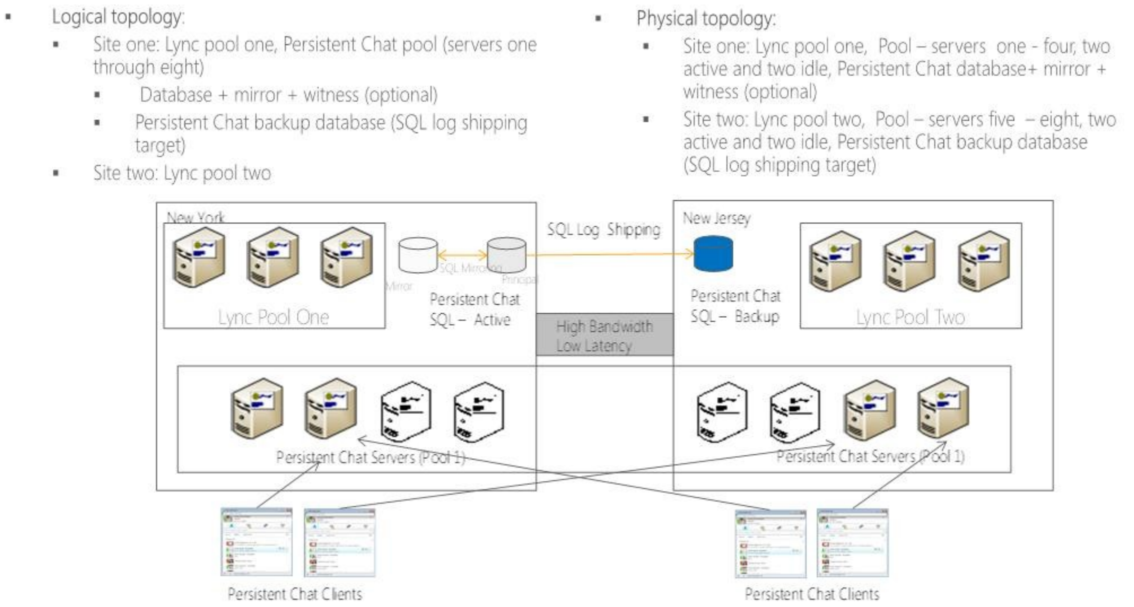
SQL Server services that are running the Persistent Chat databases in both data centers. This share is not defined as part of a FileStore role.

- A file share on the secondary database server to serve as the destination folder for the SQL Server transaction logs that are copied from the primary server file share.

The following figures provide examples about how the entire Persistent Chat Server pool can be configured in the two different stretched pool topologies:

- Stretched Persistent Chat Server pool when data centers are geo-located with high bandwidth/low latency.
- Stretched Persistent Chat Server pool when data centers are geo-located with low bandwidth/high latency.

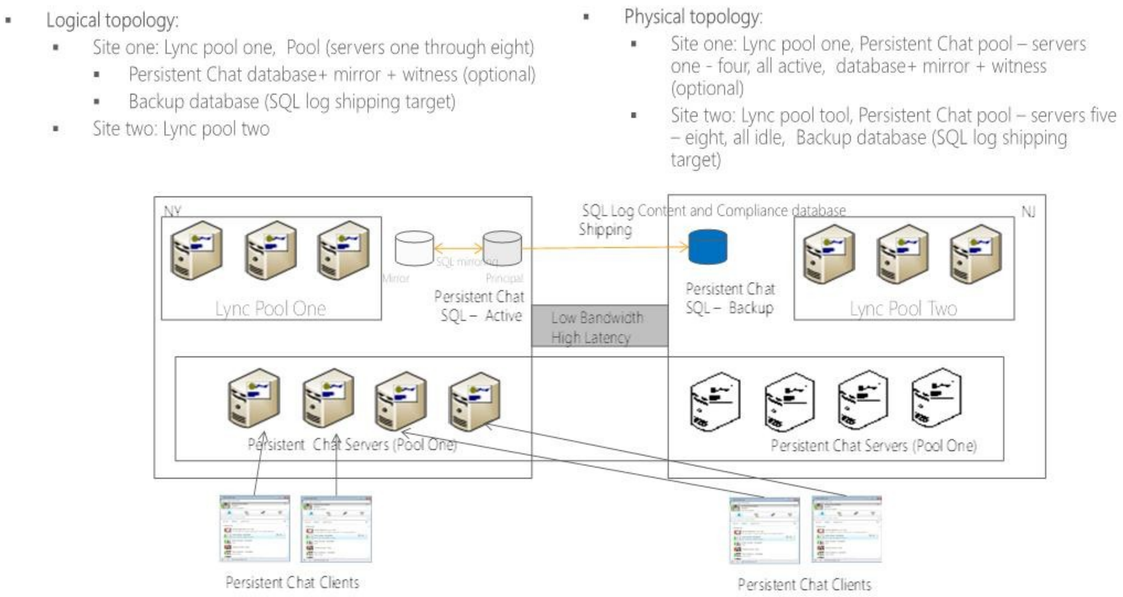
The following figure shows a stretched Persistent Chat Server pool topology where data centers are geo-located with high bandwidth/low latency.



- Logical topology:
  - Site one: Lync pool one, Persistent Chat pool (servers one through eight)
    - Database + mirror + witness (optional)
    - Persistent Chat backup database (SQL log shipping target)
  - Site two: Lync pool two
- Physical topology:
  - Site one: Lync pool one, Pool – servers one - four, two active and two idle, Persistent Chat database+ mirror + witness (optional)
  - Site two: Lync pool two, Pool – servers five – eight, two active and two idle, Persistent Chat backup database (SQL log shipping target)

New York
Lync Pool One
Mirror
SQL Mirroring
Principal
Persistent Chat SQL – Active
SQL Log Shipping
High Bandwidth Low Latency
New Jersey
Persistent Chat SQL – Backup
Lync Pool Two
Persistent Chat Servers (Pool 1)
Persistent Chat Servers (Pool 1)
Persistent Chat Clients
Persistent Chat Clients

The following figure shows a stretched Persistent Chat Server pool topology where data centers are geo-located with low bandwidth/high latency.



- Logical topology:
  - Site one: Lync pool one, Pool (servers one through eight)
    - Persistent Chat database+ mirror + witness (optional)
    - Backup database (SQL log shipping target)
  - Site two: Lync pool two
- Physical topology:
  - Site one: Lync pool one, Persistent Chat pool – servers one - four, all active, database+ mirror + witness (optional)
  - Site two: Lync pool tool, Persistent Chat pool – servers five – eight, all idle, Backup database (SQL log shipping target)

NY
Lync Pool One
SQL mirroring
Mirror
Principal
Persistent Chat SQL – Active
SQL Log Shipping
Content and Compliance database
Low Bandwidth High Latency
NJ
Persistent Chat SQL – Backup
Lync Pool Two
Persistent Chat Servers (Pool One)
Persistent Chat Servers (Pool One)
Persistent Chat Clients
Persistent Chat Clients

1.4.9.11.2 Using Topology Builder to Configure High Availability and Disaster Recovery

Using Topology Builder to Configure High Availability and Disaster Recovery

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-06*

Perform the following steps within Topology Builder to configure high availability and disaster recovery for Persistent Chat Server.

1. Add the mirror databases and the log shipping secondary database SQL Server stores.
2. Edit the Persistent Chat Server service properties to:
   2.a.Enable mirroring for the primary database.
   2.b.Add the primary mirror SQL Server store.
   2.c.Enable the SQL Server Log Shipping database.
   2.d.Add the SQL Server Log Shipping secondary SQL Server store.
   2.e.Add the SQL Server store mirror for the secondary database.
   2.f.Publish the topology.

1.4.9.11.3 Using a Stretched Persistent Chat Server Pool for Disaster Recovery

Using a Stretched Persistent Chat Server Pool for Disaster Recovery

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-06*

The disaster recovery solution for Persistent Chat Server is built on a stretched Persistent Chat Server pool. This is similar to metropolitan site resiliency in Lync Server 2010;

however, there is no requirement for a stretched virtual local area network (VLAN). By stretching Persistent Chat Server pool, you essentially configure one pool in the topology logically, but you physically place the servers in the pool in two different data centers. Configure SQL Server mirroring for the database in the same way, and deploy the database and the mirror in the same data center. You need to configure a backup database in the secondary data center (with an optional mirror to provide high availability during disaster recovery). This is the backup database used for failover during disaster recovery.

For details about how to configure SQL Server mirroring for high availability, see SQL Server Mirroring. For details about failing over the database for disaster recovery, see Setting Up SQL Server Log Shipping for the Persistent Chat Server Primary Database and Setting Up SQL Server Log Shipping between the Primary Mirror and the Log Shipping Secondary Database.

1.4.9.11.4 SQL Server Mirroring

SQL Server Mirroring

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-29*

Establish the SQL Server mirroring session between the primary Persistent Chat database and its mirror. For information about how to deploy SQL Server mirroring, see Deploying SQL Mirroring for Back End Server High Availability.

1.4.9.11.5 Setting Up SQL Server Log Shipping for the Persistent Chat Server Primary Database

Setting Up SQL Server Log Shipping for the Persistent Chat Server Primary Database

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2012-11-12*

Using SQL Server Management Studio, connect to the Persistent Chat Server secondary Log Shipping database instance, and be sure that SQL Server Agent is running.

Using SQL Server Management Studio connected to the Persistent Chat primary database instance, perform the following steps:

1. Be sure that the SQL Server Agent is running.
2. Right-click the mgc database, and then click **Properties**.
3. Under **Select a page**, click **Transaction Log Shipping**.
4. Select the **Enable this as a primary database in a log shipping configuration** check box.
5. Under **Transaction log backups**, click **Backup Settings**.
6. In the **Network path to the backup folder** box, type the network path to the share that you created for the transaction log backup folder.
7. If the backup folder is located on the primary server, type the local path to the backup folder in the **If the backup folder is located on the primary server, type a local path to the folder (example: c:\backup)** box. (If the backup folder is not on the primary server, you can leave this box empty.)

> **Important:**
> If the SQL Server service account on your primary server runs under the local system account, you must create your backup folder on the primary server and specify a local path to that folder.

8. Configure the **Delete files older than** and **Alert if no backup occurs within** parameters.
9. Look at the backup schedule listed in the **Schedule** box under **Backup job**. To customize the schedule for your installation, click **Schedule**, and adjust the SQL Server Agent schedule as required.
10. Under **Compression**, select **Use the default server setting**, and then click **OK**.
11. Under **Secondary server instances and databases**, click **Add**.
12. Click **Connect** and connect to the instance of SQL Server that you have configured as your secondary server.
13. In the **Secondary Database** box, select the **mgc** database from the list.
14. On the **Initialize Secondary database** tab, choose the option **Yes, generate a full backup of the primary database and restore it into the secondary database (and create the secondary database if it doesn't exist)**.
15. On the **Copy Files** tab, in the **Destination folder for copied files** box, type the path of the folder into which the transaction logs backups should be copied. This folder is often located on the secondary server.
16. Note the copy schedule listed in the **Schedule** box under **Copy job**. To customize the schedule for your installation, click **Schedule**, and adjust the SQL Server Agent schedule as required. This schedule should be approximately the same as the backup schedule.
17. On the **Restore** tab, under **Database state when restoring backups**, choose the **No recovery mode** option.
18. Under **Delay restoring backups at least:**, select **0 minutes**.
19. Choose an alert threshold under **Alert if no restore occurs within**.
20. Look at the restore schedule listed in the **Schedule** box under **Restore job**. To customize the schedule for your installation, click **Schedule**, adjust the SQL Server Agent schedule as required, and click **OK**. This schedule should be approximately the same as the backup schedule.
21. On the **Database Properties** dialog box, click **OK** to begin the configuration process.

1.4.9.11.6 Setting Up SQL Server Log Shipping between the Primary Mirror and the Log Shipping Secondary Database

Setting Up SQL Server Log Shipping between the Primary Mirror and the Log Shipping Secondary Database

See Also

Planning > Planning for High Availability and Disaster Recovery > Configuring Persistent Chat Server for High Availability and Disaster Recovery >

Topic Last Modified: *2013-02-21*

Perform the following steps for log shipping to continue if the primary Persistent Chat database is failed over to its mirror database.

1. Manually fail over the primary Persistent Chat database to the mirror. This is done by using the Lync Server Management Shell and the **Invoke-CsDatabaseFailover** cmdlet. For details, see "Using Lync Server Management Shell Cmdlets" in Deploying SQL Mirroring for Back End Server High Availability.
2. Using the SQL Server Management Studio, connect to the primary Persistent

Chat Server mirror instance.

3. Be sure that the SQL Server Agent is running.
4. Right-click the mgc database, and then click **Properties**.
5. Under **Select a page**, click **Transaction Log Shipping**.
6. Select the **Enable this as a primary database in a log shipping configuration** check box.
7. Under **Transaction log backups**, click **Backup Settings**.
8. In the **Network path to the backup folder** box, type the network path to the share you created for the transaction log backup folder.
9. If the backup folder is located on the primary server, type the local path to the backup folder in the **If the backup folder is located on the primary server, type a local path to the folder** box. (If the backup folder is not on the primary server, you can leave this box empty.)

> **Important:**
> If the SQL Server service account on your primary server runs under the local system account, you must create your backup folder on the primary server and specify a local path to that folder.

10. Configure the **Delete files older than** and **Alert if no backup occurs within** parameters.
11. Look at the backup schedule listed in the **Schedule** box under **Backup job**. To customize the schedule for your installation, click **Schedule**, and adjust the SQL Server Agent schedule, as required.

> **Important:**
> Use the same settings that you used for the primary database.

12. Under **Compression**, select **Use the default server setting**, and click **OK**.
13. Under **Secondary server instances and databases**, click **Add**.
14. Click **Connect**, and connect to the instance of SQL Server that you have configured as your secondary server.
15. In the **Secondary Database** box, select the **mgc** database from the list.
16. On the **Initialize Secondary database** tab, select the option **No, the secondary database is initialized**.
17. On the **Copy Files** tab, in **Destination folder for copied files**, type the path of the folder into which the transaction logs backups should be copied, and click **OK**. This folder is often located on the secondary server.
18. Open the **Script Configuration** drop-down list, and select **Script Configuration to New Query Window**.
19. In the new query window, in **Database Properties**, click **OK** to begin the configuration process.
20. Select and run the first half of the query (see step 18) up to the line: -- ****** End: Script to be run at Primary: ******.

> **Important:**
> Manually running this script is necessary because SQL Server Management Studio does not support multiple primary databases in a SQL Server Log Shipping configuration.

21. Select **Cancel** to close the Log File shipping configuration panel and to establish a working setup that correctly implements the log file shipping for both the primary and mirrored database (in case of failover).
22. Manually fail back the primary Persistent Chat database to the primary. This is done by using the Lync Server Management Shell, and the **Invoke-CsDatabaseFailover** cmdlet. For details, see "Using Lync Server Management Shell Cmdlets" in Deploying SQL Mirroring for Back End Server High Availability.

Concepts

Deploying SQL Mirroring for Back End Server High Availability
Deploying SQL Mirroring for Back End Server High Availability

1.4.10 Deploying Clients and Devices

Deploying Clients and Devices

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2013-01-15*

This section outlines the procedures for deploying Lync Server 2013 clients and devices.

In This Section

- Deploying Lync Clients
- Deploying the Lync VDI Plug-in
- Deploying Lync Web App
- Deploying Devices
- Deploying Mobile Clients
- Deploying Lync Windows Store App
- Using Lync Connectivity Analyzer

1.4.10.1 Deploying Lync Clients

Deploying Lync Clients

Microsoft Lync Server 2013 > Deployment > Deploying Clients and Devices >

Topic Last Modified: *2012-10-03*

Lync 2013 introduces a different approach to client deployment. In a departure from previous releases, Lync 2013 no longer has its own installer. Instead, Lync is included with the Office 2013 setup program. To deploy Lync 2013 to your users, you can use Office 2013 installation methods and customization tools.

- **Office 2013 Windows Installer** is a Windows Installer-based installation package that consists of multiple MSI files. A language-neutral core MSI package is combined with one or more language-specific packages to make a complete product. Setup assembles the individual packages and performs customization and maintenance tasks during and after installation of Office on users' computers. The topics in this section describe how to use and customize the Office 2013 Windows Installer to deploy Lync 2013.
- **Office 2013 Click-to-Run** is an installation program that streams Office setup files to the user from the Microsoft Office 365 portal. Administrators can customize installation by using the Office Deployment Tool for Click-to-Run. Because Office 2013 Click-to-Run is primarily used in the Microsoft Office 365 environment, this installation method is not described in detail in this section. Detailed information about using and customizing Click-to-Run installation is available in the Office 2013 Resource Kit documentation. Administrators can also download the Office 2013 Click-to-Run program and language source files to an on-premises location, which is useful when you want to minimize the demand on the network or prevent users from installing software from the Internet because of corporate security requirements.

The topics in this section focus on how to deploy clients by using the Office 2013 MSI-based installer. Your primary reference should be the Office 2013 Resource Kit documentation, which describes in detail how to prepare your infrastructure, customize setup, and deploy Office 2013. However, you should use the Office documentation in conjunction with topics in this section, which point out deployment considerations that are specific to Lync 2013.

Note:

- The Online Meeting Add-in for Lync 2013, which supports meeting management from within the Outlook messaging and collaboration client, installs automatically with Lync 2013.
- The Office 2013 setup program does not uninstall previous versions of Lync or Office Communicator. The Lync 2013 client installs side-by-side with other Lync or Office Communicator clients

In This Section

- Customizing Client Installation
- Customizing Lync Behavior and the User Interface
- Customizing the Online Meeting Add-in
- Configuring the Meeting Join Page
- Configuring Supported Client Versions
- Configuring Enhanced Presence Privacy Mode

1.4.10.1.1 Customizing Client Installation

Customizing Client Installation

Deployment > Deploying Clients and Devices > Deploying Lync Clients >

Topic Last Modified: *2012-10-03*

Enterprise administrators can customize the Office 2013 Windows Installer-based (.msi) installation by using the methods discussed in this section. Because no single tool provides all customization options, you'll likely use a combination of these methods in your Lync 2013 deployment. At a minimum, you might use the tools described in the following sections:

- Using the Office Customization Tool (OCT) to customize setup options and features for Lync and other Office programs.
- Using Config.xml to Perform Installation Tasks to specify the path of the network installation point and perform silent installation.
- Using Setup Command-Line Options to specify the Config.xml file to use during installation.
- Configuring Client Bootstrapping Policies by using the Group Policy Object Editor MMC snap-in.

There will probably be other options you'll want to configure as you deploy the Office suite of products. The topics in this section give an overview of these customization tools and discuss Lync-specific considerations. Included are links to detailed Office help for each tool.

1.4.10.1.1.1 Using the Office Customization Tool (OCT)

Using the Office Customization Tool (OCT)

Deploying Clients and Devices > Deploying Lync Clients > Customizing Client Installation >

Topic Last Modified: *2012-10-02*

The Office Customization Tool (OCT) is part of the Setup program and is the recommended tool for many customizations. By using the OCT, you customize Office and save your customizations in a Setup customization .msp file. You place the file in the Updates folder on the network installation point. When you install Office, Setup looks for a Setup customization file in the Updates folder and applies the customizations. The Updates folder can be used only to deploy software updates during an initial installation of Office 2013.

The OCT is part of setup and it is included in volume license versions of the product. You run the OCT by typing `setup.exe /admin` at the command line from the root of the network installation point that contains the Office 2013 source files. For example, use the following:

```
\\server\share\Office15\setup.exe /admin
```

Administrators use the OCT to create a setup customization .msp file. As in the Microsoft Office 2010 OCT, administrators can customize the following areas:

- **Setup** Used to specify default installation location on the client and default organization name, additional network installation sources, product key, end-user license agreement, display level, earlier versions of Office to remove, custom programs to run during installation, security settings, and Setup properties.
- **Features** Used to configure user settings and to customize how Office features are installed. Administrators can use the OCT to specify initial default values of Office application settings for users. Users can modify most of the settings after the installation.
- **Additional content** Used to add or remove files, add or remove registry entries, and configure shortcuts.
- **Outlook** Used to customize a user's default Outlook profile, specify Exchange settings, add accounts, remove accounts and export settings, and specify Send\Receive groups.

For information about the OCT, see http://go.microsoft.com/fwlink/p/?linkid=267516.

1.4.10.1.1.2 Using Config.xml to Perform Installation Tasks

Using Config.xml to Perform Installation Tasks

Deploying Clients and Devices > Deploying Lync Clients > Customizing Client Installation >

Topic Last Modified: *2012-10-02*

Although the Office Customization Tool (OCT) is the primary tool for customization installation, administrators can use the Config.xml file to specify additional installation instructions that are not available in the OCT. The following customizations can only be made by using the Config.xml file:

- Specify the path of the network installation point.
- Select the products to install.
- Configure logging and the location of the Setup customization file and software updates.
- Specify installation options, such as user name.
- Copy the local installation source (LIS) to the user's computer without installing Office.
- Add or remove languages from the installation.

We recommend that you use the Config.xml file to configure Lync 2013 silent installation.

By default, the Config.xml file that is stored in the core product folder (for example, \*product*.WW) directs Setup to install that product. For example, the Config.xml file in the following folder installs Lync 2013:

- \\server\share\Lync15\Lync.WW \Config.xml

The Config.xml elements most commonly used for Lync 2013 installation are listed in the following table.

Config.xml elements

Element	Description
Configuration	Top-level element (required). Contains the Product attribute, for example: Product=Lync
OptionState	Specifies how specific product features are handled during installation. Use the following attributes to prevent installation of Business Connectivity Services, which includes shared components that interfere with Outlook 2010: • Id="LOBiMain" • State="Absent" • Children="Force"
Display	The level of UI that Setup displays to the user. Typical attributes include the following: • CompletionNotice="Yes" | "No"(default) • AcceptEula="Yes" | "No"(default)
Logging	Options for the kind of logging that Setup performs. Typical attributes include the following: • Type ="Off" | "Standard"(default) | "Verbose" • Template=”*filename*.txt” (the name of the log file)
Setting	Specifies values for Windows Installer properties. Typical attributes include the following: • Setting Id="*name*" (the name of the Windows Installer property) • Value="*value*" (the value to assign to the property)
DistributionPoint	The fully qualified path of the network installation point from which the installation is to run. Includes the Location attribute: • Location=”*path*”

The following example shows a Config.xml file for a typical silent installation of Lync 2013.

```
<Configuration Product="Lync">
  <OptionState Id="LOBiMain" State="Absent" Children="Force" />
  <Display Level="None" CompletionNotice="No" AcceptEula="Yes" />
  <Logging Type="verbose" Path="%temp%" Template="LyncSetupVerbose(*).log" />
  <Setting Id="SETUP_REBOOT" Value="Never" />
  <DistributionPoint Location="\\server\share\Lync15" />
</Configuration>
```

Detailed information about using the Config.xml file to perform Office installation and maintenance tasks is available at http://go.microsoft.com/fwlink/p/?linkid=267514.

To customize the Config.xml file

1. Open the Config.xml file by using a text editor tool, such as Notepad.
2. Locate the lines that contain the elements you want to change.
3. Modify the element entry with the silent options that you want to use. Make sure that you remove the comment delimiters, "<!--" and "-->". For example, use the following syntax:

```
< DistributionPoint Location="\\server\share\Lync15" />
```

4.Save the Config.xml file.

1.4.10.1.1.3 Using Setup Command-Line Options

Using Setup Command-Line Options

[Deploying Clients and Devices](#) > [Deploying Lync Clients](#) > [Customizing Client Installation](#) >

Topic Last Modified: *2012-10-03*

The Setup.exe command line is used for very few operations in Office setup. Instead of using the Setup command-line options, you’ll typically use the Office Customization Tool and the Config.xml file for product setup and feature customization.

The Office Setup.exe command line recognizes the command-line options described in the following table.

Office Setup Command-Line Options

Setup Command-Line Option	Description
/admin	Runs the Office Customization Tool to create a Setup customization file (.msp file).
/adminfile [path]	Applies the specified Setup customization file to the installation. You can specify a path of a specific customization file (.msp file) or to the folder where you store customization files.
/config [path]	Specifies the Config.xml file that Setup uses during the installation. Use the /config option to specify the Config.xml file you customized for Lync 2013 installations, for example: `/config \\server\share\Lync15\Lync.WW\Config.xml`
/modify Lync	Used with a modified Config.xml file to run Setup in maintenance mode and make changes to an existing Office installation. For example, you can use the /modify option to add or remove Lync features.
/repair Lync	Runs Setup from the user’s computer to repair Lync.
/uninstall Lync	Runs Setup to remove Lync from the user’s computer.

For details about using the setup command-line options, see http://go.microsoft.com/fwlink/p/?linkid=267515.

1.4.10.1.1.4 Configuring Client Bootstrapping Policies

Configuring Client Bootstrapping Policies

Deploying Clients and Devices > Deploying Lync Clients > Customizing Client Installation >

Topic Last Modified: *2013-02-21*

The Group Policy Management Console (GPMC) and the Group Policy Object Editor are tools that you use to manage Group Policy. Included with the Office Group Policy Administrative Template are Lync 2013.admx (ADMX) and .adml (ADML) Administrative Templates, which contain the registry-based policy settings that you configure for Group Policy objects in the domain. ADML files are language-specific complements to ADMX files. Each ADMX and ADML file contains the policy settings for a single Office application. For more information, see "Office 2013 Administrative Template files (ADMX, ADML)" in the Office 2013 documentation at http://go.microsoft.com/fwlink/p/?linkid=267516.

For Lync 2013, there are several client bootstrapping policies that you should consider configuring before users sign in to the server for the first time. For example, the default servers and security mode that the client should use until sign-in is complete. You can use Group Policy to establish these settings in users' computer registries before they sign in and begin receiving in-band provisioning settings from the server. The following table lists the Group Policy settings that are available for Lync 2013.

Group Policy Settings for Lync 2013

Group Policy setting	Description
Specify Server (ConfigurationMode)	Specifies how Lync 2013 identifies the transport and server to use during sign-in. Within this setting, you specify the following: • ServerAddressExternal: Specifies the server name or IP address used by clients and federated contacts when connecting from outside the external firewall. • ServerAddressInternal: Specifies the server name or IP address used when clients connect from inside the organization's firewall. • Transport: Specifies either Transmission Control Protocol (TCP) or Transport Layer Security (TLS).
Additional server versions supported (ConfiguredServerCheckValues)	Specifies a list of server version names separated by semi-colons that Lync Server 2013 will log on to, in addition to the server versions that are supported by default.
Disable automatic upload of sign-in failure logs (DisableAutomaticSendTracing)	Automatically uploads sign-in failure logs to Lync Server for analysis. No logs are automatically uploaded if sign-in is successful. If this policy is not configured, the following happens: • For Lync Online users: Sign-in failure logs are automatically uploaded. • For Lync on-premises users: A confirmation dialog box is shown to the user before upload. When this setting is disabled, sign-in logs are automatically uploaded to the Lync Server for both

	Lync on-premises and Lync Online users. When this setting is enabled, sign-in logs are never uploaded automatically.
Disable HTTP fallback for SIP connection (DisableHttpConnect)	Prevents Lync Server from trying to connect to the server by using HTTP, if TLS or TCP are unavailable. By default, Lync first attempts to connect to the server by using TLS or TCP and, if neither of these transport methods is successful, Lync tries to connect by using HTTP. Use this policy to disable the fallback HTTP connection attempt.
Require logon credentials (DisableNTCredentials)	Requires the user to provide logon credentials for Lync rather than automatically using Windows credentials during sign-in to a SIP server.
Disable server version check (DisableServerCheck)	If you set this policy to 1, prevents Lync from checking the server name and version before signing in. By default, Lync makes these checks before signing in.
Enable using BITS to download Address Book Service files (EnableBitsForGalDownload)	Enables Lync to use Background Intelligent Transfer Service (BITS) to download the Address Book Services files.
Configure SIP security mode (EnableSIPHighSecurityMode)	Enables Lync to send and receive instant messages more securely. This policy has no effect on Windows .NET or Microsoft Exchange Server services. If you do not configure this policy setting, Lync can use any transport. But if it does not use TLS and if the server authenticates users, Lync must use either NTLM or Kerberos authentication.
Global Address Book Download Initial Delay (GalDownloadInitialDelay)	Specifies the time period before a download of the global address list (GAL) occurs. The default value is 60 minutes, which means the server delays the download of GAL file for a random period of between 0 and 60 minutes.
Prevent users from running Microsoft Lync (PreventRun)	Prevents users from running Lync. You can configure this policy setting under both Computer Configuration and User Configuration, but the policy setting under Computer Configuration takes precedence.
Allow storage of user passwords (SavePassword)	Enables Lync to store passwords.
Configure SIP compression mode (SipCompression)	Specifies when to turn on SIP compression. By default, SIP compression is enabled based on the adapter speed. Note that setting this policy might cause an increase in sign-in time.
Trusted Domain List (TrustModelData)	Lists the trusted domains that do not match the prefix of the customer SIP domain.

Policies configured on the server take precedence over Group Policy settings and client options configured by the user. The following table summarizes the order in which settings take precedence when a conflict occurs.

Group Policy Precedence

Precedence	Location or Method of Setting
1	Lync Server 2013 in-band provisioning
2	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\15.0\Lync
3	HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\15.0\Lync
4	The Lync - Options dialog box in Lync 2013

⊟To define Group Policy settings by using the Lync 2013 administrative template files

1. Create a root-level folder to contain all language-neutral ADMX files. For example, create the root folder for the central store on your domain controller at this location:
   `%systemroot%\sysvol\domain\policies\PolicyDefinitions`

Note:
This procedure assumes that you want to manage multiple computers in your domain. In this case, you store the templates in a central store in the Sysvol folder on the primary domain controller. This provides a replicated central storage location for domain Administrative Templates.

2. Create a subfolder for each language that you'll use. These subfolders will contain the language-specific ADML resource files. For example, create a subfolder for United States English (EN-US) at this location:
   `%systemroot%\sysvol\domain\policies\PolicyDefinitions\EN-US`

1.4.10.1.2 Customizing Lync Behavior and the User Interface

Customizing Lync Behavior and the User Interface

Deployment > Deploying Clients and Devices > Deploying Lync Clients >

Topic Last Modified: *2013-02-20*

This section describes how to add custom features to Lync 2013.

- Configuring Media Port Range Settings
- Adding Commands to Lync Menus
- Integrating a Third-Party Collaboration Application with Lync
- Configuring Custom Presence States
- Adding a Custom Link to Lync Error Messages
- Adding Custom Text to Instant Messages
- Starting Lync from Another Application

1.4.10.1.2.1 Configuring Media Port Range Settings

Configuring Media Port Range Settings

Deploying Clients and Devices > Deploying Lync Clients > Customizing Lync Behavior and the User Interface >

Topic Last Modified: *2012-10-18*

Media port range settings can significantly impact client performance and should be configured. You can configure these settings by using Lync Server Management Shell.

Media Port Range Settings

Setting	Description	Lync Server Management Shell cmdlet	Cmdlet parameters
Portrange\Enabled	Specifies whether the port ranges sent by the server should be used by the client for media and signaling. Used in conjunction with the subvalues MinMediaPort and MaxMediaPort.	**CsConferencingConfiguration**	ClientMediaPortRange Enabled
Portrange \MinMediaPort	Specifies the starting port number to use for media. Combines with MaxMediaPort to specify the range of ports. The recommended minimum range is 40 ports.	**CsConferencingConfiguration**	ClientMediaPort (represents the starting port number to use for client media)
Portrange \MaxMediaPort	Specifies the highest port number to use for media. Combines with MinMediaPort to specify the range of ports. The recommended minimum range is 40 ports.	**CsConferencingConfiguration**	ClientMediaPortRange (indicates the total number of ports available for client media; default is 40)

⊟To Configure Media Port Range Settings

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the following cmdlet:

```
Get-CsConferencingConfiguration
```

   This cmdlet returns the conferencing configuration settings.
3. Run the following cmdlet with the parameters and values you want to change (for details about the parameters for this cmdlet, see the Lync Server Management Shell documentation):

```
Set-CsConferencingConfiguration
```

Note:
You can create additional sets of conferencing configuration settings for specific sites. Use the **New- CsConferencingConfiguration** cmdlet with a site identity. When you create new conferencing configuration settings for sites, the site settings take precedence over the global settings. For details, see

the Lync Server Management Shell documentation.

1.4.10.1.2.2 Adding Commands to Lync Menus

Adding Commands to Lync Menus

Deploying Clients and Devices > Deploying Lync Clients > Customizing Lync Behavior and the User Interface >

Topic Last Modified: *2013-02-20*

You can add custom commands to Lync 2013 menus and pass the SIP Uniform Resource Identifier (URI) of the current user and selected contacts to the application that the custom command starts.

The custom commands that you add can appear on one or more of the following menus:

- The Tools menu, on the menu bar in the Lync main window
- The shortcut menu for contacts in the Contacts list
- The More Options menu, in the Conversation window
- The shortcut menu for people listed in the Conversation window participant list
- The options menu in a contact card

You can define custom commands for two types of applications—applications that do either of the following:

- Apply only to the current user and are started on the local computer.
- Involve additional users, such as an online collaboration program, and must be started on each user's computer.

The custom command can be invoked in the following ways:

- Select one or more users, and then choose the custom command.
- Start a two-party or multiparty conversation, and then choose the custom command.

To add a custom command

Use the registry settings in the following table to add a command to the menus. These entries are placed in the registry at the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\Lync\CustomCommands

Custom Command Registry Entries

Name	Type	Data
Name	REG_SZ	Name of the application as it appears on the menu.
ApplicationType	DWORD	0 = Executable (default) **Note:** Requires ApplicationInstallPath. 1 = Protocol
ApplicationInstallPath	REG_SZ	Full path of the executable. **Note:** Must be specified if

		ApplicationType is 0 (Executable).
Path	REG_SZ	Full path to be started along with any parameters, including the default parameters *%user-id%* and *%contact-id%*.
SessionType	DWORD	0 = Local session. The application is started on the local computer. 1 = Two-party session (default). Lync 2013 starts the application locally and then sends a desktop notification to the other user. The other user clicks the notification to start the application on their computer. 2 = Multiparty session. Lync 2013 starts the application locally and then sends desktop notifications to the other users. The other user clicks the notification to start the specified application on their computer.
ExtensibleMenu	REG_SZ	A list of the menus where this command will appear, separated by semicolons. Possible values are: MainWindowActions MainWindowRightClick ConversationWindowActions ConversationWindowRightClick ContactCardMenu If ExtensibleMenu is not defined, the default values of MainWindowRightClick and ConversationWindowActions are used.

For example, the following Registry Editor (.REG) file shows the results of adding a Contoso Sales Contact Manager menu item to Actions menu in the Conversation window:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\Lync\CustomCommands\{1F9F07C6-
"Name"="Contoso Sales Contact Manager"
"HelpMessage"="The Contoso Sales Contact Manager is not installed. Contact the He
"ApplicationType"=dword:00000000
```

```
"ApplicationInstallPath"="C:\\cscm.exe"
"Path"="C:\\cscm.exe %user-id% %contact-id%"
"SessionType"=dword:00000001
"ExtensibleMenu"="ConversationWindowActions;MainWindowRightClick"
```

To access a custom command

To access a custom command after it is added, do one of the following, depending on the ExtensibleMenu values that you define:

- **MainWindowActions** In the Lync main window, click **Tools**, and then click your custom command.
- MainWindowRightClick In the Lync main window, right-click a contact, and then click your custom command.
- **ConversationWindowActions** In the Conversation window, click the **More Options** icon, and then click your custom command.
- **ConversationWindowRightClick** In the Conversation window, right-click a contact name, and then click your custom command.
- **ContactCardMenu** In a person's contact card, click the options icon, and then click your custom command.

1.4.10.1.2.3 Integrating a Third-Party Collaboration Application with Lync

Integrating a Third-Party Collaboration Application with Lync

Deploying Clients and Devices > Deploying Lync Clients > Customizing Lync Behavior and the User Interface >

Topic Last Modified: *2013-02-20*

You can integrate Lync 2013 with any third-party online collaboration application by adding information about the application to the registry. You can use Lync 2013 to start data conferencing sessions hosted on an in-house server, an Internet-based service, or both. The collaboration or data conferencing session can be started from the Contacts list or from an existing instant messaging, voice, or video session. Lync 2013 acts only as the vehicle for starting the application. Any existing Lync 2013 conversations remain active after the online collaboration session has begun.

The following sections describe how to integrate Lync 2013 with Internet-based and server-based collaboration applications.

Integrating an Internet-Based Collaboration Application with Lync 2013

Generally, the steps involved in integrating a third-party collaboration application are as follows:

1. Information about the application is added to the registry.
2. The organizer signs in to Lync 2013 and selects contacts for data sharing and collaboration. Or, the organizer may already be in a conversation and decide to add data conferencing.
3. Lync 2013 reads the registry, starts the collaboration application, and then sends a custom SIP message—an appINVITE—to the selected participants.
4. Participants accept the invitation, and the collaboration application is started on each person's computer. Lync 2013 uses the registry to determine which collaboration application to use, and then starts that application by using the parameters included in the appINVITE message.

The following table describes the registry entries required to integrate an Internet-based collaboration application with Lync 2013. These entries are placed in the registry in the following location:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Office\15.0\Lync\SessionManager\Apps\Parameters

Registry Entries for an Internet-based Collaboration Application

Name	Type	Data
Name	REG_SZ	The application name for Lync 2013 menus.
SmallIcon	REG_SZ	Path to 16-pixel x 16-pixel icon, BMP or PNG.
Path	REG_SZ	Participant path for starting the online collaboration application.
OriginatorPath	REG_SZ	Organizer path for starting the online collaboration application. This path can contain one or more custom parameters as defined in the Parameters subkey. For example, `https://meetserv.adatum.com/cc/%param1%/join?id=%param2%&role=present&pw=%param3%`
SessionType	DWORD	0 = Local session. The application is started on the local computer. 1 = Two-party session (default). Lync 2013 starts the application locally, and then sends a system notification to the other user. The other user clicks the notification and starts the specified application on their computer. 2 = Multiparty session. Lync 2013 starts the application locally, and then sends system notifications to the other users, prompting them to start the specified application on their own computer.
ExensibleMenu	REG_SZ	A list of the menus where this command will appear, separated by semi-colons. Possible values are: • MainWindowActions • MainWindowRightClick • ConversationWindowActions • ConversationWindowButton • ConversationWindowRightClick If ExtensibleMenu is not defined, the default values of MainWindowRightClick and

		ConversationWindowActions are used.

The following table describes the registry entries for parameters. These entries are place at HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync\SessionManager\Apps \Parameters.

Registry Entries for an Internet-based Collaboration Application

Name	Type	Data
Param1	REG_SZ	Used in tokenized format (%Parm1%) to add user-specific values to the OriginatorPath registry key.
Param2	REG_SZ	See Param1.
Param3	REG_SZ	See Param1.

The following example registry settings integrate ADatum Collaboration Client with Lync 2013:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\Lync\SessionManager]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\Lync\SessionManager\Apps]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\Lync\SessionManager\Apps\{C3F6
"Path"="https://meetingservice.adatum.com/cc/%param1%/meet/%param2%"
"OriginatorPath"="https://meetserv.adatum.com/cc/%param1%/join?id=%param2%&role=p
"SessionType"=dword:00000002
"ApplicationType"=dword:00000001
"LiveServerIntegration"=dword:00000000
"Name"="ADatum Online Collaboration Service"
"Extensiblemenu"="MainWindowActions;MainWindowRightClick;ConversationWindowAction
[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync\SessionManager]
[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync\SessionManager\Apps]
[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync\SessionManager\Apps\Parame
[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync\SessionManager\Apps\Parame
"Param1"="meetserv"
"Param2"="admin"
"Param3"="abcdefg123"
```

Integrating a Server-Based Collaboration Application with Lync 2013

The settings to add commands for starting a server-based collaboration application from within Lync 2013 are similar to those described in the previous section, Integrating an Internet-Based Collaboration Application with Lync 2013. However, the OriginatorPath is not required, and some values are changed. Registry entries are placed in the following location:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Office\15.0\Lync\SessionManager \Apps\Parameters

Registry Entries for a Server-based Collaboration Application

Name	Type	Data
Name	REG_SZ	Name of the application as it appears on the menu.
ApplicationType	DWORD	Value = 1. Sets the application type to

		protocol. The other possible values do not apply in this case. If not present, ApplicationType is set to 0 (executable).
Path	REG_SZ	Protocol used to start the collaboration application. For Live Meeting 2007, the value of Path is set to `meet:%conf-uri%`.
SessionType	DWORD	0 = Local session. The application is started on the local computer. 1 = Two-party session (default). Lync 2013 starts the application locally, and then sends a system notification to the other user. The other user clicks the notification and starts the specified application on their computer. 2 = Multiparty session. Lync 2013 starts the application locally, and then sends system notifications to the other users, prompting them to start the specified application on their computer.
MCUType	REG_SZ	DATA = The type of server.
ExtensibleMenu	REG_SZ	A list of the menus where this command will appear, separated by semicolons. Possible values are: • MainWindowActions • MainWindowRightClick • ConversationWindowActions • ConversationWindowButton • ConversationWindowRightClick If ExtensibleMenu is not defined, the default values of MainWindowRightClick and ConversationWindowActions are used.

The following example adds commands to start ADatum Collaboration Client from within Lync 2013:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\Lync\SessionManager]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\Lync\SessionManager\Apps]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\Lync\SessionManager\Apps\{2787
"Path"="meet:%conf-uri%"
"SessionType"=dword:00000002
"LiveServerIntegration"=dword:00000001
"ApplicationType"=dword:00000001
"Name"="ADatum Collaboration Client"
"MCUType"="Data"
"Extensiblemenu"="MainWindowActions;MainWindowRightClick;ConversationWindowAction
```

Configuring Custom Presence States

Deploying Clients and Devices > Deploying Lync Clients > Customizing Lync Behavior and the User Interface >

Topic Last Modified: *2013-01-10*

To define custom presence states in Lync 2013, create an XML custom presence configuration file, and then specify its location by using the Lync Server Management Shell cmdlets **New-CSClientPolicy** or **Set-CSClientPolicy** with the parameter CustomStateURL.

Configuration files have the following properties:

- Custom presence states can be configured with the Available, Busy, and Do Not Disturb presence indicators.
- The availability attribute determines which presence indicator is associated with the status text of the custom state. In the example later in this topic, the status text Working from Home is displayed to the right of the green (Available) presence indicator.
- The maximum length of the status text is 64 characters.
- A maximum of four custom presence states can be added.
- The CustomStateURL parameter specifies the location of the configuration file. In Lync 2013, SIP high security mode is enabled by default, so you will need to store the custom presence configuration file on a web server that has HTTPS enabled. Otherwise, Lync 2013 clients will be unable to connect to it. For example, a valid address would be `https://lspool.corp.contoso.com/ClientConfigFolder/CustomPresence.xml`.

Note:

Although it is not recommended in a production environment, you can test a configuration file that is located on a non-HTTPS file share by using the EnableSIPHighSecurityMode registry setting to disable SIP high security mode on the client. Then you can use the CustomStateURL registry setting to specify a non-HTTPS location for the configuration file. Note that Lync 2013 honors Lync 2010 registry settings, but the registry hive has been updated. You would create the registry settings as follows:

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\15.0\Lync\EnableSIPHighSecurityMode
  Type: DWORD
  Value data: 0
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\15.0\Lync\CustomStateURL
  Type: String (REG_SZ)
  Value data (examples): file://\\lspool.corp.contoso.com\LSFileShare\ClientConfigFolder\Presence.xml or file:///c:/LSFileShare/ClientConfigFolder/Group_1_Pres.xml

Localize your custom presence state by specifying one or more locale ID (LCID) schema in the XML configuration file. The example later in this topic shows localization into English - United States (1033), Norwegian - Bokmål (1044), French - France (1036), and Turkish (1055). For a list of LCIDs, see Locale IDs Assigned by Microsoft at http://go.microsoft.com/fwlink/p/?linkid=157331.

To add custom presence states to Lync 2013

1. Create an XML configuration file that uses the format of the following example:

```
<?xml version="1.0"?>
<customStates xmlns="http://schemas.microsoft.com/09/2009/communicator
  <customState ID="1" availability="online">
    <activity LCID="1033">Working from Home</activity>
    <activity LCID="1044">activity 2 for 1044</activity>
    <activity LCID="1055">activity 3 for 1055</activity>
  </customState>
  <customState ID="2" availability="busy">
    <activity LCID="1033">In a Live Meeting</activity>
    <activity LCID="1036">Equivalent French String for - In a Live Mee
  </customState>
  <customState ID="3" availability="busy">
    <activity LCID="1033">Meeting with Customer</activity>
    <activity LCID="1055">meeting with client</activity>
    <activity LCID="1036">Equivalent French String for - Meeting with
  </customState>
  <customState ID="4" availability="do-not-disturb">
    <activity LCID="1033">Interviewing</activity>
  </customState>
</customStates>
```

2. Save the XML configuration file to a web server with HTTPS enabled. In this example, the file is named Presence.xml and saved to the location https://lspool.corp.contoso.com/ClientConfigFolder/CustomPresence.xml.
3. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
4. In the Lync Server Management Shell, define the location of your XML configuration file by using a command similar to the following:

```
New-CsClientPolicy -Identity ContosoCustomStates
-CustomStateURL "https://lspool.corp.contoso.com/ClientConfigFolder/Cu
```

5. Use the **Grant-CSClientPolicy** cmdlet to assign this new policy to users.

For details, see New-CsClientPolicy and Grant-CsClientPolicy in the Lync Server Management Shell documentation.

Note:

- By default, Lync Server 2013 updates client policies and settings every three hours.
- If you want to continue using Group Policy settings from previous releases, such as CustomStateURL, Lync 2013 will recognize the settings if they are located in the new policy registry hive (HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\15.0\Lync). However, server-based client policies take precedence.

1.4.10.1.2.5 Adding a Custom Link to Lync Error Messages

Adding a Custom Link to Lync Error Messages

Deploying Clients and Devices > Deploying Lync Clients > Customizing Lync Behavior and the User Interface >

Topic Last Modified: *2013-02-20*

Customize Lync 2013 error messages by adding a link to your own troubleshooting or help desk information. To do this, use the **New-CSClientPolicy** or **Set-CSClientPolicy** Lync Server Management Shell cmdlets with the CustomLinkInErrorMessages parameter. The text of the custom link is "Click here for support topics from your administrator," and it cannot be customized.

For example, the following command causes the custom link to appear in the footnote area of every Lync 2013 error message and sets the link destination to http://contoso.com/help/LyncHelpDesk.aspx:

```
New-CsClientPolicy -Identity LyncErrorLink -CustomLinkInErrorMessages "http://con
```

Use **Grant-CSClientPolicy** to assign this new policy to users. For details, see **New-CSClientPolicy** and **Grant-CSClientPolicy** in the Lync Server Management Shell documentation.

1.4.10.1.2.6 Adding Custom Text to Instant Messages

Adding Custom Text to Instant Messages

Deploying Clients and Devices > Deploying Lync Clients > Customizing Lync Behavior and the User Interface >

Topic Last Modified: *2013-02-20*

Add a disclaimer or warning to the beginning of every Lync 2013 instant messaging (IM) conversation by using the **New-CSClientPolicy** or **Set-CSClientPolicy** Lync Server Management Shell cmdlets with the IMWarning parameter.

The command in the following example adds a security reminder at the top of the Conversation window whenever a new IM conversation begins:

```
New-CsClientPolicy -Identity IMSecurityNotice -IMWarning
"Remember, security is everyone's responsibility. Keep it confidential."
```

Use **Grant-CSClientPolicy** to assign this new policy to users. For details, see **New-CSClientPolicy** and **Grant-CSClientPolicy** in the Lync Server Management Shell documentation.

1.4.10.1.2.7 Starting Lync from Another Application

Starting Lync from Another Application

Deploying Clients and Devices > Deploying Lync Clients > Customizing Lync Behavior and the User Interface >

Topic Last Modified: *2013-02-20*

You can use command-line parameters to quick-start Lync 2013. For example, if a user clicks a phone number in another application, the application can start an instance of Lync 2013 and initiate a call to that number.

Lync 2013 can also recognize a semicolon-delimited list of contact names for multiparty conferencing.

If Lync 2013 is configured to automatically sign in when started, then starting Lync 2013 with command-line parameters will open the Lync main window. If Lync is not configured to automatically sign in when started, the sign-in window opens.

The following table shows the available parameters.

Lync 2013 Command-Line Parameters

Extension	Format of Data	Action
tel:	tel URI	Opens the Conversation window for an audio call but does not dial the specified number.
callto:	tel:, sip:, or typeable tel URI	Opens the Conversation window for an audio call but does not dial the specified number.
sip:	SIP URI	Opens the Conversation window with the specified SIP Uniform Resource Identifier (URI) in the participant list.
Sips:	SIP URI	If Lync 2013 is configured to use the Transport Layer Security (TLS) protocol, functions exactly like sip:. If TLS is not being used, displays a dialog box informing the user that a higher level of security is required.
conf:	SIP URI of conference to join	If URI is self, instantiates the focus and brings up roster-only view. Otherwise, brings up roster view but does not send INVITE.
im:	SIP URI	Displays an instant messaging (IM)-only Conversation window with the SIP URI. Accepts multiple SIP URIs specified inside angle brackets (<>) without any separator. `im:<sip:user1@host><sip:user2@host>`

The following table provides examples of these command-line parameters.

Command-Line Parameter Examples

Instance	Results
Tel:+14255550101	Opens a phone-only view with +14255550101.
Callto:tel:+ 14255550101	Opens a phone-only view with +14255550101.
Callto:sip:kazuto@litwareinc.com	Opens a phone-only view with kazuto@litwareinc.com.
sip:kazuto@litwareinc.com	Opens a Conversation window with kazuto@litwareinc.com.
conf:sip:https://meet.contoso.com/kazuto/7322994	Opens a Conversation window and displays meeting audio join options.

1.4.10.1.3 Customizing the Online Meeting Add-in

Customizing the Online Meeting Add-in

Deployment > Deploying Clients and Devices > Deploying Lync Clients >

Topic Last Modified: *2012-06-28*

The Online Meeting Add-in for Lync 2013 supports meeting management from within the Outlook messaging and collaboration client. There are several ways you can customize the behavior of the add-in. Among these are new options for adding logos and text to the body of online meeting invitations.

- Updating the Outlook Enable List

- Configuring the Meeting Invitation

1.4.10.1.3.1 Updating the Outlook Enable List

Updating the Outlook Enable List

Deploying Clients and Devices > Deploying Lync Clients > Customizing the Online Meeting Add-in >

Topic Last Modified: *2013-01-07*

You can ensure that Online Meeting Add-in for Microsoft Lync 2013 always remains enabled for users by creating a policy that includes it in the Add-in Management List for Outlook. The Add-in Management List policy is included in the Office administrative template files for the Group Policy Management Console. It creates a registry key under HKCU\Software\Policies\Microsoft\Office\15.0\Outlook15\Resiliency\AddinList. You can add a value for the ucaddin.dll to this key, and configure the ucaddin.dll value so that it is always enabled and so that users cannot manually disable it

⊟To Add ucaddin.dll to the Outlook Add-in List

- To the AddinList registry key, located under HKCU\Software\Policies\Microsoft\Office\15.0\Outlook15\Resiliency\AddinList, add the following value:
  - Registry Type = REG_SZ
  - Name = ucaddin.dll
  - Value = 1 (specifies that the add-in is always enabled and cannot be managed by the end user)

1.4.10.1.3.2 Configuring the Meeting Invitation

Configuring the Meeting Invitation

Deploying Clients and Devices > Deploying Lync Clients > Customizing the Online Meeting Add-in >

Topic Last Modified: *2012-10-03*

You can customize meeting invitations sent by the Online Meeting Add-in for Lync 2013 by including the following optional items in the body of the meeting invitation:

- **Your organization's logo** Add your organization's logo to meeting invitations by using the Logo URL option. If meeting invitations will be sent to people external to your organization, the image should be located at a publicly available URL. The supported image formats are GIF and JPG. Although Lync Server 2013 stores the URL with no size restrictions on the image, for best results, the maximum size of the image should be 30 pixels high by 188 pixels wide.
- **A Custom Help or Support Link** Add a URL for your organization's help or support team website. If meeting invitations will be sent to people external to your organization, the URL should be publicly available. The maximum URL length is 1 KB.
- **Legal disclaimer text** Add a URL for legal text or a disclaimer that will be displayed in all meeting invitations. If meeting invitations will be sent to people external to your organization, the URL should be publicly available. The maximum URL length is 1 KB.
- **Custom footer text** Add text that will be rendered as a custom footer in the invitation. The maximum length of text that can be added is 2 KB.

You can configure these options by using either Lync Server Control Panel or Lync Server Management Shell.

To Customize the Meeting Invitation by using Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Meeting Configuration**.
4. On the **Meeting Configuration** page, click **New**, and then do one of the following:
   - To create a site-level policy, click **Site configuration**. In the **Select a Site** search field, type all or part of the name of the site for which you want to define meeting join settings. In the resulting list of sites, click the site you want, and then click **OK**.
   - To create a pool-level policy, click **Pool configuration**. In the **Select a Service** search field, type all or part of the name of the pool service for which you want to define meeting join settings. In the resulting list of services, click the pool you want, and then click **OK**.
5. Do any of the following:
   - In the **Logo URL** field, type the URL for your organization’s logo image.
   - In the **Help URL** field, type the URL to your organization’s help or support site.
   - In the **Legal text** field, type the URL to the legal text or disclaimer that you want to include in meeting invitations.
   - In the **Custom footer text** field, type footer text, up to 2 KB.

To Customize the Meeting Invitation by using Lync Server Management Shell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the **New-CsMeetingConfiguration** or **Set-CsMeetingConfiguration** cmdlet to create or configure the meeting invitation options. For example, run:

```
New-CsMeetingConfiguration -Identity site:Redmond -EnableInviteCustomi
```

1.4.10.1.4 Configuring the Meeting Join Page

Configuring the Meeting Join Page

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Conferencing >

Topic Last Modified: *2012-12-14*

When a user clicks a meeting link in a meeting request, the meeting join page detects whether a Lync 2013 client is already installed on the user’s computer. If a client is already installed, the client opens and joins the meeting. If a client is not installed, by default the 2013 version of Lync Web App opens.

You can modify the behavior of the meeting join page if you want to allow users to join meetings with Office Communicator 2007 R2 or Lync 2010 Attendant. These configuration options have been removed from the Lync Server 2013 Control Panel, but you configure them by using the Set-CsWebServiceConfiguration cmdlet.

Meeting Join Page Set-CsWebServiceConfiguration Parameters

Set-CsWebServiceConfiguration Parameter	Description
ShowJoinUsingLegacyClientLink	If set to True, users joining a meeting by using a client application other than Lync will be given the opportunity to join the meeting by using Office Communicator 2007 R2. The default value is False.
ShowAlternateJoinOptionsExpanded	When set to True then alternate options for joining an online conference (such as Office Communicator 2007 R2) will automatically be expanded and shown to users. When set to False (the default value) these options will be available, but the user will have to display the list of options for themselves.

To configure the meeting join page by using Lync Server 2013 Management Shell

1. Start the Lync Server 2013 Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. To view the web service configuration settings, run the following cmdlet:

   ```
   Get-CsWebServiceConfiguration
   ```

3. Run the following command, with the parameters set to True or False, depending on your preference (for details about the parameters for this cmdlet, see Set-CsWebServiceConfiguration in the Lync Server 2013 Management Shell documentation):

   ```
   Set-CsWebServiceConfiguration -Identity global -ShowJoinUsingLegacyCli
   ```

⊟See Also

Other Resources

Set-CsWebServiceConfiguration

1.4.10.1.5 Configuring Supported Client Versions

Configuring Supported Client Versions

Deployment > Deploying Clients and Devices > Deploying Lync Clients >

Topic Last Modified: *2012-12-14*

In Lync Server 2013, you can set up client version policies to specify the versions of clients that are supported in your environment. Additionally, you can use the global client version configuration to specify a default action for clients that do not already have a version policy defined and, therefore, are not explicitly supported or restricted.

You can also use client version policies to manage client updates. When you set a client version policy and use the options **Allow and upgrade** and **Block and upgrade**, clients will receive updated software from the Windows Server Update Service (if you are using this service) or from Microsoft Update.

Client Version Policy Settings

The default client version policy requires that all clients run Lync. If clients in your environment are running earlier versions of Communicator, you may need to reconfigure the Client Version rules to prevent clients and devices from being unexpectedly blocked or updated when connecting to Lync Server 2013. You can modify the default rule, or you can add a rule higher in the Client Version Policy list to override the default rule. Additionally, as Cumulative Updates (CUs) are released, you should configure the Client Version Policy to require the latest updates. For details, see Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 in the Operations documentation.

1.4.10.1.6 Configuring Enhanced Presence Privacy Mode

Configuring Enhanced Presence Privacy Mode

See Also

Deployment > Deploying Clients and Devices > Deploying Lync Clients >

Topic Last Modified: *2012-10-18*

With enhanced presence privacy mode, users can restrict their presence information so that it is visible only to the contacts listed in their Lync 2013 Contacts list. The **New-CsPrivacyConfiguration** and **Set-CsPrivacyConfiguration** cmdlets have an EnablePrivacyMode parameter controls this option. When EnablePrivacyMode is set to True, the option to restrict presence information to contacts becomes available in the Lync 2013 Status options. When EnablePrivacyMode is set to False, users can choose either to always allow everyone to see their presence information or to adhere to any future changes the administrator makes to the privacy mode.

> **Important:**
>
> Lync 2013 and Lync 2010 privacy settings are not honored by previous versions (Microsoft Office Communicator 2007 R2 or Microsoft Office Communicator 2007). If previous versions of Office Communicator are allowed to sign in, a Lync 2013 user's status, contact information, or picture could be viewed by someone who has not been authorized to view it. Additionally, a Lync 2013 user's privacy settings are reset if he or she later signs in with previous version of Communicator.
>
> For these reasons, in a migration scenario, before you enable enhanced presence privacy mode:
>
> - Ensure that every user has Lync 2013 installed.
> - Define a client version policy rule to prevent previous versions of Communicator from signing in.

To enable enhanced presence privacy mode

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the following command:

```
Get-CsPrivacyConfiguration | Set-CsPrivacyConfiguration -EnablePrivacy
```

   This command enables privacy mode for all the privacy configuration settings currently in use in the organization.

Other Resources

Get-CsPrivacyConfiguration
New-CsPrivacyConfiguration
Set-CsPrivacyConfiguration

1.4.10.2 Deploying the Lync VDI Plug-in

Deploying the Lync VDI Plug-in

Microsoft Lync Server 2013 > Deployment > Deploying Clients and Devices >

Topic Last Modified: *2012-10-03*

The Lync 2013 client supports audio and video in a Virtual Desktop Infrastructure (VDI) environment. A user can connect an audio or video device (for example, a headset or a camera) to the local computer (for example, a thin client or repurposed computer). The user can connect to the virtual machine, sign in to the Lync 2013 client that is running on the virtual machine, and participate in real-time audio and video communications as though the client is running locally.

The Lync VDI Plug-in is a stand-alone application that installs on the local computer and allows the use of local audio and video devices with the Lync 2013 client running on the virtual machine. The plug-in does not require Lync to be installed on the local computer. After the user signs in to the Lync 2013 client that is running on the virtual machine, Lync prompts the user to re-enter his or her credentials to establish a connection with the Lync VDI Plug-in that is running on the local computer. After this connection is established, the user is ready to make and receive audio and video calls.

In This Section

1.4.10.2.1 Lync VDI Plug-in Prerequisites

Lync VDI Plug-in Prerequisites

Deployment > Deploying Clients and Devices > Deploying the Lync VDI Plug-in >

Topic Last Modified: *2013-02-20*

In a virtual desktop infrastructure (VDI) environment, the virtual machines and the user’s local computer must meet the requirements outlined in this section.

Note:

Refer to your virtualization solution provider for details about how to install and deploy the virtualized environment. For information about deploying a virtualized environment based on Hyper-V and Remote Desktop Services, see the following articles in the Microsoft TechNet Library:

- Hyper-V at http://go.microsoft.com/fwlink/p/?linkid=247514
- Remote Desktop Services in Windows Server 2008 R2 at http://go.microsoft.com/fwlink/p/?linkid=247513

The following are requirements for the virtual machines running on the data center computer:

- Virtual machines must be configured with Windows 8, Windows 7, or Windows Server 2008 R2 with the latest service packs.

The following are requirements for the user and the user's local computer:

- The user must be homed on Lync Server 2013.
- The local computer must be running Windows Embedded Standard 7 with SP1, Windows 7 with SP1, or Windows 8.
- If you are using Remote Desktop Services, the Lync VDI plug-in bitness (that is, whether the application is 32-bit or 64-bit) must match the local computer's operating system bitness. The bitness of the operating system on the local computer and the operating system on the virtual machine do not need to match. If you are using another virtualization solution or platform, refer to guidance from your virtualization solution provider about bitness requirements.
- The local computer must be running the latest version of the remote desktop client. Install the latest updates of Remote Desktop Services client from Microsoft or the latest remote desktop client software from your virtualization solution provider. For the latest Remote Desktop Services updates, see http://go.microsoft.com/fwlink/p/?LinkId=268032.
- On the local computer, the remote desktop client settings must be configured so that audio plays on the local computer and remote recording is disabled. To configure these settings for Remote Desktop Connection in Windows, see the next section, "To configure Remote Desktop Connection settings."

To configure Remote Desktop Connection settings

To prepare Remote Desktop Connection in Windows for the Lync VDI plug-in, follow these steps.

1. If the local computer is running Windows 8, skip this step. If the local computer is running Windows 7 with SP1, install the latest Windows 8 version of the Remote Desktop Services client, available at http://go.microsoft.com/fwlink/p/?LinkId=268032.
2. Start the Remote Desktop Services client by clicking **Start**, and then clicking **Remote Desktop Connection**.
3. Click **Options**.
4. Click the **Local Resources** tab. Under **Remote audio**, click **Settings**, and then do the following:
   - Under **Remote audio playback**, select **Play on this computer**.
   - Under **Remote audio recording**, select **Do not record**.
   - Click **OK**.
5. Click the **Experience** tab. Under **Performance**, clear the **Persistent bitmap caching** check box.
6. Click the **General** tab. In **Computer**, type the name of the virtual machine, and then click **Connect**.

1.4.10.2.2 Preparing Your Environment for VDI

Preparing Your Environment for VDI

Deployment > Deploying Clients and Devices > Deploying the Lync VDI Plug-in >

Topic Last Modified: *2013-02-22*

To prepare the environment for the Lync VDI plug-in, the administrator must perform the following steps.

1. In Lync Server 2013, ensure that EnableMediaRedirection is set to TRUE for

all VDI users. For details, see the Help topics for the New-CsClientPolicy cmdlet and the Set-CsClientPolicy cmdlet.

2. On the data center computer, install the Lync 2013 client on all virtual machines.
3. On the local computers, install the Lync VDI plug-in.

1.4.10.2.3 Signing In and Using Lync 2013 on the Virtual Machine

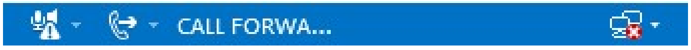
Signing In and Using Lync 2013 on the Virtual Machine

Deployment > Deploying Clients and Devices > Deploying the Lync VDI Plug-in >

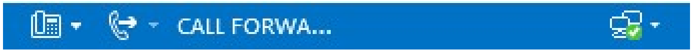
Topic Last Modified: *2012-10-03*

After the VDI plug-in is enabled, the following steps occur when the user signs in to Lync 2013.

1. The user types his or her credentials in to the Lync 2013 client running on the virtual machine.
2. After Lync detects the availability of the VDI plug-in, Lync prompts the user to re-enter his or her credentials. In this dialog box, we recommend that the user select the **Save my password** check box so that he or she will not be required to enter credentials during subsequent sign in.
3. Lync begins pairing with the VDI plug-in. Before pairing is complete, the client displays two icons in the Lync status bar. The icon in the lower left indicates that no audio devices are available, and the blinking icon in the lower right indicates that the VDI pairing is in progress, as shown:



4. After VDI pairing is successful, the icons change to indicate the audio device that will be used for calls and the VDI pairing success:



5. After Lync pairs with the VDI plug-in, the user can see his or her presence on Lync compatible devices that are connected to the local computer. The user can now place and answer calls as usual.

1.4.10.2.4 Troubleshooting the Lync VDI Plug-in

Troubleshooting the Lync VDI Plug-in

Deployment > Deploying Clients and Devices > Deploying the Lync VDI Plug-in >

Topic Last Modified: *2012-10-10*

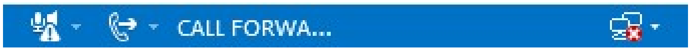
Troubleshooting Issues with Installing the Lync VDI Plug-in on a Thin Client

If there are issues with installing the VDI plug-in on a thin client, check the following:

- Ensure that there is sufficient space in the folder that you specified in the TEMP and TMP system variables.
- Ensure that write-protect is turned off. Refer to your device manufacturer’s documentation for instructions.

Troubleshooting Issues with Pairing

When VDI plug-in pairing fails, the pairing icon in the lower right displays as a red “X” as shown:



The following are possible reasons for failures and the corrective actions you can take.

- **The user entered incorrect credentials during sign-in.**
  The user should sign out of Lync and sign in again with the correct credentials. The pairing dialog box will reappear and show whether pairing is successful.
- **Another instance of the remote desktop client is running.**
  If they are using Remote Desktop Connection in Windows, users should do the following:
  .1. Start Task Manager: Press **Alt+Ctrl+Delete**, and then click **Start Task Manager**.
  .2. Click the **Processes** tab and look for all processes named **mstsc.exe** in the list.
  .3. Highlight each **mstsc.exe** process and then click **End Process**.
  .4. Start a new remote desktop session and try connecting again.
- **The necessary files did not install correctly.**
  After the plug-in is installed on the local computer, the following files should be present under C:\Program Files\Microsoft Office\Office15 (or the appropriate drive letter):
  .1. LyncVdiPlugin.dll
  .2. UcVdi.dll
  If there are any issues with VDI pairing, check to make sure that these files are present on the local computer.
- **The Lync client is running on the local computer.**
  To use the Lync VDI plugin, a Lync client must not be running on the local computer, otherwise pairing will fail. As a best practice, the user should not install a Lync client on the local computer.

1.4.10.2.5 Known Limitations for VDI

Known Limitations for VDI

Deployment > Deploying Clients and Devices > Deploying the Lync VDI Plug-in >

Topic Last Modified: *2012-12-14*

The following are known limitations when you are using Lync 2013 in a VDI environment:

- There is limited support for Call Delegation and Response Group Agent Anonymization features.
- There is no support for the following features:
  - Integrated Audio Device and Video Device tuning pages.
  - Multi-view video.
  - Recording of conversations.
  - Joining meetings anonymously (that is, joining Lync meetings hosted by an organization that does not federate with your organization).
  - Using the Lync VDI plug-in along with a Lync Phone Edition device.
  - Call continuity in case of a network outage.
  - Customized ringtones and music on hold features.
- The Lync VDI plug-in is not supported in an Office 365 environment.

1.4.10.3 Deploying Lync Web App

Deploying Lync Web App

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Clients and Devices >

Topic Last Modified: *2013-03-04*

Lync Web App is an Internet Information Services (IIS) web client that installs with Lync Server 2013 and is enabled by default. No additional steps are necessary to either enable Lync Web App on the server or deploy the web client to users. Whenever a user clicks a meeting URL but does not have the Lync 2013 client installed, the user is presented with the option to join the meeting by using the latest version of Lync Web App.

The voice, video, and sharing features in Lync Web App require a Microsoft ActiveX control. You can either install the ActiveX control in advance or allow users to install it when prompted, which happens the first time they use Lync Web App or the first time they access a feature that requires the ActiveX control.

Note:

In Lync Server 2013 Edge Server deployments, an HTTPS reverse proxy in the perimeter network is required for Lync Web App client access. You must also publish simple URLs. For details, see Setting Up Reverse Proxy Servers and Planning for Simple URLs.

Enabling Multi-Factor Authentication for Lync Web App

The Lync Server 2013 version of Lync Web App supports multi-factor authentication. In addition to user name and password, you can require additional authentication methods, such as smart cards or PINs, to authenticate external users when they sign in to Lync meetings. You can enable multi-factor authentication by deploying Active Directory Federation Service (AD FS) federation server and enabling passive authentication in Lync Server 2013. After AD FS is configured, external users who attempt to join Lync meetings are presented with an AD FS multi-factor authentication webpage that contains the user name and password challenge along with any additional authentication methods that you have configured.

Important:

The following are important considerations if you plan to configure AD FS for multi-factor authentication:

- If you use hardware load balancers, enable cookie persistence on the load balancers so that all requests from the Lync Web App client are handled by the same Front End Server.
- When you establish a relying party trust between Lync Server and AD FS servers, assign a token life that is long enough to span the maximum length of your Lync meetings. Typically, a token life of 240 minutes is sufficient.

To Configure Multi-Factor Authentication

1. Install an AD FS federation server role. For details, see the Active Directory Federation Services 2.0 Deployment Guide at http://go.microsoft.com/fwlink/p/?linkid=267511
2. Create certificates for AD FS. For more information, see the "Federation server certificates" section of the Plan for and deploy AD FS for use with single sign-on topic at http://go.microsoft.com/fwlink/p/?LinkId=285376.
3. From the Windows PowerShell command-line interface, run the following command:

   ```
   add-pssnapin Microsoft.Adfs.powershell
   ```

4. Establish a partnership by running the following command:

```
Add-ADFSRelyingPartyTrust -Name ContosoApp -MetadataURL https://lyncpo
```

5. Set the following relying party rules:

```
$IssuanceAuthorizationRules = '@RuleTemplate = "AllowAllAuthzRule" =>
$IssuanceTransformRules = '@RuleTemplate = "PassThroughClaims" @RuleNa
```

```
Set-ADFSRelyingPartyTrust -TargetName ContosoApp -IssuanceAuthorizatio
```

```
Set-CsWebServiceConfiguration -UseWsFedPassiveAuth $true -WsFedPassive
```

BranchCache Configuration

The BranchCache feature in Windows 7 and Windows Server 2008 R2 can interfere with Lync Web App web components. To prevent issues for Lync Web App users, make sure that BranchCache is not enabled.

For details about disabling BranchCache, see the BranchCache Deployment Guide, which is available in Word format at the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?LinkId=268788 and in HTML format in the Windows Server 2008 R2 Technical Library at http://go.microsoft.com/fwlink/p/?LinkId=268789.

Verifying Lync Web App Deployment

You can use the Test-CsUcwaConference cmdlet to verify that a pair of test users can participate in a conference using the Unified Communications Web API (UCWA). For details about this cmdlet, see Test-CsUcwaConference in the Lync Server Management Shell documentation.

Troubleshooting Plug-in Installation on Windows Server 2008 R2

If installation of the plug-in fails on a computer running Windows Server 2008 R2, you may need to modify the Internet Explorer security setting or the DisableMSI registry key setting.

To modify the security setting in Internet Explorer

1. Open Internet Explorer.
2. Click **Tools**, click **Internet Options**, and then click **Advanced**.
3. Scroll down to the **Security** section.
4. Clear **Do not save encrypted pages to disk**, and then click **OK**.

> **Note:**
> If selected, this setting will also cause an error when trying to download an attachment from Lync Web App.

5. Rejoin the meeting. The plug-in should download without errors.

To modify the DisableMSI Registry setting

1. Click **Start**, and then click **Run**.
2. To access the Registry Editor, type **regedit**.
3. Navigate to HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer.
4. Edit or add the DisableMSI registry key of type REG_DWORD and set it to 0.
5. Rejoin the meeting.

See Also

Concepts

Configuring the Meeting Join Page
Lync Web App Supported Platforms

1.4.10.4 Deploying Devices

Deploying Devices

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Clients and Devices >

Topic Last Modified: *2013-02-28*

Lync Server 2013 includes Lync Phone Edition, software that runs on qualified devices and provides traditional and advanced telephony features, integrated security, manageability, and more. Lync Phone Edition works the same way with Lync Server 2013 as it does with Lync Server 2010. For details about deploying devices, see Deploying Lync Phone Editionin the Lync Server 2010 TechNet Library.

Other Resources

Planning for Devices
Client and Device Software and Infrastructure Support

1.4.10.5 Deploying Mobile Clients

Deploying Mobile Clients

Microsoft Lync Server 2013 > Deployment > Deploying Clients and Devices >

Topic Last Modified: *2013-02-19*

Lync 2013 apps for mobile clients provide instant messaging (IM), enhanced presence, and telephony for users in your organization who are connecting from a smartphone or a phone running a Professional edition of Windows Mobile. You can instruct your users to install Lync 2013 by directing them to the app marketplace for their mobile phone.

Note:

Lync Server 2013 also supports Lync 2010 for mobile clients. For details, refer to the following articles in the Lync Server 2010 TechNet library:

- "Planning for Mobile Clients" at http://go.microsoft.com/fwlink/p/?LinkID=235955.
- "Deploying Mobile Clients" at http://go.microsoft.com/fwlink/p/?LinkID=236068.

- Deploying Lync for Windows Phone
- Deploying Lync for iPhone and iPad

1.4.10.5.1 Deploying Lync for Windows Phone

Deploying Lync for Windows Phone

Deployment > Deploying Clients and Devices > Deploying Mobile Clients >

Topic Last Modified: *2013-02-19*

This section describes how to deploy Lync 2013 for Windows Phone for your mobile users.

- Installing Lync for Windows Phone
- Removing Lync for Windows Phone

1.4.10.5.1.1 Installing Lync for Windows Phone

Installing Lync for Windows Phone

Deploying Clients and Devices > Deploying Mobile Clients > Deploying Lync for Windows Phone >

Topic Last Modified: *2013-02-19*

Lync 2013 for Windows Phone is a user-installable application that is available in the Windows Phone Marketplace.

Installing Lync for Windows Mobile

You can instruct your users to install Lync 2013 for Windows Phone on their devices by directing them to the Windows Phone Marketplace at http://go.microsoft.com/fwlink/p/?linkid=231901.

Verifying Mobile Client Installation

After you configure the client and sign in successfully, use the following tests to verify that your installation of Lync 2013 is working correctly on your mobile device.

Search for a contact in the corporate directory

1. In the Contacts list, tap **Search** at the bottom.
2. Search for a contact that exists only in the global address list.
3. Verify that the contact name appears in the search results.

Test instant messaging and presence

1. In the Contacts list, tap a contact.
2. In the contact card, tap the **IM** icon.
3. Verify that an instant messaging (IM) window appears and that you can type and send an IM.

Test dial-out conferencing

1. In Outlook, schedule a Lync meeting.
2. On the mobile device, open the meeting invitation.
3. Click the link in the meeting to join.
4. Answer the call from the conference service and verify that you are connected to meeting audio.

Test push notifications

1. On user A’s mobile device, sign in to Lync with user A’s account.
2. Open another application on the mobile device.
3. On a different client, sign in to Lync with user B’s account.
4. Send an IM from user B to user A.
5. Verify that the IM notification appears on user A’s mobile device.

1.4.10.5.1.2 Removing Lync for Windows Phone

Removing Lync for Windows Phone

Deploying Clients and Devices > Deploying Mobile Clients > Deploying Lync for Windows Phone >

Topic Last Modified: *2013-02-19*

To remove the Lync 2013 for Windows Phone application from the mobile device, perform the following steps:

1. On the mobile device, from the start screen, swipe to see the application list.
2. Tap and hold the Lync application, and then select **Uninstall**.

1.4.10.5.2 Deploying Lync for iPhone and iPad

Deploying Lync for iPhone and iPad

Deployment > Deploying Clients and Devices > Deploying Mobile Clients >

Topic Last Modified: *2013-02-19*

This section describes how to deploy Lync 2013 for iPhone and Lync 2013 for iPad for your mobile users.

- Installing Lync for iPhone and iPad
- Removing Lync for iPhone and iPad

1.4.10.5.2.1 Installing Lync for iPhone and iPad

Installing Lync for iPhone and iPad

Deploying Clients and Devices > Deploying Mobile Clients > Deploying Lync for iPhone and iPad >

Topic Last Modified: *2013-02-19*

Lync 2013 for iPhone and Lync 2013 for iPad are user-installable applications that are available in the Apple App Store.

Installing Lync for iPhone and Lync for iPad

You can instruct your users to install Lync 2013 for iPhone and Lync 2013 for iPad by directing them to the App Store from their devices. The App Store for each device is also available online.

- Lync for iPhone is available in the App Store at < http://www.apple.com/iphone/from-the-app-store/>
- Lync for iPad is available in the App Store at < http://www.apple.com/ipad/from-the-app-store/>

Verifying Mobile Client Installation

After you configure the client and sign in successfully, use the following tests to verify that your Lync installation is working correctly on your mobile device.

Search for a contact in the corporate directory

1. In the Contacts list, tap inside the search bar at the top, and begin typing the name of a contact that exists only in the global address list (GAL).
2. Verify that the contact name appears in the search results.

Test instant messaging and presence

1. In the Contacts list, tap a contact.
2. In the contact card, tap the **IM** icon.
3. Verify that an instant messaging (IM) window appears and that you can type and send an IM.

Test dial-out conferencing

1. In Outlook, schedule a Lync meeting.
2. On the mobile device, open the meeting invitation.
3. Click the link in the meeting to join.
4. Answer the call from the conference service and verify that you are connected to the meeting audio.

Test push notifications

1. On user A’s mobile device, sign in to Lync with user A’s account.
2. Open another application on the mobile device.
3. On a different client, sign in to Lync with user B’s account.
4. Send an IM from user B to user A.
5. Verify that the IM notification appears on user A’s mobile device.

1.4.10.5.2.2 Removing Lync for iPhone and iPad

Removing Lync for iPhone and iPad

Deploying Clients and Devices > Deploying Mobile Clients > Deploying Lync for iPhone and iPad >

Topic Last Modified: *2013-02-19*

To remove Lync 2013 for iPhone or Microsoft Lync 2010 for iPad from the device, perform the following steps:

1. On the mobile device home screen, tap and hold the Lync icon.
2. When the tiles begin to shake and the **X** appears, tap the **X** to delete the application.

1.4.10.6 Deploying Lync Windows Store App

Deploying Lync Windows Store App

Microsoft Lync Server 2013 > Deployment > Deploying Clients and Devices >

Topic Last Modified: *2013-02-19*

Before making Lync Windows Store app available to users, make sure that your deployment meets the Lync Windows Store App Requirements. For details about configuring Lync Server 2013 to support Lync Windows Store app, see the NextHop Blog article, "Lync Server Autodiscover and the Lync Windows Store App," at http://go.microsoft.com/fwlink/?LinkId=271966. After your server environment is configured correctly, you can direct users to download the Lync app from the Windows Store by searching for "Lync."

Known Issues that Can Prevent Sign-in

The time and date are not set accurately on the device running Lync Windows Store app

The time setting on the device must be synchronized with the time setting on the server. This is particularly important for devices such as Microsoft Surface, and other devices running Windows RT that are not joined to a domain. To set the time on these devices automatically from a time server, run the following command from an elevated command prompt on the device:

```
w32tm /resync
```

Lync Windows Store app cannot access the Lync server or services

Lync Windows Store app may not be able to access the Lync server or services through network adapters, such as 4G LTE USB modems, that do not register with Windows 8 as physical devices. Lync Windows Store app may have this issue even when the desktop apps and browsers are able to access other servers and web sites.

Use Lync Windows Store app logs to troubleshoot issues

You can use the logs generated on the device to troubleshoot issues. The logs are stored in the following folder:

%LocalAppData%\Packages\Microsoft.LyncMX_8wekyb3d8bbwe\LocalState\Tracing

Before you get the logs from a user, make sure that logging is turned on, and then ask the user to save the logs so that all the information stored in memory is also saved to files on the hard drive.

To turn on logging

1. Open Lync Windows Store app on the device.
2. Swipe from the right side of the screen. If you're using a mouse, point to the upper-right corner of the screen and then move the mouse pointer down the screen.
3. Select **Settings**, select **Options**, and then set **Diagnostic Logs** to **On**.
4. If **Diagnostic Logs** was off previously, you must restart Lync. To restart Lync, do one of the following:
   - Restart the device.
   - End the Lync task and launch the app again. To end the task, open the Windows Task Manager, select **Lync**, and then tap **End task**. If Lync is not listed, tap **More details** and look for Lync under **Background processes**.

To save the logs

1. Open Lync Windows Store app on the device.
2. Try signing in.
3. Swipe from the right side of the screen. If you're using a mouse, point to the upper-right corner of the screen and then move the mouse pointer down the screen.
4. Select **Settings**, select **About**, and then select **Save logs**.

1.4.10.7 Using Lync Connectivity Analyzer

Using Lync Connectivity Analyzer

Microsoft Lync Server 2013 > Deployment > Deploying Clients and Devices >

Topic Last Modified: *2013-01-15*

Microsoft Lync Connectivity Analyzer helps Lync administrators determine whether the deployment and configuration of their on-premises Lync Server environment meets the requirements to support connections from Lync app from Windows Store for Windows 8 and Windows RT, and from Lync apps on mobile devices.

Lync Connectivity Analyzer attempts to connect to your on-premises Lync Server by using the same services and protocols that are used by Lync Windows Store app and Lync mobile apps. You can perform the connection tests over your internal network or over an external network that connects to Lync Server. Lync Connectivity Analyzer provides a report with detailed information about each connection step to help you validate your configuration and troubleshoot connection problems.

Lync Connectivity Analyzer tests the following Lync Server components:

- Autodiscover service

- Authentication Broker (Reach) service
- Mobility (MCX) service
- WebTicket service

Lync Connectivity Analyzer tests the configuration of the following other components:

- Publication of DNS records for Autodiscover URLs
- Certificates
- Proxy servers

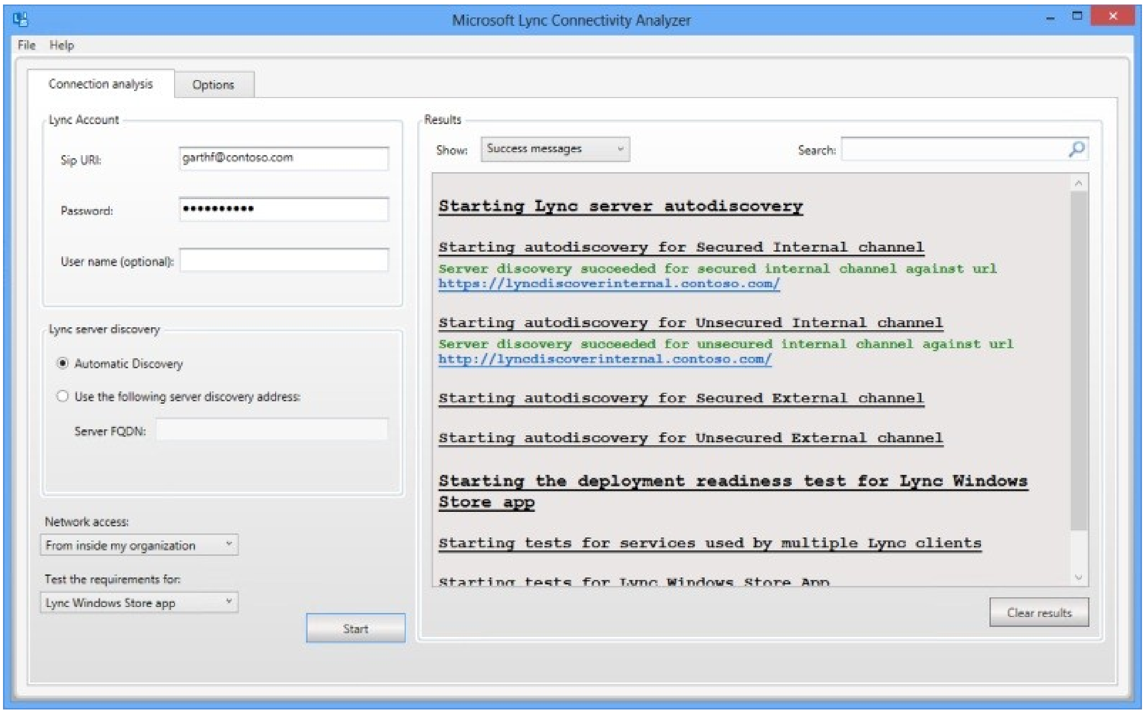
You can download Lync Connectivity Analyzer from the Microsoft Download Center at http://go.microsoft.com/fwlink/?LinkId=277056.

Note:
Lync Connectivity Analyzer cannot be used to test accounts for Office 365 Lync servers.

To Analyze Your Connectivity

1. Enter the credentials for a valid Lync account that will be used by the tool to test the connection:
   - In **SIP URI**, enter the SIP sign-in address for the Lync connection in the format **user@domain.com**.
   - In **Password**, enter the password associated with this account.
   - In **User name (optional)**, enter a user name if applicable. The user name is also known as the User Principal Name (UPN). If the user name and the SIP URI are the same, you do not need to enter a user name. If they are not the same, enter the user name in the format **user@domain.com** or **domain\user**, as appropriate.
   - Under **Lync server discovery**, select the type of test to perform:
     - If you want the tool to discover the Lync server automatically, select **Automatic discovery**.
     - If you want the tool to bypass the autodiscover test, or if you know the name of the server you would like to connect to, select **Use the following server discovery address**, and then in **Server FQDN**, specify the fully qualified domain name (FQDN) of the Lync server—for example, **lync.company.com**.
2. Under **Network access**, choose **From inside my organization** if you are running Lync Connectivity Analyzer from a computer connected to your internal network. Otherwise, choose **External (Internet)**. Lync Connectivity Analyzer always performs both internal and external tests, but specifying whether you are inside or outside of your own network helps the tool interpret whether certain failures are expected.
3. Under **Test the requirements for**, select whether to perform connectivity tests for **Lync Windows Store app** or **Lync mobile apps**.
4. Click **Start**.

The following figure shows sample results from Lync Connectivity Analyzer.



Lync Account

Sip URI: garthf@contoso.com

Password: •••••••••••

User name (optional):

Lync server discovery

● Automatic Discovery

○ Use the following server discovery address:

Server FQDN:

Network access: From inside my organization

Test the requirements for: Lync Windows Store app

Results

Show: Success messages

Search:

```
Starting Lync server autodiscovery

Starting autodiscovery for Secured Internal channel
Server discovery succeeded for secured internal channel against url
https://lyncdiscoverinternal.contoso.com/

Starting autodiscovery for Unsecured Internal channel
Server discovery succeeded for unsecured internal channel against url
http://lyncdiscoverinternal.contoso.com/

Starting autodiscovery for Secured External channel

Starting autodiscovery for Unsecured External channel

Starting the deployment readiness test for Lync Windows
Store app

Starting tests for services used by multiple Lync clients

Starting tests for Lync Windows Store App
```

Components Tested by Lync Connectivity Analyzer

Lync Connectivity Analyzer attempts to discover the Lync server and establish a connection by using the same steps used by Lync Windows Store app and Lync mobile apps. It performs the tests as described in this section.

If **Automatic discovery** is selected, Lync Connectivity Analyzer does the following:

- Queries Domain Name Service (DNS) for autodiscover URLs.
- Attempts discovery by using the secured internal channel. For example, **HTTPS://lyncdiscoverinternal.company.com/**.
- Attempts discovery by using the unsecured internal channel. For example, **HTTP://lyncdiscoverinternal.company.com/**.
- Attempts discovery by using the secured external channel. For example, **HTTPS://lyncdiscover.company.com**.
- Attempts discovery by using the unsecured external channel. For example, **HTTP://lyncdiscover.company.com**.

If **Use the following server discovery address** is selected, Lync Connectivity Analyzer does the following:

- Queries DNS for the server’s FQDN.
- Attempts discovery by using the secured channel. For example, **HTTPS://serverFQDN/**.
- Attempts discovery by using the unsecured channel. For example, **HTTP://serverFQDN/**.

If **Lync Windows Store app** is selected under **Test the requirements for**, Lync Connectivity Analyzer does the following:

- Verifies that the WebTicket service is available and tests authentication of the Lync account credentials.
- Verifies that the Authentication Broker (Reach) service is available.

If **Lync mobile apps** is selected under **Test the requirements for**, Lync Connectivity Analyzer does the following:

- Verifies that the WebTicket service is available and tests authentication of the Lync account credentials.
- Verifies that the Mobility (MCX) service is available.

While performing these tests, Lync Connectivity Analyzer validates the certificates installed on Lync Server, hardware load balancers, proxy servers, and the computer on which you are running the tests.

Other Resources

Microsoft also provides Microsoft Remote Connectivity Analyzer, a web-based connectivity test tool, which is available at https://testconnectivity.microsoft.com/. Lync Connectivity Analyzer and Remote Connectivity Analyzer differ in the following ways:

- Remote Connectivity Analyzer can test connectivity for Microsoft Exchange and Outlook, in addition to Microsoft Lync.
- Remote Connectivity Analyzer completes the SIP sign-in, whereas Lync Connectivity Analyzer only validates the account credentials, without signing in.
- Remote Connectivity Analyzer tests connections only from outside of your organization's network because it runs from a public web server.
- Remote Connectivity Analyzer does not test the availability of Authentication Broker (Reach), Mobility (MCX), and WebTicket services.
- Lync Connectivity Analyzer tests the Autodiscover service.
- Remote Connectivity Analyzer can connect to any version of Lync Server, whereas Lync Connectivity Analyzer can connect successfully only to Lync Server 2010 with Cumulative Updates for Lync Server 2010: February 2012 (at a minimum), or the latest version of Lync Server.

The following documentation describes the requirements and procedures for deploying and configuring Lync Server to support Lync Windows Store app and Lync mobile clients:

- Deploying Clients and Devices
- Planning for Mobility
- Deploying Mobility

1.4.11 Planning and Deploying Unified Contact Store

Planning and Deploying Unified Contact Store

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-06-14*

Unified contact store is a feature that provides a consistent contact experience across Microsoft Office products. This feature enables users to store all contact information in Exchange 2013 so that the information is available globally across Lync, Exchange, Outlook, and Outlook Web Access.

In This Section

- Requirements for Unified Contact Store
- Deploying Unified Contact Store

1.4.11.1 Requirements for Unified Contact Store

Requirements for Unified Contact Store

Microsoft Lync Server 2013 > Deployment > Planning and Deploying Unified Contact Store >

Topic Last Modified: *2012-10-01*

The following list describes the requirements for implementing unified contact store in Lync Server 2013:

- You must be running Microsoft Lync Server 2013 and Exchange 2013.
- Users must use Lync 2013 to initiate the migration of contacts from Lync Server 2013 to Exchange 2013.
- User mailboxes must be migrated to Exchange 2013.
- You must have server-to-server authentication configured between Lync Server 2013 and Exchange 2013.

> **Note:**
>
> For detailed requirements about setting up authentication between Lync Server 2013 and Exchange 2013, see Managing Server-to-Server Authentication (Oauth) and Partner Applications in the Operations documentation.

1.4.11.2 Deploying Unified Contact Store

Deploying Unified Contact Store

Microsoft Lync Server 2013 > Deployment > Planning and Deploying Unified Contact Store >

Topic Last Modified: *2012-10-07*

Enabling unified contact store in Lync Server 2013 does not require any topology settings. Enabling unified contact store for users requires the following:

- Unified contact store policy is enabled (default is enabled).
- Users log in with Lync 2013 at least once.

After a user’s contacts have been migrated, which happens automatically when a user logs in with Lync 2013, the user can access and manage their Lync contacts from Lync 2013, Outlook 2013, or Outlook Web Access. The user does not have to be logged in to Lync to manage their contacts from Outlook or Outlook Web Access.

> **Important:**
>
> If a user logs in from Lync 2010 after migration, contacts and groups are available and up-to-date, but the user cannot manage (that is, add, delete, move, tag, untag, or modify) those contacts.

- Enable Users for Unified Contact Store
- Migrate Users to Unified Contact Store
- Roll back Migrated Users

1.4.11.2.1 Enable Users for Unified Contact Store

Enable Users for Unified Contact Store

Deployment > Planning and Deploying Unified Contact Store > Deploying Unified Contact Store >

Topic Last Modified: *2012-10-07*

When you deploy Lync Server 2013 and publish the topology, unified contact store is enabled for all users by default. You do not need to take any additional action to enable unified contact store after you deploy Lync Server 2013. However, you can use the **Set-CsUserServicesPolicy** cmdlet to customize which users have unified contact store available. You can enable this feature globally, by site, by tenant, or by individuals or groups of individuals.

To enable users for unified contact store

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Do any of the following:
   - To enable unified contact store globally for all Lync Server users, at the command line, type:

     ```
     Set-CsUserServicesPolicy -Identity global -UcsAllowed $True
     ```

   - To enable unified contact store for the users at a specific site, at the command line, type:

     ```
     New-CsUserServicesPolicy -Identity site:<site name> -UcsAllo
     ```

     For example:

     ```
     New-CsUserServicesPolicy -Identity site:Redmond -UcsAllowed
     ```

   - To enable unified contact store by tenant, at the command line, type:

     ```
     Set-CsUserServicesPolicy -Tenant <tenantId> -UcsAllowed $Tru
     ```

     For example:

     ```
     Set-CsUserServicesPolicy -Tenant "38aad667-af54-4397-aaa7-e9
     ```

   - To enable unified contact store for specific users, at the command line, type:

     ```
     New-CsUserServicesPolicy -Identity "<policy name>" -UcsAllow
     Grant-CsUserServicesPolicy -Identity "<user display name>" -
     ```

     Note:
     You can also use user alias or SIP URI instead of the user display name.

     For example:

     ```
     New-CsUserServicesPolicy -Identity "UCS Enabled Users" -UcsA
     Grant-CsUserServicesPolicy -Identity "Ken Myer" -PolicyName
     ```

     Note:
     In the preceding example, the first command creates a new per-user policy named *UCS Enabled Users* with the UcsAllowed flag set to True. The second command assigns the policy to the user with the display name Ken Myer, which means that Ken Myer is now enabled for unified contact store.

1.4.11.2.2 Migrate Users to Unified Contact Store

Migrate Users to Unified Contact Store

[Deployment](#) > [Planning and Deploying Unified Contact Store](#) > [Deploying Unified Contact Store](#) >

Topic Last Modified: *2012-10-15*

A user's contacts are automatically migrated to the Exchange 2013 server when the user:

- Has been assigned a user services policy that has UcsAllowed set to True.
- Has been provisioned with an Exchange 2013 mailbox and has signed into the mailbox at least once.
- Logs in by using a Lync 2013 rich client.

If the user logs in with a Lync 2010 or earlier client, or if the user is not connected to an Exchange 2013 server, the user services policy is ignored and the user's contacts remain in Lync Server.

You can determine whether a user's contacts have been migrated by using either of the following methods:

- Check the following registry key on the client computer: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Lync\<SIP URL>\UCS If the user's contacts are stored in Exchange 2013, this key contains a value of InUCSMode with a value of 2165.
- Run the **Test-CsUnifiedContactStore** cmdlet. At the Lync Server Management Shell command line, type:

  ```
  Test-CsUnifiedContactStore -UserSipAddress "sip:kenmyer@litwareinc.com"
  ```

  If **Test-CsUnifiedContactStore** succeeds, the user's contacts were migrated to unified contact store.

1.4.11.2.3 Roll back Migrated Users

Roll back Migrated Users

Deployment > Planning and Deploying Unified Contact Store > Deploying Unified Contact Store >

Topic Last Modified: *2012-10-07*

If you need to roll back the unified contact store feature, roll back the contacts only if you move the user back to Exchange 2010 or Lync Server 2010. To roll back, disable the policy for the user, and then run the **Invoke-CsUcsRollback** cmdlet. Just running **Invoke-CsUcsRollback** alone is not enough to ensure permanent rollback, because unified contact store migration will be initiated again if the policy is not disabled. For example, if a user is rolled back because Exchange 2013 is rolled back to Exchange 2010, and then the user’s mailbox is moved to Exchange 2013, the unified contact store migration will be initiated again seven days after the rollback, as long as unified contact store is still enabled for the user in the user services policy.

> **Important:**
>
> The **Move-CsUser** cmdlet automatically rolls back the user's contact store from Exchange 2013 to Lync Server 2013 in the following situations:
>
> - When users are moved from Lync Server 2013 to Lync Server 2010.
> - When users are migrated cross premises, such as when a user is moved from Lync Online to Lync Server 2013 on-premises, or vice versa.

> **Important:**
>
> Importing unified contact store data from a backup database can cause unified contact store data and user data to become corrupted if the unified contact store mode changed between the export and the import. For example:
>
> - If you export contact lists before the users' contacts are migrated to Exchange 2013 and then, after the migration, import the same data, the unified contact store data and contact lists will be corrupted.
> - If you export userdata after you migrate users to Exchange 2013, roll back the migration, and then for some reason you import the data from after the migration, the unified contact store data and contact lists will be corrupted.

> **Important:**
>
> Before you move an Exchange mailbox from Exchange 2013 to Exchange 2010, the

Exchange administrator must make sure that the Lync Server administrator has first rolled back the Lync Server user contacts from Exchange 2013 to Lync Server. To roll back unified contact store contacts to Lync Server, see procedure "To roll back unified contact store contacts from Exchange 2013 to Lync Server 2013," later in this section.

The following procedure describes how to roll back user contacts. If you use the **Move-CsUser** cmdlet to move users between Lync Server 2013 and Lync Server 2010, you can skip these steps because the **Move-CsUser** cmdlet automatically rolls back unifed contact store when it moves users from Lync Server 2013 to Lync Server 2010. **Move-CsUser** does not disable unified contact store policy, so the migration to unified contact store will recur if the user is moved back to Lync Server 2013.

To roll back user contacts from Lync Server 2013 to Lync Server 2010

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Disable unified contact store for the users to be rolled back so that they will not be remigrated after rollback. (Perform this step only if you want to make sure that users will not remigrate in the future.) To disable unified contact store for individual users, at the command line, type:

   ```
   Set-CsUserServicesPolicy -Identity "<policy name>" -UcsAllowed $False
   ```

   For example:

   ```
   Set-CsUserServicesPolicy -Identity "UCS Enabled Users" -UcsAllowed $Fa
   ```

3. Before moving a user from Lync Server 2013 to Lync Server 2010, roll back the Buddy List for the specified users on Lync Server.

   Important:
   If this step is omitted, the Buddy List will be lost.

4. Roll back the specified users. At the command line, type:

   ```
   Invoke-CsUcsRollback -Identity "<user display name>"
   ```

   For example:

   ```
   Invoke-CsUcsRollback -Identity "Ken Myer"
   ```

   Important:
   We do not recommend using the –Force option to force the rollback. If you use this option, the users' contacts will be lost.

To roll back unified contact store contacts from Exchange 2013 to Lync Server 2013

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Disable unified contact store for the users to be rolled back so that they will not be remigrated after rollback. To disable unified contact store for individual users, at the command line, type:

   ```
   Set-CsUserServicesPolicy -Identity "<policy name>" -UcsAllowed $False
   ```

   For example:

   ```
   Set-CsUserServicesPolicy -Identity "UCS Enabled Users" -UcsAllowed $Fa
   ```

3. Roll back the specified users. At the command line, type:

   ```
   Invoke-CsUcsRollback -Identity "<user display name>"
   ```

   For example:

   ```
   Invoke-CsUcsRollback -Identity "Ken Myer"
   ```

Important:
You must first roll back the Lync Server user, and then move the Exchange 2013 mailbox. The Exchange administrator is blocked from rolling back Exchange until the Lync Server rollback is complete. We do not recommend using the –Force option to force the rollback. If you use this option, the users' contacts will be lost.

4. After you roll back the user to Lync Server, the Exchange administrator can roll back the Exchange user from Exchange 2013 to Exchange 2010.

1.4.12 Managing Server-to-Server Authentication (Oauth) and Partner Applications

Managing Server-to-Server Authentication (Oauth) and Partner Applications

See Also

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2013-01-22*

Microsoft Lync Server 2013 must be able to securely, and seamlessly, communicate with other applications and server products. For example, you can configure Lync Server 2013 so that contact data and/or archiving data is stored in Microsoft Exchange Server 2013; however, this can only be done if Lync Server and Exchange are able to securely communicate with one another. Likewise, you can schedule a Lync Server conference from within Microsoft SharePoint Server; again, however, this can only be done if the two servers (SharePoint and Lync Server) trust one another. Although it's possible to use one authentication mechanism for Lync-to-Exchange communication and a separate mechanism for Lync-to-SharePoint communication, a better and more efficient approach is to use a standardized method for all server-to-server authentication and authorization.

Using a single, standardized method for server-to-server authentication is the approach taken by Lync Server 2013. For the 2013 release, Lync Server 2013 (as well as other Microsoft Server products, including Exchange 2013 and Microsoft SharePoint Server) support the OAuth (Open Authorization) protocol for server-to-server authentication and authorization. With OAuth, a standard authorization protocol used by a number of major websites, user credentials and passwords are not passed from one computer to another. Instead, authentication and authorization is based on the exchange of security tokens; these tokens grant access to a specific set of resources for a specific amount of time.

OAuth authentication typically involves three parties: a single authorization server and the two realms that need to communicate with one another. (You can also do server-to-server authentication without using an authorization server, a process that will be discussed later in this document.) Security tokens are issued by the authorization server (also known as a security token server) to the two realms that need to communicate; these tokens verify that communications originating from one realm should be trusted by the other realm. For example, the authorization server might issue tokens that verify that users from a specific Lync Server 2013 realm are able to access a specified Exchange 2013 realm, and vice-versa.

Note:
A realm is simply a security container. By default, Lync Server 2013 uses your default SIP domain as its OAuth realm.

Lync Server 2013 supports three server-to-server authentication scenarios. With Lync Server 2013 you can:

- Configure server-to-server authentication between an on-premise installation of Lync Server 2013 and an on-premises installation of Exchange 2013 and/or

Microsoft SharePoint Server.

- Configure server-to-server authentication between a pair of Office 365 components (for example, between Microsoft Exchange 365 and Microsoft Lync Server 365, or between Microsoft Lync Server 365 and Microsoft SharePoint 365).
- Configure server-to-server authentication in a cross-premises environment (that is, server-to-server authentication between an on-premises server and an Office 365 component).

Note that, at this point in time, only Exchange 2013, SharePoint Server, and Lync Server 2013 support server-to-server authentication; if you are not running one of these servers then you will not be able to fully implement OAuth authentication.

It should also be pointed out that you do not need to use server-to-server authentication: server-to-server authentication is not required in order to deploy Lync Server 2013. If Lync Server 2013 does not need to communicate with other servers (such as Exchange 2013) then server-to-server authentication is not needed.

However, server-to-server authentication is required if you want to use some of Lync Server's new features, such as the "unified contact store." With unified contact store, Lync Server 2013 contact information is stored in Exchange 2013 instead of in Lync Server; this enables users to have a single set of contacts that is readily accessible from within Lync, Microsoft Outlook, or Microsoft Outlook Web Access. Because the unified contact store requires Lync Server 2013 to share information with Exchange 2013, you must use server-to-server authentication in order to deploy the feature. Server-to-server authentication is also required if you choose to use Exchange archiving, in which the transcripts of instant messaging sessions are saved as Exchange 2013 emails rather than as individual database records.

For the Office 365 version of Lync Server to communicate with its Exchange counterpart, Lync Server 2013 must first obtain a security token from the authorization server. Lync Server then uses that security token to identify itself to Exchange 365. The Office 365 version of Exchange must go through the same process in order to communicate with Lync Server 2013.

However, for on-premises server-to-server authentication between two Microsoft servers there is no need to use a third-party token server. Server products such as Lync Server 2013 and Exchange 2013 have a built-in token server that can be used for authentication purposes with other Microsoft servers (such as SharePoint server) that support server-to-server authentication. For example, Lync Server 2013 can issue and sign a security token by itself, then use that token to communicate with Exchange 2013. In a case like this, there is no need for a third-party token server.

In order to configure server-to-server authentication for an on-premises implementation of Lync Server 2013 you must do two things:

- Assign a certificate to Lync Server's built-in token issuer.
- Configure the server that Lync Server 2013 will communicate with to be a "partner application." For example, if Lync Server 2013 needs to communicate with Exchange 2013 then you will need to configure Exchange to be a partner application.

Note:

A "partner application" is any application that Lync Server 2013 can directly exchange security tokens with, without having to go through a third-party security token server.

Concepts

Assigning a Server-to-Server Authentication Certificate to Microsoft Lync Server 2013
Configuring Microsoft Lync Server 2013 in a Cross-Premises Environment

1.4.12.1 Assigning a Server-to-Server Authentication Certificate to Microsoft Lync Server 2013

Assigning a Server-to-Server Authentication Certificate to Microsoft Lync Server 2013

Microsoft Lync Server 2013 > Deployment > Managing Server-to-Server Authentication (Oauth) and Partner Applications >

Topic Last Modified: *2012-10-01*

To determine whether or not a server-to-server authentication certificate has already been assigned to Microsoft Lync Server 2013, run the following command from the Lync Server 2013 Management Shell:

```
Get-CsCertificate -Type OAuthTokenIssuer
```

If no certificate information is returned you must assign a token issuer certificate before you can use server-to-server authentication. As a general rule, any Lync Server 2013 certificate can be used as your OAuthTokenIssuer certificate; for example, your Lync Server 2013 default certificate can also be used as the OAuthTokenIssuer certificate. (The OAUthTokenIssuer certificate can also be any Web server certificate that includes the name of your SIP domain in the Subject field.) The primary two requirements for the certificate used for server-to-server authentication are these: 1)the same certificate must be configured as the OAuthTokenIssuer certificate on all of your Front End Servers; and, 2) the certificate must be at least 2048 bits.

If you do not have a certificate that can be used for server-to-server authentication you can obtain a new certificate, import the new certificate, and then use that certificate for server-to-server authentication. After you have requested and obtained the new certificate you can then log on to any one of your Front End Servers and use a Windows PowerShell command similar to this one to import and assign that certificate:

```
Import-CsCertificate -Identity global -Type OAuthTokenIssuer -Path C:\Certificate
```

In the preceding command the Path parameter represents the full path to the certificate file, and the Password parameter represents the password that was assigned to the certificate. This procedure should be run just one time: Lync Server's replication service will then automatically create a set of scheduled tasks that will decrypt and deploy the certificate to all your Front End Servers.

Alternatively, you can use an existing certificate as your server-to-server authentication certificate. (As noted, the default certificate can be used as the server-to-server authentication certificate.) The following pair of Windows PowerShell commands retrieve the value of the default certificate's Thumbprint property, then use that value to make the default certificate the server-to-server authentication certificate:

```
$x = (Get-CsCertificate -Type Default).Thumbprint
Set-CsCertificate -Identity global -Type OAuthTokenIssuer -Thumbprint $x
```

In the preceding command, the retrieved certificate is configured to function as the global server-to-server authentication certificate; that means that the certificate will be replicated to, and used by, all your Front End Servers. Again, this command should only be run one time, and only on one of your Front End Servers. Although all Front End Servers must use the same certificate, you should not configure the OAuthTokenIssuer certificate on each Front End Server. Instead, configure the certificate once, then let Lync Server's replication server take care of copying that certificate to each server.

The Set-CsCertificate cmdlet takes the certificate in question and immediately configures that certificate to act as the current OAuthTokenIssuer certificate. (Lync Server 2013 keeps two copies of a certificate type: the current certificate and the previous certificate.)

If you need the new certificate to immediately begin to act as the OAuthTokenIssuer certificate then you should use the Set-CsCertificate cmdlet.

You can also use the Set-CsCertificate cmdlet to "roll" a new certificate. "Rolling" a certificate simply means that you configure a new certificate to become the current OAuthTokenIssuer certificate at a specified point in time. For example, this command retrieves the default certificate and then configure that certificate to take over as the current OAuthTokenIssuer certificate as of July 1, 2012:

```
$x = (Get-CsCertificate -Type Default).Thumbprint
Set-CsCertificate -Identity global -Type OAuthTokenIssuer -Thumbprint $x -Effecti
```

On July 1, 2012 the new certificate will be configured as the current OAuthTokenIssuer certificate and the "old" OAuthTokenIssuer certificate will be configured as the previous certificate.

If you do not want to use Windows PowerShell you can also use the Certificates MMC console to export a certificate from one Front End Server and then import that same certificate on all your other Front End Servers. If you do this, make sure that you export the private key along with the certificate itself.

Caution:

In this case, the procedure must be performed on each Front End Server. When exporting and importing certificates in this manner Lync Server 2013 will not replicate that certificate to each Front End Server.

After the certificate has been imported to all your Front End Servers, that certificate can then be assigned by using the Lync Server Deployment Wizard instead of Windows PowerShell. To assign a certificate by using the Deployment Wizard, complete the following steps on a computer where the Deployment Wizard has been installed:

1. Click Start, click All Programs, click **Microsoft Lync Server 2013 (Technical Preview)**, and then click **Lync Server Deployment Wizard**.
2. In the Deployment Wizard, click **Install or Update Lync Server System**.
3. On the **Lync Server 2013 (Technical Preview)** page, click the **Run** button under the heading **Step 3: Request, Install or Assign Certificates**. (Note: If you have already installed certificates on this computer then the **Run** button will be labeled **Run Again**.)
4. In the Certificate Wizard, select the **OAuthTokenIssuer** certificate and then click **Assign**.
5. In the Certificate Assignment wizard, on the **Certificate Assignment** page, click **Next**.
6. On the **Certificate Store** page, select the certificate to be used for server-to-server authentication and then click **Next**.
7. On the Certificate Assignment Summary page, click **Next**.
8. On the Executing Commands page, click **Finish**.
9. Close the Certificate Wizard and the Deployment Wizard.

1.4.12.2 Configuring an On-Premises Partner Application for Microsoft Lync Server 2013

Configuring an On-Premises Partner Application for Microsoft Lync Server 2013

Microsoft Lync Server 2013 > Deployment > Managing Server-to-Server Authentication (Oauth) and Partner Applications >

Topic Last Modified: *2013-02-04*

After you have assigned the OAuthTokenIssuer certificate you must then configure your

Microsoft Lync Server 2013 partner applications. (The procedure about to be discussed configures both Microsoft Exchange Server 2013 and Microsoft SharePoint to act as partner applications.) To configure an on-premises partner application, you must start by copying the following Windows PowerShell script and pasting the code into Notepad (or any other text editor):

```
if ((Get-CsPartnerApplication -ErrorAction SilentlyContinue) -ne $Null)
   {
       Remove-CsPartnerApplication app
   }
$exch = Get-CsPartnerApplication microsoft.exchange -ErrorAction SilentlyContinue
if ($exch -eq $null)
   {
      New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl https://
    }
else
    {
       if ($exch.ApplicationIdentifier -ne "00000002-0000-0ff1-ce00-000000000000"
          {
             Remove-CsPartnerApplication microsoft.exchange
New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl https://atl-ex
           }
        else
           {
             Set-CsPartnerApplication -Identity microsoft.exchange -ApplicationTr
           }
     }
$shp = Get-CsPartnerApplication microsoft.sharepoint -ErrorAction SilentlyContinu
if ($shp -eq $null)
   {
      New-CsPartnerApplication -Identity microsoft.sharepoint -MetadataUrl http:/
    }
else
    {
       if ($shp.ApplicationIdentifier -ne "00000003-0000-0ff1-ce00-000000000000")
          {
             Remove-CsPartnerApplication microsoft.sharepoint
             New-CsPartnerApplication -Identity microsoft.sharepoint -MetadataUrl
           }
        else
           {
             Set-CsPartnerApplication -Identity microsoft.sharepoint -Application
            }
   }
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000
```

After copying the code, save the script using a .PS1 file extension (for example, C:\Scripts \ServerToServerAuth.ps1). Note that, before you run this script, you must replace the metadata URLs https://atl-exchange-001.litwareinc.com/autodiscover/metadata/json/1 and http://atl-sharepoint-001.litwareinc.com/jsonmetadata.ashx with the metadata URLs used by your Exchange 2013 and SharePoint servers, respectively. See the product documentation for Exchange 2013 and SharePoint for information on how you can identify the respective product's metadata URL.

If you look at the last line of the script you will notice that the Set-CsOAuthConfiguration cmdlet is called using this syntax:

```
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000
```

Because the Realm parameter was not used when calling Set-CsOAuthConfiguration the realm will automatically be set to the fully qualified domain name (FQDN) of your organization (for example, litwareinc.com). If your realm name is different from your organization name then you should include the realm name, like this:

```
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000 -Realm
```

After making these changes you can then execute the script, and configure both Exchange 2013 and SharePoint as partner applications, by running the script file from within the Lync Server 2013 Management Shell. For example:

```
C:\Scripts\ServerToServerAuth.ps1
```

Note that you can run this script even if you do not have both Exchange 2013 and SharePoint Server installed:, no problems will occur if you, say, configure SharePoint Server as a partner application even though you do not have SharePoint Server installed.

When you run this script you might receive an error message similar to the following:

```
New-CsPartnerApplication : Cannot bind parameter 'MetadataUrl' to the target. Exc
```

This error message typically means one of two things: 1) that one of the URLs specified in the script is not valid (that is, one of your metadata URLs is not an actual metadata URL); or, 2) one of the metadata URLs could not be contacted. If this happens, verify that the URLs are correct and are accessible, and the re-run the script.

After creating the partner application for Lync Server 2013 you must then configure Lync Server to be a partner application for Exchange 2013. You can configure partner applications for Exchange 2013 by running the script Configure-EnterprisePartnerApplication.ps1; all you need to do is specify the metadata URL for Lync Server and indicate that Lync Server is the new partner application.

To configure Lync Server as a partner application for Exchange, open the Exchange Management Shell and run a command similar to this

```
"c:\Program Files\Microsoft\Exchange Server\V15\Scripts\Configure-EnterprisePartn
```

1.4.12.3 Configuring Microsoft Lync Server 2013 in a Cross-Premises Environment

Configuring Microsoft Lync Server 2013 in a Cross-Premises Environment

Microsoft Lync Server 2013 > Deployment > Managing Server-to-Server Authentication (Oauth) and Partner Applications >

Topic Last Modified: *2012-10-02*

In a cross-premise configuration, some of your users are homed on an on-premises installation of Microsoft Lync Server 2013 while other users are homed on the Office 365 version of Lync Server. In order to configure server-to-server authentication in a cross-premises environment, you must first configure your on-premises installation of Lync Server 2013 to trust the Office 365 Authorization server. The initial step in this process can be carried out by running the following Lync Server Management Shell script:

```
$TenantID = (Get-CsTenant -DisplayName "Fabrikam.com").TenantId
$sts = Get-CsOAuthServer microsoft.sts -ErrorAction SilentlyContinue
   if ($sts -eq $null)
      {
         New-CsOAuthServer microsoft.sts -MetadataUrl "https://accounts.accesscon
      }
   else
      {
         if ($sts.MetadataUrl -ne  "https://accounts.accesscontrol.windows.net/$T
            {
               Remove-CsOAuthServer microsoft.sts
               New-CsOAuthServer microsoft.sts -MetadataUrl "https://accounts.acc
            }
        }
```

```
$exch = Get-CsPartnerApplication microsoft.exchange -ErrorAction SilentlyContinue
if ($exch -eq $null)
   {
      New-CsPartnerApplication -Identity microsoft.exchange -ApplicationIdentifie
    }
else
    {
       if ($exch.ApplicationIdentifier -ne "00000002-0000-0ff1-ce00-000000000000"
          {
             Remove-CsPartnerApplication microsoft.exchange
             New-CsPartnerApplication -Identity microsoft.exchange -ApplicationId
          }
       else
          {
             Set-CsPartnerApplication -Identity microsoft.exchange -ApplicationTr
          }
   }
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000
```

Keep in mind that the realm name for a tenant is typically different than the organization name; in fact, the realm name is almost always the same as the tenant ID. Because of that, the first line in the script is used to return the value of the TenantId property for the specified tenant (in this case, fabrikam.com) and then assign that name to the variable $TenantId:

```
$TenantID = (Get-CsTenant -DisplayName "Fabrikam.com").TenantId
```

After the script completes you must then configure a trust relationship between Lync Server 2013 and the authorization server, and a second trust relationship between Exchange 2013 and the authorization server. This can only be done by using the Microsoft Online Services cmdlets.

Note:

If you have not installed the Microsoft Online Services cmdlets you will need to do two things before proceeding. First, download and install the 64-bit version of the Microsoft Online Services Sign-in Assistant. After installation is complete, download and install the 64-bit version of the Microsoft Online Services Module for Windows PowerShell. Detailed information for installing and using the Microsoft Online Services Module can be found on the Office 365 web site. These instructions will also tell you how to configure single sign-on, federation, and synchronization between Office 365 and Active Directory.

After you have configured Office 365, and after you have created Office 365 service principals for Lync Server 2013 and Exchange 2013, you will then need to register your credentials with these service principals. In order to do this, you must first obtain an X.509 Base64 saved as a .CER file. This certificate will then be applied to the Office 365 service principals.

When you have obtained the X.509 certificate, start the Microsoft Online Services Module (click **Start**, click **All Programs**, click **Microsoft Online Services**, and then click **Microsoft Online Services Module for Windows PowerShell**). After the Services Module opens, type the following to import the Microsoft Online Windows PowerShell module containing the cmdlets that can be used to manage service principals:

```
Import-Module MSOnlineExtended
```

When the module has been imported, type the following command and then press ENTER in order to connect to Office 365:

```
Connect-MsolService
```

After you press ENTER, a credentials dialog box will appear. Enter your Office 365 user name and password in the dialog box, and then click OK.

As soon as you are connected to Office 365 you can then run the following command in order to return information about your service principals:

```
Get-MsolServicePrincipal
```

You should get back information similar to this for all your service principals:

```
ExtensionData        : System.Runtime.Serialization.ExtensionDataObject
AccountEnabled       : True
Addresses            : {}
AppPrincipalId       : 00000004-0000-0ff1-ce00-000000000000
DisplayName          : Microsoft Lync Server
ObjectId             : aada5fbd-c0ae-442a-8c0b-36fec40602e2
ServicePrincipalName : LyncServer/litwareinc.com
TrustedForDelegation : True
```

The next step is to import, encode, and assign the X.509 certificate. To import and encode the certificate, use the following Windows PowerShell commands, being sure to specify the complete file path to your .CER file when you call the Import method:

```
$certificate = New-Object System.Security.Cryptography.X509Certificates.X509Certi
$certificate.Import("C:\Certificates\Office365.cer")
$binaryValue = $certificate.GetRawCertData()
$credentialsValue = [System.Convert]::ToBase64String($binaryValue)
```

After the certificate has been imported and encoded, you can then assign the certificate to your Office 365 service principals. To do that, first use the Get-MsolServicePrincipal to retrieve the value of the AppPrincipalId property for both the Lync Server and the Microsoft Exchange service principals; the value of the AppPrincipalId property will be used to identify the service principal being assigned the certificate. With the AppPrincipalId property value for Lync Server 2013 in hand, use the following command to assign the certificate to the Office 365 version of Lync Server (the StartDate and EndDate properties should correspond to the validity period for the certificate):

```
New-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000000
```

You should then repeat the command, this time using the AppPrincipalId property value for Exchange 2013.

If you later need to delete that certificate, you can do so by first retrieving the KeyId for the certificate:

```
Get-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000000
```

That command will return data like this one:

```
Type      : Asymmetric
Value     :
KeyId     : bc2795f3-2387-4543-a95d-f92c85c7a1b0
StartDate : 6/1/2012 8:00:00 AM
EndDate   : 5/31/2013 8:00:00 AM
Usage     : Verify
```

You can then delete the certificate by using a command similar to this:

```
Remove-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000
```

In addition to assigning a certificate you must also configure the Exchange Online Service Principal and configure your on-premise version of Lync Server 2013 as an Office 365 service principal. That can be done by carrying out the following two commands:

```
Set-MSOLServicePrincipal -AppPrincipalID 00000002-0000-0ff1-ce00-000000000000 -Ac
$lyncSP = Get-MSOLServicePrincipal -AppPrincipalID 00000004-0000-0ff1-ce00-000000
$lyncSP.ServicePrincipalNames.Add("00000004-0000-0ff1-ce00-000000000000/lync.cont
Set-MSOLServicePrincipal -AppPrincipalID 00000004-0000-0ff1-ce00-000000000000 -Se
```

1.4.13 Updating From the Evaluation Version of Lync Server 2013

Updating From the Evaluation Version of Lync Server 2013

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-06-20*

If you have installed the Evaluation version of Microsoft Lync Server 2013, you will eventually need to update that installation a licensed copy of the software; that's because the evaluation version expires 180 days after it was installed. However, you will not need to completely uninstall the evaluation version and then install the licensed version. Instead, after you have obtained a valid licensing key, you can update the evaluation version of Lync Server 2013 by carrying out the following procedure on each computer acting as a Lync Server Front End Server, Director, or Edge Server. Note that you do not have to update computers carrying out other server roles, such as a Monitoring Server or Archiving Server.

Updating from the Evaluation Version of Microsoft Lync Server 2013

To update a computer from the evaluation version of Lync Server 2013 to the licensed version of the software:

Updating from the Evaluation Version of Microsoft Lync Server 2013

1. Log on to the computer as a local administrator.
2. Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. In the Lync Server Management Shell, type the following command and then press ENTER:

   ```
   msiexec.exe /fvomus server.msi EVALTOFULL=1 /qb
   ```

   Note that you might need to specify the full path to the file server.msi. This file can be found in the Setup folder of the Lync Server Volume media installation files.
4. After Setup finishes running, type the following from the command prompt and then press ENTER:

   ```
   Enable-CsComputer
   ```
5. Repeat this procedure on any other Front End Server, Director, or Edge Server running an evaluation copy of Lync Server. This procedure should also be performed on any Branch Office Servers that were deployed by using the Lync Server media installation files.

If you are not sure if the evaluation version of Lync Server is running on a given computer you can verify that by running the following command from within the Lync Server Management Shell:

```
Get-CsServerVersion
```

The Get-CsServerVersion cmdlet will analyze the local computer and report back one of the following:

- That the Lync Server volume license key has been installed on the computer, meaning that no updating is necessary.
- That the Lync Server evaluation license key has been installed, meaning that

the computer must be updated.

- That no volume license key is required on the computer. Updating from the evaluation version to the licensed version is only required on Front End Servers, Directors, and Edge Servers.

1.4.14 Deploying Remote Call Control

Deploying Remote Call Control

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-10-20*

This section guides you through the process of deploying remote call control functionality to users in your organization.

> **Note:**
> Although remote call control features are available to remote users while they are outside of your organization’s firewall, details about deploying external access scenarios are beyond the scope of this documentation. For details about deploying external user access, see Deploying External User Access in the Deployment documentation.

- Configuring Lync Server 2013 to Route to a SIP/CSTA Gateway
- Configure a Static Route for Remote Call Control
- Configure a Trusted Application Entry for Remote Call Control
- Define a SIP/CSTA Gateway IP Address (only if the gateway is configured to use TCP)
- Enable Lync Users for Remote Call Control
- Remote Call Control and Phone Number Normalization
- Remove a Legacy Authorized Host (Optional) (only if you are migrating users previously enabled for remote call control)

⊟Related Sections

Planning for Remote Call Control

1.4.14.1 Configuring Lync Server 2013 to Route to a SIP/CSTA Gateway

Configuring Lync Server 2013 to Route to a SIP/CSTA Gateway

Microsoft Lync Server 2013 > Deployment > Deploying Remote Call Control >

Topic Last Modified: *2012-10-05*

A SIP/CSTA gateway is a gateway between SIP and a computer-supported telecommunications application (CSTA). A SIP/CSTA gateway provides the interface between an existing private branch exchange (PBX) and Lync Server for routing remote call control requests to the PBX. After you install a SIP/CSTA gateway, you must perform the following procedures on each Lync Server pool for which you want to configure remote call control:

- Configure a Static Route for Remote Call Control
- Configure a Trusted Application Entry for Remote Call Control

1.4.14.2 Configure a Static Route for Remote Call Control

Configure a Static Route for Remote Call Control

See Also

Topic Last Modified: *2012-09-22*

Remote call control requires that every Lync Server pool is configured with a path from that pool to the SIP/CSTA gateway that connects to the private branch exchange (PBX). This path requires that each pool has one static route for each gateway to which the pool will proxy SIP call control messages associated with calls to the PBX. If you configure a global static route for remote call control, each pool that is not configured with a static route at the pool level will use the global static route.

To configure a static route for remote call control

1. Log on to a computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or a role-based access control (RBAC) role to which you have assigned the **New-CsStaticRoute** cmdlet.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. To create a static route and put it in the variable $TLSRoute or $TCPRoute, do one of the following:

Tip:

To match child domains of a domain, you can specify a wildcard value in the MatchUri parameter. For example, ***.contoso.net**. That value matches any domain that ends with the suffix **contoso.net**.

- For a Transport Layer Security (TLS) connection, type the following at the command prompt:

```
$TLSRoute = New-CsStaticRoute -TLSRoute -Destination <gatewa
```

For example:

```
$TLSRoute = New-CsStaticRoute -TLSRoute -Destination rccgate
```

If UseDefaultCertificate is set to False, you must specify TLSCertIssuer and TLSCertSerialNumber parameters. These parameters indicate the name of the certification authority (CA) that issued the certificate used in the static route, and the serial number of that TLS certificate, respectively. For details about these parameters, see Lync Server Management Shell Help by typing the following at the command prompt:

```
Get-Help New-CsStaticRoute -Full
```

- For a Transmission Control Protocol (TCP) connection, type the following at the command prompt:

Note:

If you specify a fully qualified domain name (FQDN), you must configure a Domain Name System (DNS) A record first.

```
$TCPRoute = New-CsStaticRoute -TCPRoute -Destination <gatewa
```

For example:

```
$TCPRoute = New-CsStaticRoute -TCPRoute -Destination 192.168
```

The following are default values for optional parameters for static routes:

- Enabled = True
- MatchOnlyPhoneUri = False
- ReplaceHostInRequestUri = False

We strongly recommend that you do not change these default values. However, if you must change any of these parameters, see Lync Server Management Shell Help by typing the following at the command prompt:

```
Get-Help New-CsStaticRoute -Full
```

4. To persist a newly created static route in the Central Management store, run one of the following, as appropriate:

```
Set-CsStaticRoutingConfiguration -Route @{Add=$TLSRoute}
```

```
Set-CsStaticRoutingConfiguration -Route @{Add=$TCPRoute}
```

Tasks

Configure a Trusted Application Entry for Remote Call Control
Define a SIP/CSTA Gateway IP Address

1.4.14.3 Configure a Trusted Application Entry for Remote Call Control

Configure a Trusted Application Entry for Remote Call Control

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Remote Call Control >

Topic Last Modified: *2012-10-22*

The SIP/CSTA gateway must be configured as a trusted application in order for Lync Server to apply a static route to route calls to the gateway.

Important:
If you are migrating users from a previous version of Lync Server deployment, be sure that you removed all existing trusted application entries (previously known as authorized host entries) you created for the SIP/CSTA gateway before following the procedures in this topic. For details, see Remove a Legacy Authorized Host (Optional).

To configure a trusted application entry for the SIP/CSTA gateway

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or a role-based access control (RBAC) role to which you have assigned the **New-CsTrustedApplicationPool** cmdlet.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. To create a trusted application entry, do one of the following:
   - For a Transport Layer Security (TLS) connection, type the following at the command prompt:

     ```
     New-CsTrustedApplicationPool -Identity <FQDN of the SIP/CSTA
     ```

     For example:

     ```
     New-CsTrustedApplicationPool -Identity rccgateway.contoso.ne
     ```

   - For a Transmission Control Protocol (TCP) connection, type the following at the command prompt:

     ```
     New-CsTrustedApplicationPool -Identity <IP address or FQDN o
     ```

     For example:

     ```
     New-CsTrustedApplicationPool -Identity 192.168.0.240 -Regist
     ```

4. To add the trusted application to the pool, do one of the following:
   - For a TLS connection, type the following at the command prompt:

     ```
     New-CsTrustedApplication -ApplicationID <application name> -
     ```

     For example:

```
New-CsTrustedApplication -ApplicationID RccGateway-1 -Truste
```

- For a TCP connection, type the following at the command prompt:

```
New-CsTrustedApplication -ApplicationID <application name> -
```

  For example:

```
New-CsTrustedApplication -ApplicationID RccGateway-1 -Truste
```

5. To implement the published changes you have made to the topology, type the following at the command prompt:

```
Enable-CsTopology
```

Tasks

Configure a Static Route for Remote Call Control
Define a SIP/CSTA Gateway IP Address

1.4.14.4 Define a SIP/CSTA Gateway IP Address

Define a SIP/CSTA Gateway IP Address

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Remote Call Control >

Topic Last Modified: *2012-09-21*

If Lync Server will connect to the SIP/CSTA gateway that you deployed for remote call control by using a Transmission Control Protocol (TCP) connection, then you must define the IP address of the gateway in Topology Builder. This step is not necessary for gateways that support Transport Layer Security (TLS) connections. For any gateway that supports TLS connections, you can skip this procedure and continue deployment of remote call control by following the steps in Enable Lync Users for Remote Call Control.

⊟To define the SIP/CSTA gateway IP address by using Topology Builder

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
3. Choose the option to download an existing topology.
4. Expand the **Trusted application servers** node.
5. Right-click the trusted application pool that you created, as described in Configure a Trusted Application Entry for Remote Call Control, and then click **Edit Properties**.
6. Clear the **Enable replication of configuration data to this pool** check box.
7. Click **Limit service usage to selected IP addresses**. The default setting is **Use all configured IP addresses**.
8. In the **Primary IP address** text box, enter the IP address of the SIP/CSTA gateway.
9. To update the topology in the Central Management store, in the console tree, click **Lync Server**, and then, from the **Actions** pane, click **Publish**.

Tasks

Configure a Static Route for Remote Call Control
Configure a Trusted Application Entry for Remote Call Control

1.4.14.5 Enable Lync Users for Remote Call Control

Enable Lync Users for Remote Call Control

Microsoft Lync Server 2013 > Deployment > Deploying Remote Call Control >

Topic Last Modified: *2012-09-21*

You can configure Lync users for remote call control by using in-band provisioning policies that are server-based. You can manage in-band provisioning settings by using Lync Server Control Panel or the Lync Server Management Shell command-line interface. These tools replace the Windows Management Instrumentation (WMI) snap-in that was used to manage Group Policy settings in earlier releases.

If you prefer to let users to configure their own remote call control settings in Lync, you can configure remote call control settings for users on the server without specifying **Line Server URI** and **Line URI** values. Be sure that you communicate the appropriate **Line Server URI** and **Line URI** values to your users, and provide your users with the instructions to configure these settings. For the procedure to manually configure remote call control in Lync Server, see "Set Phones options and numbers" at http://go.microsoft.com/fwlink/p/?linkid=210132 in the Lync client documentation on the Microsoft Office website.

If you have an existing Communications Server 2007 R2 or Communications Server 2007 deployment, Communicator 2007 R2 and Communicator 2007 clients will continue to use Group Policy during side-by-side migration. However, if you want policy settings to carry over to Lync clients, you need to configure the equivalent Lync Server in-band provisioning settings.

Note:

To enable a user for remote call control, you need to provide the user with both a Line URI and a Line Server URI. As described in Deployment Tasks for Remote Call Control, you need to be sure to use the syntax that is required by the gateway for these settings.
Be sure that the domain in the Line Server URI is the same as the destination domain that you specified in the MatchUri parameter when you configured the static route to the gateway.
The Line URI specifies the phone number assigned to the user in E.164 format, with the "TEL:" prefix (for example, tel:+14255550150). If you want to configure an extension number, then the format is tel:+14255550150;ext=111. If you previously configured the user's Line URI and the value has not changed, you do not need to specify the Line URI when you enable the user for remote call control.

⊟To enable remote call control for Lync-enabled users by using Management Shell

1. Log on to a computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or as a role-based access control role to which you have assigned the **Set-CsUser** cmdlet.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. To use the **Set-CsUser** cmdlet to configure remote call control for an existing Lync-enabled user, do the following:

   ```
   Set-CsUser -Identity <User ID> -EnterpriseVoiceEnabled $false -LineSer
   ```

   For example:

   ```
   Set-CsUser -Identity "Katie Jordan" -EnterpriseVoiceEnabled $false -Li
   ```

⊟To configure users for remote call control by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all (or the first portion) of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want, and then click **Find**.
5. In the table, click the user account that you want to modify.
6. On the **Edit** menu, click **Modify**.
7. In **Telephony**, do one of the following:
   - To enable remote call control to enable the user to control their private branch exchange (PBX) phone from Lync 2013 to make PC-to-PC audio calls and PC-to-phone calls, click **Remote call control**. In **Line URI**, specify the telephone number of the user. In **Line Server URI**, specify the SIP URI of the SIP/CSTA gateway.
   - To enable remote call control, but disable PC-to-PC audio calls, and to enable only the user to control their PBX phone from Lync 2013 to make PC-to-phone calls, click **Remote call control only**. In **Line URI**, specify the telephone number of the user. In **Line Server URI**, specify the SIP URI of the SIP/CSTA gateway.
8. When you are finished, click **Commit**.

1.4.14.6 Remote Call Control and Phone Number Normalization

Remote Call Control and Phone Number Normalization

Microsoft Lync Server 2013 > Deployment > Deploying Remote Call Control >

Topic Last Modified: *2012-09-22*

Lync clients download phone number normalization rules as part of the Address Book Service (ABS) file download. In remote call control scenarios, Address Book Service phone number normalization rules are applied to both incoming and outgoing remote call control calls. For incoming calls to a remote call control-enabled user, the phone number of the caller is first normalized to E.164 format by either the SIP/CSTA gateway or private branch exchange (PBX). When Lync Server 2013 receives the call from the gateway, it performs reverse number lookup (RNL) on the phone number of the caller against the normalized number in the callee’s Microsoft Office Outlook Contacts list or the global address list (GAL) that is stored in the Address Book Service. If reverse number lookup successfully finds a match, the caller is identified by name in the incoming call notification.

For outgoing remote call control calls, Lync applies the Address Book Service phone number normalization rules to the dialed number before routing the call to the SIP/CSTA gateway.

For details about creating phone number normalization rules for remote call control, see Dial Plans and Normalization Rules in the Planning documentation.

Migrating Phone Number Normalization Rules

If you are migrating users previously enabled for remote call control, see the following topics in the Migration documentation:

- For Lync Server 2010, see Migrate Address Book in the Migration

documentation.
- For Communications Server 2007 R2, see Migrate Address Book in the Migration documentation.

1.4.14.7 Remove a Legacy Authorized Host (Optional)

Remove a Legacy Authorized Host (Optional)

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Remote Call Control >

Topic Last Modified: *2012-09-05*

When you migrate remote call control to a Lync Server deployment, you must remove legacy authorized host entries (known as *trusted application entries* in Lync Server) for any SIP/CSTA gateways in your legacy deployment. You must use the administrative tools to remove authorized host entries from those deployments, respectively.

Tasks

Configure a Trusted Application Entry for Remote Call Control

1.4.15 Deploying Mobility

Deploying Mobility

Microsoft Lync Server 2013 > Deployment > Deploying External User Access >

Topic Last Modified: *2012-09-08*

When you deploy the Lync Server 2013 mobility feature, mobile users can use supported mobile devices for Lync functionality such as instant messaging (IM), presence, and contacts.

For details about requirements for deploying the mobility feature, see Planning for Mobility.

This section guides you through the steps for deploying and verifying the mobility and automatic discovery features.

- Creating DNS Records for the Autodiscover Service
- Modifying Certificates for Mobility
- Configuring the Reverse Proxy for Mobility
- Configuring Autodiscover for Mobility with Hybrid Deployments
- Verifying Your Mobility Deployment
- Configuring for Push Notifications
- Configuring Mobility Policy

1.4.15.1 Creating DNS Records for the Autodiscover Service

Creating DNS Records for the Autodiscover Service

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2012-10-05*

To support autodiscovery for Lync Mobile users, you need to create the following Domain Name System (DNS) records:

- An internal DNS record to support mobile users who connect from within your organization's network
- An external, or public, DNS record to support mobile users who connect from the Internet

Or

- An external, or public, DNS record to support mobile users who connect from the Internet

You must create an internal DNS record and an external DNS record for each SIP domain.

The DNS records can be either A (host) records or CNAME records. The following procedures describe how to create internal and external DNS records. For more details about the DNS requirements for mobile users, see Technical Requirements for Mobility.

⊟To create DNS CNAME records

1. Log on to a DNS server as follows:
   - To create an internal DNS record, log on to a DNS server in your network as a member of the Domain Admins group or a member of the DnsAdmins group.
   - To create an external DNS record, connect to your public DNS provider.
2. Open the DNS administrative snap-in: Click **Start**, click **Administrative Tools**, and then click **DNS**.
3. Do one of the following:
   - For an internal DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your Active Directory domain (for example, contoso.local).

Note:
This domain is the Active Directory domain where your Lync Server 2013 Director pool and Front End pool are installed.

   - For an external DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).
4. Verify that a host A record exists for your Director pool as follows:
   - For an internal DNS record, a host A record should exist for the internal Web Services fully qualified domain name (FQDN) for your Director pool (for example, lyncwebdir01.contoso.local).
   - For an external DNS record, a host A record should exist for the external web services FQDN for your Director pool (for example, lyncwebextdir.contoso.com).
5. Verify that a host A record exists for your Front End pool as follows:
   - For an internal DNS record, a host A record should exist for the internal Web Services FQDN for your Front End pool (for example, lyncwebpool01.contoso.local).
   - For an external DNS record, a host A record should exist for the external Web Services FQDN for your Front End pool (for example, lyncwebextpool01.contoso.com).
6. For an internal DNS record, in the console tree of your DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).

Note:
If you are creating an external DNS record, **Forward Lookup Zones** is already expanded for your SIP domain from step 3.

7. Right-click the SIP domain name, and then click **New Alias (CNAME)**.
8. In **Alias name**, type one of the following:
   - For an internal DNS record, type lyncdiscoverinternal as the host name for the internal Autodiscover Service URL.
   - For an external DNS record, type lyncdiscover as the host name for the external Autodiscover Service URL.

9. In **Fully qualified domain name (FQDN) for target host**, do one of the following:
   - For an internal DNS record, type or browse to the internal Web Services FQDN for your Director pool (for example, lyncwebdir01.contoso.local), and then click **OK**.
   - For an external DNS record, type or browse to the external Web Services FQDN for your Director pool (for example, lyncwebextdir.contoso.com), and then click **OK**.

   Note:
   If you do not use a Director, use the internal and external Web Services FQDN for the Front End pool, or, for a single server, the FQDN for the Front End Server or Standard Edition server.

   Important:
   You must create a new Autodiscover CNAME record in the forward lookup zone of each SIP domain that you support in your Lync Server 2013 environment.

To create DNS A records

1. Log on to a DNS server as follows:
   - To create an internal DNS record, log on to a DNS server in your network as a member of the Domain Admins group or a member of the DnsAdmins group.
   - To create an external DNS record, connect to your public DNS provider.
2. Open the DNS administrative snap-in: Click **Start**, click **Administrative Tools**, and then click **DNS**.
3. Do one of the following:
   - For an internal DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your Active Directory domain (for example, contoso.local).

     Note:
     This domain is the Active Directory domain where your Lync Server 2013 Director pool and Front End pool are installed.
   - For an external DNS record, in the console tree of the DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).
4. Verify that a host A (for IPv6, AAAA) record exists for your Director pool as follows:
   - For an internal DNS record, a host A (for IPv6, AAAA) record should exist for the internal Web Services FQDN for your Director pool (for example, lyncwebdir01.contoso.local).
   - For an external DNS record, a host A (for IPv6, AAAA) record should exist for the external Web Services FQDN for your Director pool (for example, lyncwebextdir.contoso.com).
5. Verify that a host A (for IPv6, AAAA) record exists for your Front End pool as follows:
   - For an internal DNS record, a host A (for IPv6, AAAA) record should exist for the internal Web Services FQDN for your Front End pool (for example, lyncwebpool01.contoso.local).
   - For an external DNS record, a host A (for IPv6, AAAA) record should exist for the external Web Services FQDN for your Front End pool (for example, lyncwebextpool01.contoso.com).
6. For an internal DNS record, in the console tree of your DNS server, expand **Forward Lookup Zones** for your SIP domain (for example, contoso.com).

   Note:
   If you are creating an external DNS record, **Forward Lookup Zones** is already expanded for your SIP domain from step 3.

7. Right-click the SIP domain name, and then click **New Host (A or AAAA)**.
8. In **Name**, type the host name as follows:
   - For an internal DNS record, type lyncdiscoverinternal as the host name for the internal Autodiscover Service URL.
   - For an external DNS record, type lyncdiscover as the host name for the external Autodiscover Service URL.

   Note:
   The domain name is assumed from the zone in which the record is defined and, therefore, does not need to be entered as part of the A record.
9. In **IP Address**, type the IP address as follows:
   - For an internal DNS record, type the internal Web Services IP address of the Director (or, if you use a load balancer, type the virtual IP (VIP) of the Director load balancer).

     Note:
     If you do not use a Director, type the IP address of the Front End Server or Standard Edition server, or, if you use a load balancer, type the VIP of the Front End pool load balancer.
   - For an external DNS record, type the external or public IP address of the reverse proxy.
10. Click **Add Host**, and then click **OK**.
11. To create an additional A record, repeat steps 8 through 10.

    Important:
    You must create a new Autodiscover A record in the forward lookup zone of each SIP domain that you support in your Lync Server 2013 environment.
12. When you are finished creating A (for IPv6, AAAA) records, click **Done**.

1.4.15.2 Modifying Certificates for Mobility

Modifying Certificates for Mobility

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2012-10-18*

The certificates for your Director pool, Front End pool, and reverse proxy require additional subject alternative name entries to support secure connections with mobile clients. For details about certificate requirements for mobility, see Technical Requirements for Mobility.

Note:
You can use the **Get-CsCertificate** cmdlet to view information about the currently assigned certificates. However, the default view truncates the properties of the certificate and does not display all values in the SubjectAlternativeNames property. You can use the **Get-CsCertificate** , **Request-**CsCertificate and the **Set-CsCertificate** cmdlets to view some information and to request and assign certificates. However, it’s not the best method to use if you are unsure of the properties of the subject alternative names (SAN) on the current certificate. To view the certificate and all property members, it is suggested to use the Certificates snap-in the *Microsoft Management Console (MMC)* or to use the Lync Server Deployment Wizard. In the Lync Server Deployment Wizard, you can use the Certificate Wizard to view the certificate properties. The procedures for viewing, requesting and assigning a certificate using the Lync Server Management Shell and the *Microsoft Management Console (MMC)* are detailed in the following procedures. To use the Lync Server Deployment Wizard, see details here if you have deployed the optional Director or Director pool: Configure Certificates for the Director. For the Front End Server or Front End pool, see the details here: Configure Certificates for Servers
The initial steps in this procedure are preparation steps, to orient you as to what role the current certificates play. By default, the certificates will not have a

lyncdiscover.<sipdomain> or lyncdiscoverinternal.<internal domain name> entry unless you have previously installed Mobility Services or have prepared your certificates in advance. This procedure uses the example SIP domain name 'contoso.com' and the example internal domain name 'contoso.net'.
The default certificate configuration for Lync Server 2013 and Lync Server 2010 is to use a single certificate (named 'Default') with the purposes Default (for all purposes except for the web services), WebServicesExternal and WebServicesInternal. An optional configuration is to use separate certificates for each purpose. Certificates can be managed by using the Lync Server Management Shell and Windows PowerShell cmdlets, or by using the Certificate Wizard in the Lync Server Deployment Wizard.

To update certificates with new subject alternative names using the Lync Server Management Shell

1. Log on to the computer using an account that has local administrator rights and permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Find out what certificates have been assigned to the server and for which type of use. You need this information in the next step to assign the updated certificate. At the command line, type:

```
Get-CsCertificate
```

4. Look in the output from the previous step to see whether a single certificate is assigned for multiple uses or whether a different certificate is assigned for each use. Look in the Use parameter to find out how a certificate is used. Compare the Thumbprint parameter for the displayed certificates to see if the same certificate has multiple uses.
5. Update the certificate. At the command line, type:

```
Set-CsCertificate -Type <type of certificate as displayed in the Use p
```

For example, if the **Get-CsCertificate** cmdlet displayed a certificate with Use of Default, another with a Use of WebServicesInternal, and another with a Use of WebServicesExternal, and they all had the same Thumbprint value, at the command line, type:

```
Set-CsCertificate -Type Default,WebServicesInternal,WebServicesExterna
```

Important:
If a separate certificate is assigned for each use (the Thumbprint value is different for each certificate), it is important that you do not run the **Set-CsCertificate** cmdlet with multiple types. In this case, run the **Set-CsCertificate** cmdlet separately for each use. For example:

```
Set-CsCertificate -Type Default -Thumbprint <Certificate Thumbprint>
Set-CsCertificate -Type WebServicesInternal -Thumbprint <Certificate T
Set-CsCertificate -Type WebServicesExternal -Thumbprint <Certificate T
```

6. To view the certificate, click **Start**, click **Run...**. Type MMC to open the Microsoft Management Console.
7. From the MMC menu, select **File**, select **Add/Remove snap-in...**, select Certificates. Click **Add**. When prompted, select **Computer account**, then click **Next**.
8. If this is the computer where the certificate is located, select **Local computer**. If the certificate is located on another computer, select **Another computer**, type in the fully qualified domain name of the computer or click **Browse** In **Enter the object name to select**, type the name of the computer. Click **Check Names**. When the name of the computer is resolved, it will be underlined. Click **OK**, then click **Finish**. Click **OK** to commit the selection and close the **Add or Remove Snap-ins** dialog.
9. To view the properties of the certificate, expand **Certificates**, expand **Personal**, and select **Certificates**. Select the certificate to view, right-click on

the certificate and select **Open**.

10. In the **Certificate** view, select **Details**. From here, you can select the certificate subject name by selecting **Subject** and the assigned subject name and associated properties are displayed.
11. To view the assigned subject alternative names, select **Subject Alternative Name**. All assigned subject alternative names are displayed. The subject alternative names that are found in the property are of type **DNS Name** by default. You should see the following members (all of which should be fully qualified domain names as represented in DNS host (A or, if IPv6 AAAA) records:
    - Pool name for this pool, or the single server name if this is not a pool
    - Server name that the certificate is assigned to
    - Simple URL records, typically meet and dialin
    - Web services internal and Web services external names (for example, webpool01.contoso.net, webpool01.contoso.com), based on choices made in Topology Builder and over-ridden web services selections.
    - If already assigned, the lyncdiscover.<sipdomain> and lyncdiscoverinternal.<sipdomain> records.

    The last item is what you are most interested in – if there is a lyncdiscover and lyncdiscoverinternal SAN entry.

    Once you have this information, you can close the certificate view and the MMC.
12. If an Autodiscover Service subject alternative name is missing, and you are using a single Default certificate for the Default, WebServicesInternal and WebServiceExternal types, do the following:
    - At the Lync Server Management Shell command line prompt, type:

      ```
      Request-CsCertificate -New -Type Default,WebServicesInterna
      ```

      If you have many SIP domains, you cannot use the new AllSipDomain parameter. Instead, you must use DomainName parameter. When you use the DomainName parameter, you must define the FQDN for the lyncdiscoverinternal and lyncdiscover records. For example:

      ```
      Request-CsCertificate -New -Type Default,WebServicesInterna
      ```

    - To assign the certificate, type the following:

      ```
      Set-CsCertificate -Type Default,WebServicesInternal,WebServi
      ```

      Where “Thumbprint” is the thumbprint displayed for the newly issued certificate.

13. For a missing internal Autodiscover subject alternative names when using separate certificates for Default, WebServicesInternal, and WebServicesExternal, do the following:
    - At the Lync Server Management Shell command line prompt, type:

      ```
      Request-CsCertificate -New -Type WebServicesInternal -Ca dc\
      ```

      If you have many SIP domains, you cannot use the new AllSipDomain parameter. Instead, you must use DomainName parameter. When you use the DomainName parameter, you must use an appropriate prefix for the SIP domain FQDN. For example:

      ```
      Request-CsCertificate -New -Type WebServicesInternal -Ca dc\
      ```

    - For a missing external Autodiscover subject alternative name, at the command line, type:

      ```
      Request-CsCertificate -New -Type WebServicesExternal -Ca dc\
      ```

      If you have many SIP domains, you cannot use the new AllSipDomain parameter. Instead, you must use DomainName parameter. When you use the DomainName parameter, you must use an appropriate prefix for the SIP domain FQDN. For example:

```
Request-CsCertificate -New -Type WebServicesExternal -Ca dc\
```

- To assign the individual certificate types, type the following:

```
Set-CsCertificate -Type Default -Thumbprint <Certificate Thu
Set-CsCertificate -Type WebServicesInternal -Thumbprint <Cer
Set-CsCertificate -Type WebServicesExternal -Thumbprint <Cer
```

Where “Thumbprint” is the thumbprint displayed for the newly issued individual certificates.

1.4.15.3 Configuring the Reverse Proxy for Mobility

Configuring the Reverse Proxy for Mobility

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2012-09-08*

If you want to use automatic discovery for mobile device clients, you need to modify an existing or create a new web publishing rule for the reverse proxy whether or not you update the subject alternative name lists on the reverse proxy certificates.

If you decide to use HTTPS for initial Lync Server 2013 Autodiscover Service requests and update the subject alternative names lists on the reverse proxy certificates, you need to assign the updated public certificate to the Secure Sockets Layer (SSL) Listener on your reverse proxy. For details about the required subject alternative name entries, see Technical Requirements for Mobility. You then need to modify the existing listener for the external web services or create a new web publishing rule for the external Autodiscover Service URL. If you do not already have a web publishing rule for the external Lync Server 2013 Web Services URL for your Front End pool, you also need to publish a rule for that.

Note:

The reverse proxy publishing rule and listener can service both the external web services and the Autodiscover Service, as long as the certificate assigned to the listener contains the necessary subject name and subject alternative names for both. For details on the default configuration of the web listener and publishing rule, see Setting Up Reverse Proxy Servers for more details.

If you decide to use HTTP for initial Autodiscover Service requests so that you do not need to update subject alternative names for the reverse proxy, you need to create or modify a web publishing rule for port 80.

The procedures in this section describe how to create or modify the web publishing rules in Microsoft Forefront Threat Management Gateway 2010 for automatic discovery.

Note:

These procedures assume that you have installed the Standard Edition of Forefront Threat Management Gateway (TMG) 2010. If you are using another reverse proxy, the procedures are similar, but will need to be mapped to the documentation for the third-party product.

To create a web publishing rule for the external Autodiscover URL

1. Click **Start**, point to **Programs**, point to **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, point to **New**, and then click **Web Site Publishing Rule**.

3. On the **Welcome to the New Web Publishing Rule** page, type a display name for the new publishing rule (for example, LyncDiscoveryURL).
4. On the **Select Rule Action** page, select **Allow**.
5. On the **Publishing Type** page, select **Publish a single Web site or load balancer**.
6. On the **Server Connection Security** page, select **Use SSL to connect to the published Web server or server farm**.
7. On the **Internal Publishing Details** page, in **Internal Site name**, type the fully qualified domain name (FQDN) of your Director pool (for example, lyncdir01.contoso.local). If you are creating a rule for the external Web Services URL on the Front End pool, type the FQDN of the Front End pool (for example, lyncpool01.contoso.local).
8. On the **Internal Publishing Details** page, in **Path (optional)**, type **/*** as the path of the folder to be published, and then select **Forward the original host header**.
9. On the **Public Name Details** page, do the following:
   - Under **Accept Requests for**, select **This domain name**.
   - In **Public Name**, type **lyncdiscover.**<*sipdomain*> (the external Autodiscover Service URL). If you are creating a rule for the external Web Services URL on the Front End pool, type the FQDN for the external Web Services on your Front End pool (for example, lyncwebextpool01.contoso.com).
   - In **Path**, type **/***.
10. On **Select Web Listener** page, in **Web Listener**, select your existing SSL Listener with the updated public certificate.
11. On the **Authentication Delegation** page, select **No delegation, but client may authenticate directly**.
12. On the **User Set** page, select **All Users**.
13. On the **Completing the New Web Publishing Rule Wizard** page, verify that the web publishing rule settings are correct, and then click **Finish**.
14. In the Forefront TMG list of web publishing rules, double-click the new rule you just added to open **Properties**.
15. On the **To** tab, do the following:
   - Select **Forward the original host header instead of the actual one**.
   - Select **Requests appear to come from the Forefront TMG computer**.
16. On the **Bridging** tab, configure the following:
   - Select **Web server**.
   - Select **Redirect requests to HTTP port**, and type **8080** for the port number.
   - Select **Redirect requests to SSL port**, and type **4443** for the port number.
17. Click **OK**.
18. Click **Apply** in the details pane to save the changes and update the configuration.
19. Click **Test Rule** to verify that your new rule is set up correctly.

⊟To modify an existing web publishing rule to add the external Autodiscover SAN and URL

1. Click **Start**, point to **Programs**, point to **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.

   Important:

   You will repeat the modification for each publishing rule and listener that you have. Typically, this will be one rule and listener for the Front End pools and one for the optional Directors or Director pools, if you have deployed them.

2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, click the applicable rule. On the **Tasks** tab, click **Edit Selected rule**.
3. On the **Public Name** tab, in **This rule applies to**, select **Requests for the following Web sites**.
4. Click **Add**, type the name of the new Autodiscover site (for example, "lyncdiscover.contoso.com"), and then click **OK**.

5. On the **Listener** tab, click **Select Certificate** and assign the new certificate with the added Autodiscover SAN entries. Close the Listener and Web Publishing properties.
6. Click **Apply** in the details pane to save the changes and update the configuration.
7. Click **Test Rule** to verify that your new rule is set up correctly.

⊟To create a web publishing rule for port 80

1. Click **Start**, point to **Programs**, point to **Microsoft Forefront TMG**, and then click **Forefront TMG Management**.
2. In the left pane, expand **ServerName**, right-click **Firewall Policy**, point to **New**, and then click **Web Site Publishing Rule**.
3. On the **Welcome to the New Web Publishing Rule** page, type a display name for the new publishing rule (for example, Lync Autodiscover (HTTP)).
4. On the **Select Rule Action** page, select **Allow**.
5. On the **Publishing Type** page, select **Publish a single Web site or load balancer**.
6. On the **Server Connection Security** page, select **Use non-secured connections to connect to the published Web server or server farm**.
7. On the **Internal Publishing Details** page, in **Internal Site name**, type the internal Web Services FQDN for your Front End pool (for example, lyncpool01.contoso.local).
8. On the **Internal Publishing Details** page, in **Path (optional)**, type **/*** as the path of the folder to be published, and then select **Forward the original host header instead of the one specified in the Internal site name field**.
9. On the **Public Name Details** page, do the following:
   - Under **Accept Requests for**, select **This domain name**.
   - In **Public Name**, type **lyncdiscover.**<*sipdomain*> (the external Autodiscover Service URL).
   - In **Path**, type **/***.
10. On **Select Web Listener** page, in **Web Listener**, select a Web Listener or use the New Web Listener Definition Wizard to create a new one.
11. On the **Authentication Delegation** page, select **No delegation, and client cannot authenticate directly**.
12. On the **User Set** page, select **All Users**.
13. On the **Completing the New Web Publishing Rule Wizard** page, verify that the web publishing rule settings are correct, and then click **Finish**.
14. In the Forefront TMG list of web publishing rules, double-click the new rule you just added to open **Properties**.
15. On the **Bridging** tab, configure the following:
    - Select **Web server**.
    - Select **Redirect requests to HTTP port**, and type **8080** for the port number.
    - Verify that **Redirect requests to SSL port** is not selected.
16. Click **OK**.
17. Click **Apply** in the details pane to save the changes and update the configuration.
18. Click **Test Rule** to verify that your new rule is set up correctly.
19. Verify that the external Autodiscover Service URL is not defined on any other web publishing rule.

Concepts

Setting Up Reverse Proxy Servers
Technical Requirements for Mobility

1.4.15.4 Configuring Autodiscover for Mobility with Hybrid Deployments

Configuring Autodiscover for Mobility with Hybrid Deployments

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2013-01-24*

Hybrid Deployments are configurations that use both the Microsoft Lync Online cloud service and the on premises deployment. In this type of configuration, the Autodiscover service must be able to locate where the user is actually located. That is to say, Autodiscover aids in finding the user account and where the server that hosts the user's account is, regardless if it is in the on premises deployment or in the Lync Online deployment.

For example, if a user's account is hosted on a server in Lync Online, the attempt to locate the user will happen as follows, in a process known as *discoverability*:

- User initiates a connection attempt to the on premises deployment, **contoso.com**.
- The attempt is sent to lyncdiscover.contoso.com, the DNS name associated with the Autodiscover service.
- Autodiscover refers to the assumed registrar pool at the contoso.com on premises deployment and is given information on the user's actual home server hosted in Lync Online. Autodiscover then sends the user a referral to the **lync.com** online Autodiscover service.
- The user initiates a connection attempt to the lync.com online Autodiscover service and is able to locate the user's account and the user's home server.

To enable mobile clients to discover the deployment where the user home server is located, you must configure the Autodiscover service with a new uniform resource locator (URL). Do the following to configure the Autodiscover service.

⊟Configuring Autodiscover for Hybrid Deployments

1. You use Get-CsHostingProvider to retrieve the value of the attribute ProxyFQDN.
2. From the Lync Server Management Shell, type

   ```
   Set-CsHostingProvider -Identity [identity] -AutodiscoverUrl https://we
   ```

   Where [identity] is replaced with the domain name of the shared SIP address space.

Other Resources

Get-CsHostingProvider
Set-CsHostingProvider

1.4.15.5 Verifying Your Mobility Deployment

Verifying Your Mobility Deployment

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2013-02-12*

```
Some information in this topic pertains to Cumulative Updates for Lync Server 201
```

After you deploy the Lync Server Mobility Service and Lync Server Autodiscover Service, run a test transaction to verify that your deployment works correctly. You can run **Test-CsUcwaConference** to test the ability of two users who are using Lync 2013 Mobile clients to create, join and communicate in a conference. To use this test transaction, you need two actual users or test users, and their full credentials.

You use **Test-CsMcxP2PIM** to test sending an instant message between two users who are using Lync 2010 Mobile. Similar to **Test-CsUcwaConference**, you use two actual users or two predefined test users.

⊟To test conferencing for Lync 2013 Mobile clients

1. Log on as a member of the CsAdministrator role on any computer where Lync Server Management Shell and Ocscore are installed.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. At the command line, type:

   ```
   Test-CsUcwaConference -TargetFqdn <FQDN of Front End pool> -Authentica
   ```

   You can set credentials in a script and pass them to the test cmdlet. For example:

   ```
   $passwd1 = ConvertTo-SecureString "Password01" -AsPlainText -Force
   $passwd2 = ConvertTo-SecureString "Password02" -AsPlainText -Force
   $testuser1 = New-Object Management.Automation.PSCredential("contoso\Us
   $testuser2 = New-Object Management.Automation.PSCredential("contoso\Us
   Test-CsUcwaConference -TargetFqdn pool01.contoso.com -Authentication N
   ```

⊟To test person-to-person instant messaging (IM) for Lync 2010 Mobile

1. Log on as a member of the CsAdministrator role on any computer where Lync Server Management Shell and Ocscore are installed.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. At the command line, type:

   ```
   Test-CsMcxP2PIM -TargetFqdn <FQDN of Front End pool> -Authentication <
   ```

   You can set credentials in a script and pass them to the test cmdlet. For example:

   ```
   $passwd1 = ConvertTo-SecureString "Password01" -AsPlainText -Force
   $passwd2 = ConvertTo-SecureString "Password02" -AsPlainText -Force
   $tuc1 = New-Object Management.Automation.PSCredential("contoso\UserNam
   $tuc2 = New-Object Management.Automation.PSCredential("contoso\UserNam
   Test-CsMcxP2PIM -TargetFqdn pool01.contoso.com -Authentication Negotia
   ```

Other Resources

Test-CsMcxP2PIM
Test-CsUcwaConference

1.4.15.6 Configuring for Push Notifications

Configuring for Push Notifications

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2013-02-12*

Push notifications, in the form of badges, icons, or alerts, can be sent to a mobile device even when the mobile application is inactive. Push notifications notify a user of events such as a new or missed IM invitation and voice mail. The Lync Server 2013 Mobility Service sends the notifications to the cloud-based Lync Server Push Notification Service, which then sends the notifications to the Apple Push Notification Service (APNS) (for an Apple device running the Lync 2010 Mobile client) or the Microsoft Push Notification Service (MPNS) (for a Windows Phone device running the Lync 2010 Mobile or the Lync 2013 Mobile client).

Important:

If you use Windows Phone with Lync 2010 Mobile or Lync 2013 Mobile client, push notification is an important consideration.
If you use Lync 2010 Mobile on Apple devices, push notification is an important consideration.
If you use Lync 2013 Mobile on Apple devices, you no longer need push notification.

Configure your topology to support push notifications by doing the following:

- If your environment has a Lync Server 2010 or Lync Server 2013 Edge Server, you need to add a new hosting provider, Microsoft Lync Online, and then set up hosting provider federation between your organization and Lync Online.
- If your environment has a Office Communications Server 2007 R2 Edge Server, you need to set up direct SIP federation with push.lync.com.

  Note:

  Push.lync.com is a Microsoft Office 365 domain for Push Notification Service.
- To enable push notifications, you need to run the **Set-CsPushNotificationConfiguration** cmdlet. By default, push notifications are turned off.
- Test the federation configuration and push notifications.

To configure for push notifications with Lync Server 2013 or Lync Server 2010 Edge Server

1. Log on to a computer where Lync Server Management Shell and Ocscore are installed as a member of the RtcUniversalServerAdmins group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Add a Lync Server online hosting provider. At the command line, type:

   ```
   New-CsHostingProvider -Identity <unique identifier for Lync Online hos
   ```

   For example:

   ```
   New-CsHostingProvider -Identity "LyncOnline" -Enabled $True -ProxyFqdn
   ```

   Note:

   You cannot have more than one federation relationship with a single hosting provider. That is, if you have already set up a hosting provider that has a federation relationship with sipfed.online.lync.com, do not add another hosting provider for it, even if the identity of the hosting provider is something other than LyncOnline.
4. Set up hosting provider federation between your organization and the Push Notification Service at Lync Online. At the command line, type:

   ```
   New-CsAllowedDomain -Identity "push.lync.com"
   ```

To configure for push notifications with Office Communications Server 2007 R2 Edge Server

1. Log on to the Edge Server as a member of the RtcUniversalServerAdmins group.

2. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Computer Management**.
3. In the console tree, expand **Services and Applications**, right-click **Microsoft Office Communications Server 2007 R2**, and then click **Properties**.
4. On the **Allow** tab, click **Add**.
5. In the **Add Federated Partner** dialog box, do the following:
   - In **Federated partner domain name**, type **push.lync.com**.
   - In **Federated partner Access Edge Server**, type **sipfed.online.lync.com**.
   - Click **OK**.

To enable push notifications

1. Log on to a computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Enable push notifications. At the command line, type:

```
Set-CsPushNotificationConfiguration -EnableApplePushNotificationServic
```

4. Enable federation. At the command line, type:

```
Set-CsAccessEdgeConfiguration -AllowFederatedUsers $True
```

To test federation and push notifications

1. Log on to a computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Test the federation configuration. At the command line, type:

```
Test-CsFederatedPartner -TargetFqdn <FQDN of Access Edge server used f
```

   For example:

```
Test-CsFederatedPartner -TargetFqdn accessproxy.contoso.com -Domain pu
```

4. Test push notifications. At the command line, type:

```
Test-CsMcxPushNotification -AccessEdgeFqdn <Access Edge service FQDN>
```

   For example:

```
Test-CsMcxPushNotification -AccessEdgeFqdn accessproxy.contoso.com
```

Other Resources

Test-CsFederatedPartner
Test-CsMcxPushNotification

1.4.15.7 Configuring Mobility Policy

Configuring Mobility Policy

See Also

Deployment > Deploying External User Access > Deploying Mobility >

Topic Last Modified: *2013-02-13*

```
Some information in this topic pertains to Cumulative Updates for Lync Server 201
```

Lync Server 2013 provides mobility policies that determine who can use mobility features, Call via Work, voice over IP (VoIP) or video, and whether WiFi will be required for either VoIP or video. The Call via Work feature enables a mobile user to make and receive calls on a mobile phone by using a work phone number instead of the mobile phone number.

This feature prevents the called party from seeing the caller's mobile phone number and enables a user to avoid outbound calling charges. Configuring VoIP and video makes it possible for users to receive and make VoIP calls and video. Settings for WiFi usage define if a user's device will be required to use a WiFi network over a cellular data network.

By default, mobility, Call via Work, and the VoIP and video features are enabled. The settings to require WiFi for VoIp and video are disabled. Administrators can determine who has access to these features by running a cmdlet. You can turn options off globally, by site, or by user.

To be able to use mobility features and Call via Work, users must meet the following prerequisites:

- Users must be enabled for Lync Server 2013.
- Users must be enabled for Enterprise Voice.
- Users must be assigned a mobility policy that has the **EnableMobility** option set to True.

For users to be able to use Call via Work, they must meet the following two additional prerequisites:

- Users must be assigned a voice policy that has the **Enable simultaneous ringing of phones** option selected.
- Users must be assigned a mobility policy that has the **EnableOutsideVoice** option set to True.

Note:

Users who are not enabled for Enterprise Voice can use their mobile devices to make Lync to Lync Voice over IP (VoIP) calls, or can join conferences by using the Click to Join link on their mobile devices, if you assign those users the appropriate options for voice policy. For details, see Defining Your Mobility Requirements.

For details about enabling users for Lync Server 2013, see Disable or Re-Enable User Account for Lync Server. For details about enabling users for Enterprise Voice, see Enable Users for Enterprise Voice. For details about setting voice policy options, see Modify a Voice Policy and Configure PSTN Usage Records.

To modify global mobility policy

1. Log on to any computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Turn off access to mobility and Call via Work globally. At the command line, type:

```
Set-CsMobilityPolicy -EnableMobility $False -EnableOutsideVoice $False
```

Note:

You can turn off Call via Work without turning off access to mobility. However, you cannot turn off mobility without also turning off Call via Work.

To modify mobility policy by site

1. Log on to any computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Create a site-level policy, and turn off VoIP and video, and enable Require

WiFi for IP Audio and for IP Video by site. At the command line, type:

```
New-CsMobilityPolicy -Identity site:<site identifier> -EnableIPAudioVi
```

To modify mobility policy by user

1. Log on to any computer where Lync Server Management Shell and Ocscore are installed as a member of the CsAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Create user level mobility policies and turn off mobility and Call via Work by user. At the command line, type:

```
New-CsMobilityPolicy -Identity <policy name> -EnableMobility $False -E
Grant-CsMobilityPolicy -Identity <user identifier> -PolicyName <policy
```

You can turn off Call via Work without turning off access to mobility. However, you cannot turn off mobility without also turning off Call via Work.

For example:

```
New-CsMobilityPolicy "tag:disableOutsideVoice" -EnableOutsideVoice $Fa
Grant-CsMobilityPolicy -Identity -MobileUser1@contoso.com -PolicyName
```

Tasks

Disable or Re-Enable User Account for Lync Server
Enable Users for Enterprise Voice
Modify a Voice Policy and Configure PSTN Usage Records

Concepts

Defining Your Mobility Requirements

Other Resources

New-CsMobilityPolicy
Set-CsMobilityPolicy
Get-CsMobilityPolicy
Grant-CsMobilityPolicy
Remove-CsMobilityPolicy

1.4.16 Health Configuration in Lync Server 2013

Health Configuration in Lync Server 2013

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2012-10-22*

Between various websites, Microsoft Knowledge Base articles, and Lync Server Resource Kit tools, administrators who encounter problems when running Lync Server are never far from a way to solve those problems.

Obviously there is no way to guarantee that you will never encounter problems with Lync Server 2013 because Lync Server can be affected by many things—like network crashes and hardware failures—that the product itself cannot control. By implementing health monitoring, administrators can identify potential problems before they turn into actual problems. For example, administrators can use Lync Server monitoring to identify trends and tendencies. For example, a steady increase in the number of audio/video conferences might suggest a need to add capacity before the system becomes overloaded.

In a similar fashion, administrators can use System Center Operations Manager to do such things as issue real-time alerts when specified events occur, and to run synthetic transactions that proactively test the system. Synthetic transactions are used in Lync

Server to verify that users are able to successfully complete common tasks such as logging on to the system, exchanging instant messages, or making calls to a phone located on the public switched telephone network (PSTN). For example, periodically running these tests can alert you to potential problems with users logging on to Lync Server, and give you a chance to correct the problem before your support team is flooded with calls from users unable to make a connection. By using System Center Operations Manager to run these synthetic transactions, administrators can routinely monitor their deployment of Lync Server continuously for 24 hours every day without having to do much of anything beyond responding to any alerts that might be issued.

> **Note:**
>
> For Lync Server 2013, the Management Pack for System Center Operations Manager is also able to detect "external" issues that can adversely affect Lync Server. For example, administrators can be notified if Internet Information Services (IIS) goes offline, system resources on a Lync Server computer fall below a specified amount, or a Lync Server computer experiences a hardware failure.

Health configuration in Lync Server 2013 is built around System Center Operations Manager and the use of Lync Server Management Packs. These Management Packs include a number of new features and enhancements, including:

- **Scenario availability from any location.** The Lync Server 2010 Management Pack introduced the concept of monitoring end user scenario availability with synthetic transactions. In Lync Server 2013, these agents have more synthetic transactions and can be run from a variety of locations inside the enterprise, from remote geographic locations outside of the enterprise, against branch office appliances and against Lync Server 2010 deployments to add coverage to legacy Edge deployments.
- **Synthetic transaction logs.** When a synthetic transaction fails, administrators have access to HTML logs to help determine what failed. This includes understanding which action failed, the latency of each action, the command-line used to run the test, and the error that was encountered.
- **Increased call reliability coverage.** The Lync Server 2010 Management Pack introduced call reliability alerting to detect severe connectivity issues that affect the audio calls of end users. The Lync Server 2013 Management Packs add coverage for peer-to-peer instant messaging (IM) and other basic conferencing features to maximize coverage while reducing noise.
- **Dependency monitoring.** Lync Server scenarios can fail due to a variety of external factors such as IIS being offline, limited CPU and memory resources, and disk issues. The new management packs check several critical dependencies to ensure administrators are aware of their impact.
- **Enhanced reporting.** A set of reports to help administrators estimate scenario availability, plan for capacity, and see which components are experiencing the most issues.

The Management Packs also include a variety of features to help detect and diagnose provide real-time visibility into the health your Lync Server deployment. These features are listed in the following table.

Management Pack Features

Feature	Description
Synthetic Transactions	Windows PowerShell cmdlets that can be run from various locations to ensure that end user scenarios such as sign-in, presence, IM, and conferencing are readily available to end users.
Call Reliability Alerts	Database queries for Call Detail Records (CDR). These records are written by Front

	End Servers to reflect whether end users were able to connect to a call or why a call was terminated. These queries result in alerts that indicate when a wide range of end users are experiencing connectivity issues for peer-to-peer calls or basic conferencing functionality.
Media Quality Alerts	Database queries that look at Quality of Experience (QoE) reports published by clients at the end of each call. These queries result in alerts that pinpoint scenarios where users are likely to be experiencing poor media quality during calls and conferences. The data is built upon key metrics such as packet latency and loss, metrics that are known to directly contribute to call quality.
Component Health	Individual server components raise alerts by using event logs and performance counters. These alerts indicate failure conditions that can severely impact one or more end user scenarios. These alerts can also indicate a variety of other failure conditions, including services not running, high failure rates, high message latency, or connectivity issues.
Dependency Health	Failures can occur for a variety of external reasons. The management packs now monitor and collect data for some of the critical external dependencies that might indicate severe issues, including IIS availability, CPU and memory usage of servers and processes, and disk metrics.

The alerts issued by the system have been classified into three general categories:

- **High-priority Alerts.** These alerts indicate conditions that will cause service outages for large groups of users. For example, a component failure on a single machine is not a high-priority alert because Lync Server 2013 has built-in high availability features. Instead, high-priority alerts represent problems serious enough "to wake up administrators at night." Outages detected by synthetic transactions and offline services (for example, audio/video conferencing) qualify as high-priority alerts.
- **Medium-priority alerts.**. These alerts indicate conditions that affect a subset of users or indicate call quality degradation. That includes problems such as component failures, latency in call establishment, or degraded audio quality in call. Alerts in this category are stateful and indicate the current status of the issue. For example, suppose your call establishment times exceed the alert threshold. If call establishment times return to normal, these alerts will be auto-resolved in System Center Operations Manager. The expectation for these alerts is that an administrator will look at them on the same business day.
- **Other alerts.** These are alerts from components that might affect a specific user or subset of users. For example, perhaps the Address Book service could not parse the Active Directory entry of a given user. The expectation for these alerts is that administrators will get to them when they have time available.

In This Section

- Configuring Lync Server to Work With System Center Operations Manager
- Using Rich Logging for Synthetic Transactions
- Using Microsoft SQL Server 2008 R2 as Your System Center Operations Manager Database

1.4.16.1 Configuring Lync Server to Work With System Center Operations Manager

Configuring Lync Server to Work With System Center Operations Manager

Microsoft Lync Server 2013 > Deployment > Health Configuration in Lync Server 2013 >

Topic Last Modified: *2012-10-22*

In order to configure your Microsoft Lync Server 2013 infrastructure to work with System Center Operations Manager you must do three things:

- Identify and configure your primary System Center Operations Manager management server. Configuring the management server includes installing System Center Operations Manager 2012 or System Center Operations Manager 2007 R2, as well as setting up a back-end database using SQL Server. The actual version of SQL Server that you need to be use depends on the version of System Center Operations Manager you are using. For details, see Configuring the Primary Management Server.
- Identify and configure the Lync Server computers that you want to monitor. To monitor a Lync Server computer by using System Center Operations Manager you must install the System Center Operations Manager agent files, and configure each server to act as a proxy.
- Identify and configure the computers that you want to act as Lync Server *watcher nodes*. Watcher nodes are computers that periodically run Lync Server synthetic transactions, which are Windows PowerShell cmdlets that verify that key Lync Server components, such as the ability to log on to the system or the ability to exchange instant messages are working as expected.

The topics in this section contain instructions for carrying out each of these tasks.

In This Section

- Configuring the Primary Management Server
- Installing the Lync Server 2013 Management Packs
- Configuring the Lync Server Computers That Will Be Monitored
- Installing and Configuring Watcher Nodes

1.4.16.1.1 Configuring the Primary Management Server

Configuring the Primary Management Server

Deployment > Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager >

Topic Last Modified: *2012-10-22*

In order to take full advantage of the new health monitoring capabilities included in Microsoft Lync Server 2013 administrators must first designate a computer to act as your primary management server; on that computer you must then install System Center Operations Manager 2007 R2 or System Center Operations Manager 2012. In addition, you must install a supported version of SQL Server to function as your Operations Manager back-end database. If you are using System Center Operations Manager 2012 you can use any of the following versions of SQL Server as your back-end database:

- SQL Server 2008 R2 Service Pack 1
- SQL Server 2008 R2 Service Pack 2

If you are using System Center Operations Manager 2007 R2 it is recommended that you install either SQL Server 2005 Service Pack 4 or SQL Server 2008 Service Pack 3. You can also use SQL Server 2008 R2 as the backend database for System Center Operations Manager 2007 R2. See Appendix 1 of this documentation for more information on configuring SQL Server 2008 R2 to work with System Center Operations Manager 2007 R2.

When you install System Center Operations Manager 2012 or System Center Operations Manager 2007 R2 you need to install all the components of that product, including:

- Operational database
- Server
- Console
- Windows PowerShell cmdlets
- Web console
- Reporting
- Data warehouse

These components and their installation will not be discussed in detail in this document. For details about System Center Operations Manager 2007 R2, see the Operations Manager 2007 R2 documentation at http://go.microsoft.com/fwlink/p/?linkid=257526 and the System Center Operations Manager 2012 documentation at http://go.microsoft.com/fwlink/p/?linkid=257527. You should follow those instructions if you are going to use SQL Server 2005 or SQL Server 2008 Service Pack 1 as your back-end database.

If you are using System Center Operations Manager 2012 then you can use SQL Server 2012 as your back-end database. For details about SQL Server 2012, see Books Online for SQL Server 2012 at http://go.microsoft.com/fwlink/p/?LinkId=257528.

Keep in mind that you can only have a single Root Management Server per Lync Server deployment. Also, while you can use either System Center Operations Manager 2012 or System Center Operations Manager 2007 R2, you cannot run the two applications simultaneously—you must choose one or the other. For example, if you are running System Center Operations Manager 2012 then all your System Center agents must also be runningSystem Center Operations Manager 2012. You cannot have some agents running System Center Operations Manager 2012 and other agents running System Center Operations Manager 2007 R2.

1.4.16.1.2 Installing the Lync Server 2013 Management Packs

Installing the Lync Server 2013 Management Packs

Deployment > Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager >

Topic Last Modified: *2012-10-22*

By itself, System Center Operations Manager has the ability to monitor only a small portion of the Windows operating system. However, you can extend the capabilities of System Center Operations Manager by installing management packs, software that dictates which items System Center Operations Manager can monitor, including how those items should be monitored and how alerts should be triggered and reported. Microsoft Lync Server 2013 includes two System Center Operations Manager management packs that provide the following capabilities:

- The Component and User Management Pack (Microsoft.LS.2013.Monitoring.ComponentAndUser.mp) tracks Lync Server issues recorded in event logs, registered by performance counters, or logged in the call detail records (CDR) or the Quality of Experience (QoE) databases. For critical problems, System Center Operations Manager can be configured to immediately notify administrators via email, instant message, or Short Message Service (SMS) messaging. SMS is the technology used to send text messages from one mobile device to another.

  Note:

  For more information on configuring Operations Manager notification, see Configuring Notification in the TechNet Library at http://go.microsoft.com/fwlink/p/?linkid=268785.

- The Active Monitoring Pack (Microsoft.LS.2013.Monitoring.ActiveMonitoring.mp) proactively tests key Lync Server components such as logging on to the system, exchanging instant messages, or making calls to a phone located on the public switched telephone network (PSTN). These tests are conducted using the Lync Server synthetic transaction cmdlets. For example, the **Test-CsIM** cmdlet is used to simulate an instant messaging conversation between a pair of test users. If this simulated messaging conversation fails an alert will be generated.

The two management packs included with Lync Server 2013 include a large number of enhancements over the management packs used with Microsoft Lync Server 2010. For example, the Lync Server 2013 Component Management Pack is not limited to monitoring Lync Server itself. In addition to monitoring event logs and performance counters for Lync Server, the Component Management pack can also track the performance of, and issue alerts for, crucial items such as:

- **Internet Information Services (IIS)** Alerts will be issued if Internet Information Services goes offline. This is important, because the Lync Server web services rely on IIS.
- **Process usage** Alerts will be issued if system resources (such as available memory) begin to run low. These alerts will be issued even if Lync Server is not responsible for the high system usage.
- **Computer failure events** Alerts will be issued in case of a hardware or software issue that threatens the viability of a server. For example, Lync Server administrators will be notified if a server appears to be in danger of experiencing a hard disk failure.

The new management packs also feature enhanced reporting. New reports for Lync Server 2013 include:

- **End to End Scenario Availability Report** This report details the availability/uptime for key Lync Server services such as registration or presence.
- **Capacity Report** Using performance counter information, this report shows trends for system components such as memory availability and processor usage.
- **Component Report** This report lists the top alert generators grouped by Lync Server component.

In addition to these predesigned reports, the management packs for Lync Server 2013 automatically report alerts for both Call Reliability (metrics measured by Call Detail Recording) and QoE states (metrics measured by Quality of Experience). If you have enabled Call Detail Recording, you can review Call Reliability alerts by completing the following procedure from the System Center Operations Manager console:

- Expand **Monitoring**, expand **Microsoft Lync Server 2013 Health**, expand **Call**

Reliability and Media Quality, and then click **Call Reliability**.

To view Quality of Experience alerts, complete this procedure from the System Center Operations Manager console:

- Expand **Monitoring**, expand **Microsoft Lync Server 2013 Health**, expand **Call Reliability and Media Quality**, and then expand **Media Quality**.

The management packs for Lync Server 2013 now use machine-level discovery instead of the central discovery mechanism used in Microsoft Lync Server 2010. This means that each System Center agent essentially discovers itself and reports its existence to the Central Management Server. Using machine-level discovery simplifies administration of your System Center infrastructure and also allows different versions of the Lync Server management packs (for example, management packs for Lync Server 2010 and management packs for Lync Server 2013) to coexist.

1.4.16.1.2.1 Using the Lync Server 2010 Management Packs in a Coexistence Scenario

Using the Lync Server 2010 Management Packs in a Coexistence Scenario

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Installing the Lync Server 2013 Management Packs >

Topic Last Modified: *2012-10-22*

Many customers adopt a rollout program inside of their enterprises in which users are progressively migrated from Microsoft Lync Server 2010 to Lync Server 2013. The administrators at these companies will care about monitoring both versions of Lync Server to help ensure that all of their end users are getting the best possible communication experience. For this scenario, the Lync Server 2013 Management Pack supports a side-by-side migration path with the Lync Server 2010 Management Pack.

In the Lync Server 2010, Lync Server computers were discovered through the topology document stored with the Central Management store. In this configuration, a single computer would report the existence of all the other Lync Server computers.

The management packs for Lync Server 2013 now use machine-level discovery instead of the central discovery mechanism that was used in Lync Server 2010. This means that each System Center agent essentially discovers itself and reports its existence to System Center Operations Manager. Using machine-level discovery simplifies administration of your System Center infrastructure and also enables different versions of the Lync Server management packs (for example, management packs for Lync Server 2010 and management packs for Lync Server 2013) to coexist more easily.

To support this migration, you will first need to upgrade your existing Lync Server 2010 monitoring to avoid gaps in coverage. To do this, elect an existing Lync Server 2010 computer to service the Central Discovery script for the Lync Server 2010 before upgrading your Central Management store to Lync Server 2013. This is a four-step process:

1. Upgrade the Lync Server 2010 Management Packs to Cumulative Update 7.
2. Instruct a Lync Server 2010 computer to run the Central Discovery script.
3. Override the Central Discovery Candidate in the Microsoft Lync Server 2010 Management Pack.
4. Verify that the new Central Discovery Candidate has been discovered.

Instructing a Lync Server 2010 Computer

to Run the Central Discovery script

To nominate a non-Central Management store computer (for example, a Lync Server Front End) server to handle central discovery, you will need to create the following registry key on the non-Central Management store server:

HKLM\Software\Microsoft\Real-Time Communications\Health\CentralDiscoveryCandidate

You can create this registry key by completing the following procedure:

1. Click **Start** and then click **Run**.
2. In the **Run** dialog box, type **regedit** and then press ENTER.
3. In Registry Editor, expand **HKEY_LOCAL_MACHINE**, expand **SOFTWARE**, expand **Microsoft**, and then expand **Real-Time Communications**.
4. Right-click **Health**, click **New**, and then click **Key**. If the **Health** key does not exist, then right-click **Real-Time Communications**, point to **New**, and then click **Key**. When the new key is created, type Health, and then press ENTER. After the new key has been created, type **CentralDiscoveryCandidate** and then press ENTER to rename the key.

It may take the computer several hours to pick up this change. To make the change take effect immediately, stop and then restart the Health Agent service. To restart the Health Agent service, complete the following procedure on the Lync Server 2010 computer:

1. Click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. In the console window, type the following command and then press ENTER:

   ```
   Net stop HealthService
   ```

3. You will see a message that states "The System Center Management service is stopping," followed by a second message that tells you that the service has been stopped. After the service has stopped, you can restart it by typing the following command and pressing ENTER:

   ```
   Net start HealthService
   ```

Overriding the Central Discovery Candidate in the Lync Server 2010 Management Pack

After instructing a Lync Server 2010 computer to report on Lync Server 2010 computers, you will need to inform the Lync Server 2010 Management Pack about this change as well. To do this, you will need to create an override in the Management Pack. That can be done by completing the following procedure:

1. In the Operations Manager console, click **Authoring**.
2. On the Authoring tab, expand **Management Pack Objects**, click **Object Discoveries**, and then click **Scope**.
3. In the **Scope Management Pack Objects** dialog box, select the item with the Target **LS Discovery Candidate** and then click **OK**. Note that LS Discovery Candidate will appear only if you have installed the Lync Server 2010 Management Pack.
4. In the Operations Manager console, right-click **LS Discovery Candidate**, point to **Overrides**, point to **Override the Object Discovery**, and then click **For all objects of class: LS Discovery Candidate**.
5. In the **Override Properties** dialog box, select the **Override** check box next to the parameter **Central Discovery WatcherNode Fqdn**. Type the fully qualified domain name of the Lync Server 2010 computer in the **Override Value** and **Effective Value** boxes. Select the **Enforced** check box and click **OK**.

After you have created the override, you need to restart the health service on the Root Management Server. To restart the health service, complete the following procedure on the Root Management Server:

1. Click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. In the console window, type the following command, and then press ENTER:

```
Net stop HealthService
```

3. You will see a message stating that "The System Center Management service is stopping," followed by a second message that tells you that the service has been stopped. After the service has stopped, you can then restart it by typing the following command and pressing ENTER:

```
Net start HealthService
```

Verifying that the New Central Discovery Candidate Was Discovered

The final step before upgrading Central Management store is to make sure that the new central discovery candidate was discovered by the Lync Server 2010 Management Pack. To do this, open the Operations Manager console and then click Monitoring. On the Monitoring tab, expand **Microsoft Lync Server 2010 Health**, expand **Topology Discovery**, and then click **Discovery State View**. Verify that a row in the display has a **Path** that lists the fully qualified domain name of the central discovery candidate. You should also verify that the computer state is reported as **Healthy**.

1.4.16.1.2.2 Importing the Lync Server 2013 Management Packs

Importing the Lync Server 2013 Management Packs

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Installing the Lync Server 2013 Management Packs >

Topic Last Modified: *2012-10-22*

You can extend the capabilities of System Center Operations Manager by installing management packs—software that dictates which items System Center Operations Manager can monitor, and how those items should be monitored and how alerts should be triggered and reported. Lync Server 2013 includes two System Center Operations Manager management packs that provide the following capabilities:

- The Component and User Management Pack (Microsoft.LS.2013.Monitoring.ComponentAndUser.mp) tracks Lync Server issues recorded in event logs, registered by performance counters, or logged in the call detail records (CDR) or the Quality of Experience (QoE) databases. For critical problems, System Center Operations Manager can be configured to immediately notify administrators via email, instant message, or Short Message Service (SMS) messaging. SMS is the technology used to send text messages from one mobile device to another.)

  > **Note:**
  >
  > For details about configuring Operations Manager notification, see the Configuring Notification in the TechNet Library at http://go.microsoft.com/fwlink/p/?LinkId=268785.

- The Active Monitoring Management Pack (Microsoft.LS.2013.Monitoring.ActiveMonitoring.mp) proactively tests key Lync Server components such as signing into to the system, exchanging instant messages, or making calls to a phone located on the public switched telephone network (PSTN). These tests are conducted using the Lync Server synthetic transaction cmdlets. For example, you can use the **Test-CsIM** cmdlet to simulate an instant messaging (IM) conversation between a pair of test users. If this simulated messaging conversation fails an alert is generated.

You need to import the management packs. If you do not import the management packs, you cannot use Operations Manager to monitor Lync Server events or run Lync Server synthetic transactions.

The Component and User Management Pack is only used to monitor Lync Server 2013. If you are in a coexistence scenario, where you have both Lync Server 2013 and Lync Server 2010 installed, you should continue to use the Lync Server 2010 management packs for your Lync Server 2010 computers.

Note:
Management packs for Lync Server 2010 include the Lync Server 2010 Monitoring Management Pack and the Lync Server 2010 Group Chat Monitoring Management Pack.

You can use one of the following tools to import management packs:

- **System Center Operations Manager** With this method, you use the the Operations Manager to add monitoring for Lync Server.
- **Operations Manager Shell** You can use the Operations Manager Shell to import directly or to troubleshoot any issues you encounter when you import management packs by using the System Center Operations Manager console.

Importing the Management Packs by Using System Center Operations Manager

1. Download the files Microsoft.LS.2013.Monitoring.ActiveMonitoring.mp and Microsoft.LS.2013.Monitoring.ComponentAndUser.mp.
2. In System Center Operations Manager, click **Administration**.
3. In the **Administration** pane, right-click **Management Packs**, and then click **Import Management Packs**.
4. In the **Select Management Packs** dialog box, click **Add**, and then click **Add from disk**.
5. In the **Online Catalog Connection** dialog box, click **Cancel** to prevent Operations Manager from going online to see if any dependencies exist for the Lync Server management packs. If you are using System Center Operations Manager 2012, click **No**.
6. In the **Select Management Packs to import** dialog box, locate and select the files **Microsoft.LS.2013.Monitoring.ActiveMonitoring.mp** and **Microsoft.LS.2013.Monitoring.ComponentAndUser.mp** and then click **Open**. To select multiple files in the dialog box, click the first file, hold down the Ctrl key and then click the second file.
7. In the **Select Management Packs** dialog box, click **Install**. If you get an error message and installation fails, that typically means that the management pack files are in a folder protected by the Windows User Account Control. If this occurs, copy the files to a different folder and then restart the import and installation process.
8. In the **Select Management Packs** dialog box, click **Close**. Note that the import and installation process might require several minutes to complete.

Importing Management Packs by Using the Operations Manager Shell

In general it is easier to import the management packs by using the Operations Manager.However, if an error occurs and the import fails, the console does not always provide adequate error reports. By comparison, the Operations Manager Shell, provides detailed information. If you are using Operations Manager and you run into problems importing a management pack, import the pack by using the Operations Manager Shell . The Operations Manager Shell provides more information that might help you determine why the import failed.

If you are using System Center Operations Manager 2007 R2, complete the following procedure:

1. Click **Start**, click **All Programs**, click **System Center Operations Manager 2007 R2**, and then click **Operations Manager Shell**.
2. In the Operations Manager Shell, type the following command at the command prompt, using the actual path to your copy of the file Microsoft.LS.2013.Monitoring.ActiveMonitoring.mp, and then press ENTER:
   ```
   MPImport.exe D:\MP\Microsoft.LS.2013.Monitoring.ActiveMonitoring.mp
   ```
3. After you import the first management pack, repeat the process using the path to your copy of the file Microsoft.LS.2013.Monitoring.ComponentAndUser.mp:
   ```
   MPImport.exe D:\MP\Microsoft.LS.2013.Monitoring.ComponentAndUser.mp
   ```
4. Close the Operations Manager Shell.

If you are using System Center Operations Manager 2012, complete this procedure instead:

1. Click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Operations Manager**, and then click **Operations Manager Shell**.
2. In the Operations Manager Shell, type the following command at the command prompt, using the actual path to your copy of the file Microsoft.LS.2013.Monitoring.ActiveMonitoring.mp, and then press ENTER:
   ```
   Import-SCOMManagementPack -FullName "D:\MP\ Microsoft.LS.2013.Monitori
   ```
3. After you have imported the first management pack, repeat the process using the path to your copy of the file Microsoft.LS.2013.Monitoring.ComponentAndUser.mp:
   ```
   Import-SCOMManagementPack -FullName "D:\MP\ Microsoft.LS.2013.Monitori
   ```

1.4.16.1.3 Configuring the Lync Server Computers That Will Be Monitored

Configuring the Lync Server Computers That Will Be Monitored

Deployment > Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager >

Topic Last Modified: *2012-10-20*

Because Lync Server 2013 does not use the central discovery process used in Microsoft Lync Server 2010, each Lync Server 2013 computer that you want to monitor must be able to self-report its existence to the management server. To make this possible, you must install the Operations Manager agent files on each of the computers to be monitored. After the agent files have been installed, you must configure the computer to act as a System Center proxy. Note that these procedures should be carried out after you have installed and configured Lync Server on these computers.

1.4.16.1.3.1 Installing a Certificate on a Watcher Node Located Outside the Perimeter Network

Installing a Certificate on a Watcher Node Located Outside the Perimeter Network

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Configuring the Lync Server Computers That Will Be Monitored >

Topic Last Modified: *2012-10-22*

System Center Operations Manager agents running in a perimeter network (such as a Lync Server Edge Server), outside of the enterprise (such as an external synthetic transaction watcher node), or across an Active Directory Domain Services (AD DS) trust boundary, might require the configuration of a System Center Operations Manager Gateway Server. This server role allows agents that do not have a trust relationship with the Root Management Server to raise alerts. For details, see "Managing Gateway Servers in Operations Manager 2007" in the System Center Operations Manager TechNet Library at http://go.microsoft.com/fwlink/p/?LinkId=268703.

If you deploy an agent in one of these locations, you will also need to request and configure a certificate that enables the watcher node to send alerts to System Center Operations Manager. To simplify this process, the Operations Manager team has created a set of utilities that enable you to request and install the correct type of certificate on the watcher node computer. For details, and to download these utilities, see the "Obtaining Certificates for Non-Domain Joined Agents Made Easy With Certificate Generation Wizard" blog article at http://go.microsoft.com/fwlink/p/?LinkId=267421.

1.4.16.1.3.2 Installing the Operation Manager Agent Files

Installing the Operation Manager Agent Files

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Configuring the Lync Server Computers That Will Be Monitored >

Topic Last Modified: *2012-10-20*

To install the Operations Manager agent files on the computer, complete the following steps.

1. On your System Center setup media, double-click **SetupOM.exe**.
2. In System Center Operation Manager setup, click **Install Operations Manager Agent**.
3. In System Center Setup wizard, on the **Welcome to the System Center Operations Manager Setup** wizard page, click **Next**.
4. On the **Destination Folder** page, select the folder where the Operations Manager Agent files will be installed, and then click **Next**.
5. On the **Management Group Configuration** page, select **Specify Management Group information**, and then click **Next**.
6. On the **Management Group Configuration** page, type the name of your Operations Manager Management Group in the **Management Group Name** box, and then type the host name of your Operations Manager server (for example, atl-scom-001) in the **Management Server** box. If you have changed the port number used by Operations Manager, then type the new port number in the Management Server Port box. Otherwise, leave the port at the default value of 5723 and click **Next**.
7. On the **Agent Action Account** page, select **Local System**, and then click **Next**.
8. On the **Microsoft Update** page, select **I don't want to use Microsoft Update**,

and then click **Next**.

9. On the **Ready to Install** page, click **Install**.
10. On the **Completing the System Center Operations Manager Setup wizard** page, click **Finish**.
11. Click **Exit**.

If you are using System Center 2007 R2, you can verify that the agent has been created by clicking **Start**, clicking **All Programs**, clicking **System Center Operations Manager 2007 R2**, and then clicking **Operations Manager Shell**. In the Operations Manager Shell, type the following Windows PowerShell command, and then press ENTER:

```
Get-Agent
```

A list of all your Operations Manager agents will appear onscreen.

If you are using System Center 2012, run this command from the Operations 2012 Manager Shell:

```

Get-SCOMAgent
```

1.4.16.1.3.3 Configuring the Lync Server Computer to Participate in System Center Discovery

Configuring the Lync Server Computer to Participate in System Center Discovery

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Configuring the Lync Server Computers That Will Be Monitored >

Topic Last Modified: *2012-10-20*

To make sure that your new Lync Server agent participates in discovery process for System Center Operations Manager, you must complete the following procedure on each computer where the System Center Operations Manager console has been installed:

1. On the **Administration** tab, click **Agent Managed**.
2. Right-click the name of the computer, and then click **Properties**. In the **Properties** dialog box, on the **Security** tab, select **Allow this agent to act as a proxy and discover managed objects on other computers**, and then click **OK**.

After completing step 2, reboot the Health Agent service. (Rebooting the service will “force” discovery of the new machine. If you do not reboot the service, it could take as long as 4 hours before the new machine is discovered by System Center Operations Manager.). After the service has rebooted, verify that no error events are being recorded in the Operations Manager event log on that computer.

1.4.16.1.4 Installing and Configuring Watcher Nodes

Installing and Configuring Watcher Nodes

Deployment > Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager >

Topic Last Modified: *2012-10-22*

Watcher nodes are computers that periodically run Lync Server synthetic transactions. *Synthetic transactions* are Windows PowerShell cmdlets that verify that key end user scenarios—such as the ability to sign in to the system, or the ability to exchange instant messages—are working as expected. For Lync Server 2013, System Center Operations Manager can run the synthetic transactions shown in the following table. There are three different synthetic transaction types shown in the table:

- **Default**. These are the synthetic transactions that a watcher node will run by default. When you create a new watcher node, you have the option of specifying which synthetic transactions that node will run. (That's the purpose of the Tests parameter used by the **New-CsWatcherNodeConfiguration** cmdlet.) If you do not use the Tests parameter when the watcher node is created, it will automatically run all the Default synthetic transactions and will not run any of the Non-default synthetic transactions. That means, for example, that the watcher node will be configured to run the Test-CsAddressBookService test, but will not be configured to run the Test-CsExumConnectivity test.
- **Non-default**. As the name implies, Non-default synthetic transactions are tests that watcher nodes do not run by default. However, the watcher node can be enabled to run any of the Non-default synthetic transactions. You can do this when you create the watcher node (by using the **New-CsWatcherNodeConfiguration** cmdlet), or at any time after that. Many of the Non-default synthetic transactions require extra setup steps. For details, see Special Setup Instructions for Synthetic Transactions.
- **Extended**. Extended tests are a special type of Non-default synthetic transaction. Unlike other synthetic transactions, Extended tests can be run multiple times during each pass. This can be useful when verifying behavior such as multiple public switched telephone network (PSTN) voice routes for a pool. This can be configured simply by adding multiple instances of an Extended test to a watcher node.

For details about the process of adding other synthetic transactions to a watcher node, see Managing Watcher Nodes. You can use the Lync Server Management Shell to remove synthetic transactions from a watcher node.

The synthetic transactions available to watcher nodes include the following:

Cmdlet Name (Test Name)	**Description**	**Synthetic Transaction Type**
Test-CsAddressBookService (ABS)	Confirms that users are able to look up users that aren't in their contact list.	Default
Test-CsAddressBookWebQuery (ABWQ)	Confirms that users are able to look up users that aren't in their contact list via HTTP.	Default
Test-CsIM (IM)	Confirms that users are able to send peer-to-peer instant messages.	Default
Test-CsP2PAV (P2PAV)	Confirms that users are able to place peer-to-peer audio calls (signaling only).	Default
Test-CsPresence (Presence)	Confirms that users are able to view other users' presence.	Default
Test-CsRegistration (Registration)	Confirms that users are able sign in to Lync.	Default
Test-CsAudioConferencingProvider	Not used with the on-premises version of Lync	Extended

(ACP)	Server 2013	
Test-CsPstnPeerToPeerCall (PSTN)	Confirms that users are able to place and receive calls with people outside of the enterprise (PSTN numbers).	Non-default, Extended
Test-CsAVConference (AvConference)	Confirms that users are able to create and participate in an audio/video conference.	Default
Test-CsAVEdgeConnectivity (AVEdgeConnectivity)	Confirms that the A/V Edge servers are able to accept connections for peer-to-peer calls and conference calls.	Non-default
Test-CsDataConference (DataConference)	Confirms that users can participate in a data collaboration conference, an online meeting that includes activities such as whiteboards and polls.	Non-default
Test-CsExumConnectivity (ExumConnectivity)	Confirms that a user can connect to Exchange Unified Messaging (UM).	Non-default
Test-CsGroupIM (GroupIM)	Confirms that users are able to send instant messages in conferences and participate in instant message conversations with three or more people.	Default
Test-CsGroupIM – TestJoinLauncher (JoinLauncher)	Confirms that users are able to create and join scheduled meetings via a web address link.	Non-default
Test-CsMCXP2PIM (MCXP2PIM)	Confirms that mobile device users are able to register and send instant messages.	Non-default
Test-CsPersistentChatMessage (PersistentChatMessage)	Confirms that users can exchange messages by using the Persistent Chat service.	Non-default
Test-CsUnifiedContactStore (UnifiedContactStore)	Confirms that a user's contacts can be accessed through the unified contact store. The unified contact store provides a way for users to maintain a single set of contacts that can be accessed by using Lync 2013, Outlook, and/or Outlook Web Access.	Non-default
Test-CsXmppIM (XmppIM)	Confirms that an instant message can be sent across the XMPP (Extensible	Non-default

	Messaging and Presence Protocol) gateway.	

You do not need to install watcher nodes in order to use System Center Operations Manager. If you do not install these nodes, you can still get real-time alerts from Lync Server 2013 components when an issue occurs. (The Component and User Management Pack does not use watcher nodes.) However, watcher nodes are required if you want to monitor end-to-end scenarios by using the Active Monitoring Management pack.

Note:

Administrators can also run synthetic transactions manually, without needing to use, or install, Operations Manager. For details about the various Test-Cs cmdlets, see the Lync Server 2013 Cmdlets Index.

Depending on the size of your deployment, synthetic transactions may use a large amount of computer memory and processor time. For this reason, we recommend that you use a dedicated computer as a watcher node. For example, you should not configure a Front End Server to act as a watcher node. Watcher nodes should meet the same basic hardware requirements as any other computer that plays a role in your Lync Server.

Note:

A legacy Microsoft Lync Server 2010 watcher node cannot be collocated on the same machine with a Lync Server 2013 watcher node. This is because the core system files for Lync Server 2010 and Lync Server 2013 cannot be installed on the same computer. However, Lync Server 2013 watcher nodes can simultaneously monitor both Lync Server 2013 and Lync Server 2010. The Default synthetic transactions are supported on both product versions.

Lync Server 2013 watcher nodes may be deployed inside or outside of an enterprise to help verify:

- Connectivity to pools for users inside the enterprise.
- Connectivity through perimeter networks for remote users who work outside the enterprise.
- Connectivity to branch office appliances.
- Connectivity to Lync Server 2010 inside the enterprise and through perimeter networks.

Different authentication options are available for inside and outside of the enterprise to help simplify administration. For details, see Configuring a Watcher Node to Run Synthetic Transactions.

To configure a computer to act as a watcher node, you must complete the following steps after you have installed System Center Operations Manager and imported the Lync Server 2013 management packs.

Before you install the Lync Server 2013 core files and the System Center agent files, you should also make sure that the watcher node computer meets all the prerequisites for installing Lync Server 2013. In addition, the watcher node computer should also have the following items installed:

- The full version of .NET Framework 4.5.
- Windows Identity Foundation.
- Windows PowerShell 3.0.

As soon as all these prerequisites have been met, you can configure the watcher node by:

- Installing the Lync Server 2013 core files on the watcher node computer.
- Installing System Center Operations Manager agent on the watcher node computer.

- Running the Watchernode.msi executable file.
- Using the **CsWatcherNodeConfiguration** cmdlets to configure test users to be employed by the watcher node.

1.4.16.1.4.1 Installing the Lync Server 2013 Core Files and the RTCLocal Database

Installing the Lync Server 2013 Core Files and the RTCLocal Database

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Installing and Configuring Watcher Nodes >

Topic Last Modified: *2012-10-20*

To install the Lync Server 2013 core files on a computer, complete the following procedure. The RTCLocal database is automatically installed when you install the core files. Note that you do not need to install SQL Server on the watcher nodes. Instead, SQL Server Express is automatically installed for you.

To install the Lync Server 2013 core files and the RTCLocal database:

1. On the watcher node computer, click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. In the console window, type the following command and then press ENTER, using the appropriate path to your Lync Server setup files:

   ```
   D:\Setup.exe /BootstrapLocalMgmt
   ```

To verify that the core Lync Server components were successfully installed, click **Start**, click **All Programs**, click **Lync Server 2013**, and then click **Lync Server Management Shell**. In the Lync Server 2013 Management Shell, type the following Windows PowerShell command, and then press ENTER:

```
Get-CsWatcherNodeConfiguration
```

The first time you run this command, you no data is returned because you have not configured any watcher node computers yet. As long as the command runs without returning an error, you can assume that the Lync Server setup completed successfully.

If your watcher node computer is located inside your perimeter network, you can run the following command to verify the installation of Lync Server 2013:

```
Get-CsPinPolicy
```

You will receive information similar to the following, depending on the number of personal identification number (PIN) policies configured for use in your organization:

```
Identity              : Global
Description           :
MinPasswordLength     : 5
PINHistoryCount       : 0
AllowCommonPatterns   : False
PINLifetime           : 0
MaximumLogonAttempts  :
```

If you see information about your PIN policies, it means that you have successfully installed the core components.

1.4.16.1.4.2 Installing the Operation Manager Agent Files on a Watcher Node

Installing the Operation Manager Agent Files on a Watcher Node

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Installing and Configuring Watcher Nodes >

Topic Last Modified: *2012-10-20*

Similar to setting up a Lync Server to report component alerts, a Lync Server 2013 watcher node requires System Center Operations Manager agent files to be installed. This will enable the synthetic transactions to be run and for alerts to be reported to the System Center Operations Manager Root Management Server.

To install the agent files, follow the same procedures listed in the following sections:

1. Installing a Certificate on a Watcher Node Located Outside the Perimeter Network
2. Installing the Operation Manager Agent Files
3. Configuring the Lync Server Computer to Participate in System Center Discovery

1.4.16.1.4.3 Configuring a Watcher Node to Participate in System Center Discovery

Configuring a Watcher Node to Participate in System Center Discovery

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Installing and Configuring Watcher Nodes >

Topic Last Modified: *2012-10-22*

To make sure that your watcher node participates in the discovery process for System Center Operations Manager, you must complete the following procedure on a computer where the System Center Operations Manager console has been installed:

1. On the **Administration** tab, click **Agent Managed**.
2. Right-click the name of the watcher node computer, and then click **Properties**. In the **Properties** dialog box, on the **Security** tab, select **Allow this agent to act as a proxy and discover managed objects on other computers**, and then click **OK**.

After configuring the watcher node to act as a proxy, reboot the watcher node computer. After the computer has rebooted, verify that no error events are being recorded in the Operations Manager event log on that computer. After the computer has been running for 15 minutes or so, use the Operations Manager console to verify that your Lync Server computers are listed under the **Lync** category.

1.4.16.1.4.4 Configuring a Watcher Node to Run Synthetic Transactions

Configuring a Watcher Node to Run Synthetic Transactions

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Installing and Configuring Watcher Nodes >

Topic Last Modified: *2012-10-20*

After the System Center agent files have been installed, you must next configure the watcher node itself. The steps you take to configure a watcher node will vary depending on whether your watcher node computer lies inside your perimeter network or outside your perimeter network.

When you configure a watcher node, you must also choose the type of authentication method to be employed by that node. Lync Server 2013 enables you to choose one of two authentication methods: Trusted Server or Credential Authentication. The differences between these two methods are outlined in the following table:

Configuration	Description	Locations Supported
Trusted Server	Uses a certificate to impersonate an internal server and bypass authentication challenges. This is useful for administrators who would prefer to manage a single certificate instead of many user passwords on each watcher node.	Inside the enterprise. Note that, with this method, the watcher node must be in the same domain as the pools being monitored. If the watcher node and the monitored pools are in different domains, use Credential Authentication instead.
Credential Authentication	Stores user names and passwords securely in Windows Credential Manager on each watcher node. This mode requires more password management, but is the only option for watcher nodes located outside of the enterprise. These watcher nodes cannot be treated as an endpoint trusted for authentication.	Outside the enterprise. Inside the enterprise.

Configuring a Watcher Node to Use Trusted Server Authentication

Configuring Lync Server to Work With System Center Operations Manager > Installing and Configuring Watcher Nodes > Configuring a Watcher Node to Run Synthetic Transactions >

Topic Last Modified: *2012-10-22*

If your watcher node computer lies inside the perimeter network, using Trusted Server authentication can greatly reduce administration taxes to maintaining a single certificate rather than numerous user account passwords.

The first step in configuring Trusted Server authentication is to create a trusted application pool to host the watcher node computer. After the trusted application pool has been created, you must then configure synthetic transactions on that watcher node to run as a trusted application.

> **Note:**
> A trusted application is an application that is given trusted status to run as part of Lync Server 2013, but that is not a built-in part of the product. Trusted status means that the application will not be challenged for authentication each time it runs.

To create a trusted application pool, open the Lync Server 2013 Management Shell and run a command similar to this:

```
New-CsTrustedApplicationPool -Identity atl-watcher-001.litwareinc.com -Registrar
```

> **Note:**
> For details about the parameters used in the preceding command, type the following at the Lync Server Management Shell prompt:
> Get-Help New-CsTrustedApplicationPool -Full | more

After creating the trusted application pool, configure the watcher node computer to run synthetic transactions as a trusted application. This is done by using the **New-CsTrustedApplication** cmdlet and a command similar to this:

```
New-CsTrustedApplication -ApplicationId STWatcherNode -TrustedApplicationPoolFqdn
```

When the preceding command completes and the trusted application has been created, run Enable-CsTopology to make sure that the changes take effect:

```
Enable-CsTopology
```

After running Enable-CsTopology, we recommend that you restart the computer.

To verify that the new trusted application has been created, type the following at the Lync Server Management Shell prompt:

```
Get-CsTrustedApplication -Identity "atl-watcher-001.litwareinc.com/urn:applicatio
```

Configuring a Default Certificate on the Watcher Node

Each watcher node must have a Default certificate assigned by using the Lync Server Deployment Wizard.

To assign a Default certificate

1. Click **Start**, click **All Programs**, click **Lync Server**, and then click **Lync Server Deployment Wizard**.
2. In the Lync Server Deployment Wizard, click **Install or Update Lync Server System** and then click **Run** under the heading **Request, Install, or Assign Certificate**.

   > **Note:**
   > If the **Run** button is disabled, you may need to first click **Run** under **Install Local Configuration Store**.

3. Do one of the following:
   - If you already have a certificate that can be used as the Default certificate, click **Default** in the Certificate wizard and then click **Assign**. Follow the steps in the Certificate Assignment wizard to assign that certificate.
   - If you need to request a certificate for use the Default certificate, click **Request** and then follow the steps in the Certificate Request wizard to request that certificate. If you use the default values for the Web Server certificate, you get a certificate that you can assign as the Default certificate.

Installing and Configuring a Watcher Node

After you have restarted the watcher node computer and configured a certificate, you need to run the file Watchernode.msi. (You must run Watchernode.msi on a computer where both the Operations Manager agent files and the Lync Server 2013 core components are installed.)

To install and configure a watcher node

1. Open the Lync Server Management Shell by clicking **Start**, clicking **All Programs**, clicking **Lync Server**, and then clicking **Lync Server Management Shell**.
2. In the Lync Server Management Shell, type the following command and then press ENTER (specify the actual path to your copy of Watchernode.msi):

```
C:\Tools\Watchernode.msi Authentication=TrustedServer
```

> **Note:**
> You can also run Watchernode.msi from a command window. To open a command window, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**. When the command window opens, type the same preceding command.

Note that the name/value pair in the preceding command Authentication=TrustedServer is case-sensitive. You must type it exactly as shown. The following command fails because it does not use the correct letter casing:

```
C:\Tools\Watchernode.msi authentication=trustedserver
```

You can use TrustedServer mode only with computers that are located within the perimeter network. When a watcher node is running in TrustedServer mode, administrators do not have to maintain test user passwords on the computer.

Configuring a Watcher Node to Use Credential Authentication

Configuring Lync Server to Work With System Center Operations Manager > Installing and Configuring Watcher Nodes > Configuring a Watcher Node to Run Synthetic Transactions >

Topic Last Modified: *2012-10-20*

If your watcher node computer lies outside the perimeter network, then you must follow a slightly different procedure in order to configure that watcher node to run synthetic transactions. Specifically, you should not create a trusted application pool and a trusted application, and you must install a certificate that enables the watcher node to send alerts to a computer inside the perimeter network. This means that you will need to complete two separate tasks:

- Update the membership in the computer's RTC Local Read-only Administrators Group
- Install the watcher node configuration files

Updating Membership in the RTC Local Read-Only Administrators Group

If your watcher node lies outside the perimeter network, you must add the Network

Service account to the RTC Local Read-only Administrators group on the watcher node computer. To do this, complete the following procedure on the watcher node:

1. Click **Start**, right-click **Computer**, and then click **Manage**.
2. In Server Manager, expand **Configuration**, expand **Local Users and Groups**, and then click **Groups**.
3. In the Groups pane, double-click **RTC Local Read-only Administrators**.
4. In the **RTC Local Read-only Administrators Properties** dialog box, click **Add**.
5. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Locations**.
6. In the **Locations** dialog box, select the name of the watcher node computer, and then click **OK**.
7. In the **Enter object names to select** box, type **Network Service**, and then click **OK**.
8. In the **RTC Local Read-only Administrators Properties** dialog box, click **OK**, and then close **Server Manager**.

Restart the watcher node computer.

Installing the Watcher Node Configuration Files

After the watcher node computer has restarted, your next step is to run the file Watchernode.msi. To run this file, open the Lync Server 2013 Management Shell by clicking **Start**, clicking **All Programs**, clicking **Lync Server 2013**, and then clicking **Lync Server Management Shell**. In the Lync Server Management Shell, type the following command and then press ENTER (be sure and specify the actual path to your copy of Watchernode.msi):

```
C:\Tools\Watchernode.msi Authentication=Negotiate
```

Note:

As noted previously, Watchernode.msi can also be run from a command window. To open a command window, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**. When the command window opens, type the same command as shown earlier.

The Negotiate mode is used any time the watcher node cannot be set up as a trusted application pool. In this mode, administrators will need to manage test user passwords on the watcher node.

1.4.16.1.4.5 Configuring Watcher Node Test Users and Configuration Settings

Configuring Watcher Node Test Users and Configuration Settings

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Installing and Configuring Watcher Nodes >

Topic Last Modified: *2012-10-22*

After configuring the computer that will act as a watcher node, you must:

1. Create the test accounts to be used by these watcher nodes. If you are using the Negotiate authentication method, you must also use the Set-CsTestUserCredential cmdlet to enable these test accounts for use on the watcher node.
2. Update the watcher node configuration settings.

This section covers:

- Configuring Test User Accounts
- Configuring a Basic Watcher Node with the Default Synthetic Transactions
- Configuring Extended Tests
- Adding and Removing Synthetic Transactions
- Viewing and Testing the Watcher Node Configuration

Configuring Test User Accounts

Test users do not need to represent actual people, but they must be valid Active Directory Domain Services (AD DS) accounts; in addition, these accounts must be enabled for Lync Server 2013, they must have valid SIP addresses, and they should be enabled for Enterprise Voice (to use the Test-CsPstnPeerToPeerCall synthetic transaction). If you use the TrustedServer authentication method, then all you need to do is to make sure that these accounts exist and have been configured as specified here. You should assign at least three test users for each pool that you want to test.

If you are using the Negotiate authentication method, you must also use the **Set-CsTestUserCredential** cmdlet and the Lync Server Management Shell to enable these test accounts to work with the synthetic transactions. You can do this by running a command similar to the following. (These commands assume that the three Active Directory user accounts have already been created and that those accounts have been enabled for Lync Server 2013.):

```
Set-CsTestUserCredential -SipAddress "sip:watcher1@litwareinc.com" -UserName "lit
Set-CsTestUserCredential -SipAddress "sip:watcher2@litwareinc.com" -UserName "lit
Set-CsTestUserCredential -SipAddress "sip:watcher3@litwareinc.com" -UserName "lit
```

Note that you must include not only the SIP address but also the user name and password. If you do not include the password Set-CsTestUserCredential will prompt you to enter that information. The user name can be specified using the domain name\user name format shown above, or by using the format user name@domain name; for example:

```
-UserName "watcher3@litwareinc.com"
```

To verify that the test user credentials were created, run these commands from within the Lync Server Management Shell:

```
Get-CsTestUserCredential -SipAddress "sip:watcher1@litwareinc.com"
Get-CsTestUserCredential -SipAddress "sip:watcher2@litwareinc.com"
Get-CsTestUserCredential -SipAddress "sip:watcher3@litwareinc.com"
```

Information similar to this should be returned for each user:

```
UserName                        Password
--------                        --------
Litwareinc\watcher1              System.Security.SecureString
```

Configuring a Basic Watcher Node with the Default Synthetic Transactions

After the test users have been created you can then create a watcher node by using a command similar to this:

```
New-CsWatcherNodeConfiguration -TargetFqdn "atl-cs-001.litwareinc.com" -PortNumbe
```

This command creates a new watcher node that uses the default settings and runs the default set of synthetic transactions. The new watcher node also uses the test users watcher1@litwareinc.com, watcher2@litwareinc.com, and watcher3@litwareinc.com. If the watcher node is using TrustedServer authentication, the three test accounts can be any valid user accounts enabled for Active Directory and Lync Server. If the watcher node is using the Negotiate authentication method, you must also enable these user accounts for watcher node by using the **Set-CsTestUserCredential** cmdlet.

Configuring Extended Tests

If you want to enable the public switched telephone network (PSTN test), which verifies connectivity with the public switched telephone network, you will need to do some additional configuration when setting up the watcher node. First, you need to associate your test users with the PSTN test type. To do that, run a command similar to this from within the Lync Server Management Shell:

```
$pstnTest = New-CsExtendedTest -TestUsers "sip:watcher1@litwareinc.com", "sip:wat
```

Note that the results of this command must be stored in a variable. In this example, that's a variable named $pstnTest.

At this point, you can use the **New-CsWatcherNodeConfiguration** cmdlet to associate the test type (stored in the variable $pstnTest) to a Lync Server 2013 pool. For example, the following command creates a new watcher node configuration for the pool atl-cs-001.litwareinc.com, adding the three test users that were created previously, and also adding the PSTN test type:

```
New-CsWatcherNodeConfiguration -TargetFqdn "atl-cs-001.litwareinc.com" -PortNumbe
```

Note that the preceding command will fail if you have not installed the Lync Server core files and the RTCLocal database on the watcher node computer.

To test multiple voice policies, you need to create an extended test for each policy by using the **New-CsExtendedTest** cmdlet. The users assigned to this test should be configured with the desired voice policies. The extended tests are then passed to the **New-CsWatcherNodeConfiguration** cmdlet by using a command similar to the following:

```
-ExtendedTests @{Add=$pstnTest1,$pstnTest2,$pstnTest3}
```

If New-CsWatcherNodeConfiguration is called without using the Tests parameter, that means that only the Default synthetic transactions (and the specified extended synthetic transaction) will be enabled for the new watcher node. This means that the watcher node will test the following components:

- Registration
- IM
- GroupIM
- P2PAV (peer-to-peer audio/video sessions)
- AvConference (audio/conferencing)
- Presence
- ABS (Address Book service)
- ABWQ (Address Book web service)
- PSTN (PSTN gateway calls, specified as an extended test. By default, PSTN is disabled. The test is enabled in this case only because the command enabled PSTN by using the ExtendedTests parameter.)

This also means that the following components will not be tested by default:

- AVEdgeConnectivity
- MCXP2PIM (mobile device instant messaging)
- ExumConnectivity (Exchange Unified Messaging)
- JoinLauncher

- PersistentChatMessage
- DataConference
- XmppIM
- UnifiedContactStore

Adding and Removing Synthetic Transactions

After a watcher node has been configured, you can use the **Set-CsWatcherNodeConfiguration** cmdlet to add or remove synthetic transactions from the node. For example, to add the PersistentChatMessage test to the watcher node, use the Add method and a command similar to this:

```
Set-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" -Tests @{Add
```

Multiple tests can be added by separating the test names by using commas. For example:

```
Set-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" -Tests @{Add
```

Note that an error will occur if one or more of these tests (for example, DataConference) has already been enabled on the watcher node. In this case, you will receive an error message similar to the following:

```
Set-CsWatcherNodeConfiguration : There is a duplicate key sequence 'DataConferenc
```

When this error occurs, no changes will be applied. The command should be rerun with the duplicate test removed.

To remove a synthetic transaction from a watcher node, use the Remove method instead of the Add method. For example, this command removes the ABWQ test from a watcher node:

```
Set-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" -Tests @{Rem
```

You can also use the Replace method to replace all the currently-enabled tests with one or more new tests. For example, if you only want a watcher node to run the IM test, you can configure that by using this command:

```
Set-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" -Tests @{Rep
```

When you run the preceding command, all synthetic transactions on the specified watcher node will be disabled except for IM.

Viewing and Testing the Watcher Node Configuration

If you want to view the tests that have been assigned to a watcher node, use a command similar to this:

```
Get-CsWatcherNodeConfiguration -Identity "atl-cs-001.litwareinc.com" | Select-Obj
```

The preceding command will return information similar to this, depending on the synthetic transactions that have been assigned to the node:

```
Registration
IM
GroupIM
P2PAV
AvConference
```

```
Presence
PersistentChatMessage
DataConference
```

Tip:

To view the synthetic transactions in alphabetical order, use this command instead: Get-CsWatcherNodeConfiguration –Identity "atl-cs-001.litwareinc.com" | Select-Object –ExpandProperty Tests | Sort-Object

To verify that a watcher node has been created, type the following command from within the Lync Server Management Shell:

```
Get-CsWatcherNodeConfiguration
```

You will receive information similar to this:

```
Identity      : atl-cs-001.litwareinc.com
TestUsers     : {sip:watcher1@litwareinc.com, sip:watcher2@litwareinc.com ...}
ExtendedTests : {TestUsers=IList<System.String>;Name=PSTN Test; Te...}
TargetFqdn    : atl-cs-001.litwareinc.com
PortNumber    : 5061
```

To verify that the watcher node has been configured correctly, type the following command from within the Lync Server Management Shell:

```
Test-CsWatcherNodeConfiguration
```

The preceding command will test each watcher node in your deployment and tell you information, such as whether:

- The required Registrar role been installed.
- The required registry key was created for you when you ran Set-CsWatcherNodeConfiguration.
- Your servers are running the correct version of Lync Server.
- Your ports been configured correctly.
- Your assigned test users have the required credentials.

1.4.16.1.4.6 Managing Watcher Nodes

Managing Watcher Nodes

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Installing and Configuring Watcher Nodes >

Topic Last Modified: *2012-10-20*

In addition to modifying the synthetic transactions that are executed on a watcher node, administrators can also use the **Set-CsWatcherNodeConfiguration** cmdlet to carry out two other important tasks: enabling and disabling the watcher node, and configuring the watcher node to use either internal URLs or external URLs when running its tests.

By default, watcher nodes are designed to periodically run all their enabled synthetic transactions. Sometimes, however, you may need to suspend those transactions. For example, if the watcher node is temporarily disconnected from the network, then there is no reason to run the synthetic transactions. Without network connectivity, those transactions are guaranteed to fail. If you want to temporarily disable a watcher node, run a command similar to this from the Lync Server Management Shell:

```
Set-CsWatcherNodeConfiguration -Identity "atl-watcher-001.litwareinc.com" -Enable
```

This command will disable the execution of synthetic transactions on the watcher node atl-watcher- 001.litwareinc.com. To resume execution of the synthetic transactions, set the Enabled property back to True ($True):

```
Set-CsWatcherNodeConfiguration -Identity "atl-watcher-001.litwareinc.com" -Enable
```

Note:

The Enabled property can be used to turn watcher nodes on or off. If you want to permanently delete a watcher node, use the **Remove-CsWatcherNodeConfiguration** cmdlet:

Remove-CsWatcherNodeConfiguration –Identity "atl-watcher-001.litwareinc.com"

That command removes all the watcher node configuration settings from the specified computer, which prevents the computer from automatically running synthetic transactions. However, the command does not uninstall the System Center agent files or the Lync Server 2013 system files.

By default, watcher nodes use an organization's external URLs when conducting their tests. However, watcher nodes can also be configured to use the organization's internal URLs. This enables administrators to verify URL access for users located inside the perimeter network. To configure a watcher node to use internal URLs instead of external URLs, set the UseInternalWebUrls property to True ($True):

```
Set-CsWatcherNodeConfiguration -Identity "atl-watcher-001.litwareinc.com" -UseInt
```

If you reset this property to the default value of False ($False), the watcher will then use the external URLs:

```
Set-CsWatcherNodeConfiguration -Identity "atl-watcher-001.litwareinc.com" -UseInt
```

1.4.16.1.4.7 Special Setup Instructions for Synthetic Transactions

Special Setup Instructions for Synthetic Transactions

Health Configuration in Lync Server 2013 > Configuring Lync Server to Work With System Center Operations Manager > Installing and Configuring Watcher Nodes >

Topic Last Modified: *2013-01-22*

Most synthetic transactions can run on a watcher node as-is; that is, as soon as the synthetic transaction has been added to the watcher node configuration settings, the watcher node can begin using the synthetic transaction during its test passes. However, this is not true for all synthetic transactions. The exceptions—synthetic transactions that require special setup instructions—are discussed in the following sections.

Dealing With Server Timeout Errors

In some cases you might find that your synthetic transactions are failing with server timeout errors (error code 504). These errors are typically due to firewall problems. When a synthetic transaction is executed, that transaction runs under the MonitoringHost.exe process; in turn, MonitoringHost.exe starts an instance of the PowerShell.exe process. If either MonitoringHost.exe or PowerShell.exe is blocked by your firewall then the synthetic transaction will fail and will generate a 504 error.

To resolve this issue, you should manually create inbound firewall rules for both MonitoringHost.exe and PowerShell.exe.

Data Conferencing Synthetic Transactions

If your watcher node computer is located outside your perimeter network, you will probably not be able to run the Data Conferencing Synthetic Transaction unless you first disable the Internet Explorer proxy settings for the Network Service account. To disable the proxy settings for this service, complete the following procedure:

1. On the watcher node computer, click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. In the console window, type the following command and then press ENTER:

```
bitsadmin /util /SetIEProxy NetworkService NO_PROXY
```

The following message will appear in the command window:

```
BITSAdmin is deprecated and is not guaranteed to be available in future versions
Internet proxy settings for account NetworkService set to NO_PROXY.
(connection = default)
```

This message means that you have disabled the Internet Explorer proxy settings for the Network Service account.

Exchange Unified Messaging Synthetic Transactions

The Exchange Unified Messaging (UM) synthetic transaction verifies that test users can connect to voicemail accounts homed in Exchange. These test users will need to be preconfigured with voicemail accounts before they can use the Exchange UM tests.

Persistent Chat Synthetic Transactions

To use the Persistent Chat synthetic transaction, administrators must first create a channel and give the test users permissions to use it. The Test-CsPersistentChatMessage cmdlet can be used to properly configure these test users:

```
$cred1 = Get-Credential "litwareinc\kenmyer"
$cred2 = Get-Credential "litwareinc\pilar"
Test-CsPersistentChatMessage -TargetFqdn atl-cs-001.litwareinc.com -SenderSipAddr
```

This setup task must be run from inside the enterprise:

- If run from a nonserver machine, the user who runs the cmdlet must be a member of the PersistentChatAdministrators role for Role-Based Access Control (RBAC).
- If run from the server itself, the user who runs the cmdlet should be a member of the RTCUniversalServerAdmins group.

In the preceding command, the Setup parameter was included and set to True ($True). If you include the Setup parameter, Test-CsPersistentChatMessage will create a special Persistent Chat room and populate that room with the test users. This helps to ensure that there is actually a chat room available for testing purposes. Note that the Setup parameter should be run only from a Front End Server.

The chat room that is created by Test-CsPersistentChatMessage can be deleted only by an administrator.

PSTN Peer-to-Peer Call Synthetic Transactions

The Test-CsPstnPeerToPeerCall synthetic transaction verifies the ability to place and receive calls via the public switched telephone network (PSTN).

To run this synthetic transaction, administrators must configure:

- Two test users (a caller and a receiver) enabled for Enterprise Voice.
- Direct Inward Dialing (DID) numbers for each user account.
- Voice policies and voice routes that enable calls to the receiver's number to reach the PSTN gateway.
- A PSTN gateway that accepts calls, and media that route calls backs to a receiver's home pool based on the number dialed.

Unified Contact Store Synthetic Transactions

The Unified Contact Store synthetic transaction verifies that Lync Server 2013 is able to retrieve contacts on behalf of a user from Microsoft Exchange Server 2013.

To use this synthetic transaction, the following conditions must be met:

- Managing Server-to-Server Authentication (Oauth) and Partner Applications must be configured between Lync Server 2013 and Exchange 2013.
- Test users must have a valid Exchange 2013 mailbox.

After these conditions are met, administrators can run the following command to verify that the user with the SIP address kenmyer@litwareinc.com can retrieve his contacts from the unified contact store:

```
Test-CsUnifiedContactStore -TargetFqdn atl-cs-001.litwareinc.com -UserSipAddress
```

Note the use of the Setup parameter used in the preceding command. If the Setup parameter is included when running Test-CsUnifiedContactStore then the specified user's contacts (in this case, sip:kenmyer@litwareinc.com) will be moved to the unified contact store. (Of course, if the user's contacts are already in the Unified Contact Store then they do not have to be moved.) The Setup parameter is typically used only one time (the first time Test-CsUnifiedContactStore is executed), and should only be used with test users; that is, with user accounts that will never actually be logged on to Lync Server. After your test user has been migrated to the unified contact store, you can verify that the user's contacts can be retrieved by calling Test-CsUnifiedContactStore without the Setup parameter:

```
Test-CsUnifiedContactStore -TargetFqdn atl-cs-001.litwareinc.com -UserSipAddress
```

XMPP Synthetic Transactions

The XMPP (Extensible Messaging and Presence Protocol) IM synthetic transaction requires that the XMPP feature be configured with one or more federated domains.

To enable the XMPP synthetic transaction, an XmppTestReceiverMailAddress parameter must be provided with a user account at a routable XMPP domain. For example:

```
Set-CsWatcherNodeConfiguration -Identity pool0.contoso.com -Tests @{Add="XmppIM"}
```

In this example, a Lync Server 2013 rule will need to exist to route messages for litwareinc.com to an XMPP gateway.

1.4.16.2 Using Rich Logging for Synthetic Transactions

Using Rich Logging for Synthetic Transactions

Microsoft Lync Server 2013 > Deployment > Health Configuration in Lync Server 2013 >

Topic Last Modified: *2012-10-22*

Synthetic transactions (introduced in Microsoft Lync Server 2010) provide a way for administrators to verify that users are able to successfully complete common tasks such as logging on to the system, exchanging instant messages, or making calls to a phone located on the public switched telephone network (PSTN). These tests (which are packaged as a set of Lync Server Windows PowerShell cmdlets) can be conducted manually by an administrator, or they can be automatically run by an application such as System Center Operations Manager.

In Lync Server 2010, synthetic transactions proved extremely useful in helping administrators to identify problems with the system. For example, the **Test-CsRegistration** cmdlet could alert administrators to the fact that some users were having difficulty registering with Lync Server. However, the synthetic transactions were somewhat less useful in helping administrators determine why these users were having difficulty registering with Lync Server. This was due to the fact that the synthetic transactions did not provide detailed logging information that could help administrators troubleshoot problems with Lync Server. At best, the verbose output from a synthetic transaction provided step-by-step information that might enable an administrator to make an educated guess as to where a problem likely occurred.

In Microsoft Lync Server 2013, synthetic transactions have been re-architected to provide rich logging. "Rich logging" means that, for each activity that a synthetic transaction undertakes, information such as this will be recorded:

- The time that the activity started
- The time that the activity finished
- The action that was performed (for example, creating, joining, or leaving a conference; signing on to Lync Server; sending an instant message; and so on)
- Informational, verbose, warning, or error messages generated when the activity ran
- SIP registration messages
- Exception records or diagnostic codes generated when the activity ran
- The net result of running the activity

This information is automatically generated each time a synthetic transaction is run. However, the information is not automatically displayed or saved to a log file. Instead, administrators who are manually running a synthetic transaction can use the OutLoggerVariable parameter to specify a Windows PowerShell variable in which the information will be stored. From there, administrators can then use a pair of methods that enable them to save and/or view the rich log in either XML or HTML format.

For example, Lync Server 2010 administrators might run the **Test-CsRegistration** cmdlet by using a command similar to the following:

```
Test-CsRegistration -TargetFqdn atl-cs-001.litwareinc.com
```

Administrators have the option of including the OutLoggerVariable parameter followed by a variable name of their choosing:

```
Test-CsRegistration -TargetFqdn atl-cs-001.litwareinc.com -OutLoggerVariable Regi
```

Note:

Do not preface the variable name with the $ character. Use a variable name like RegistrationTest and not $RegistrationTest.

The preceding command outputs content similar to the following:

```
Target Fqdn   : atl-cs-001.litwareinc.com
Result        : Failure
Latency       : 00:00:00
Error Message : This machine does not have any assigned certificates.
Diagnosis     :
```

However, much more detailed information is available for this failure than just the error message shown above. To access that information in HTML format, use a command similar to this in order to save the information stored in the variable RegistrationTest to an HTML file:

```
$RegistrationTest.ToHTML() | Out-File C:\Logs\Registration.html
```

Alternatively, you can use the ToXML() method to save the data to an XML file:

```
$RegistrationTest.ToXML() | Out-File C:\Logs\Registration.xml
```

These files can then be viewed using Internet Explorer, Visual Studio, or any other application capable of opening HTML/XML files.

Synthetic transactions run from inside of System Center Operations Manager will automatically generate these log files for failures. However, these logs will not be generated if the execution fails before Windows PowerShell is able to load and run the synthetic transaction.

Important:

By default, Lync Server 2013 saves log files to a folder that is not shared. To make these logs readily accessible, you should share this folder (for example, \\atl-watcher-001.litwareinc.com\WatcherNode.

1.4.16.3 Using Microsoft SQL Server 2008 R2 as Your System Center Operations Manager Database

Using Microsoft SQL Server 2008 R2 as Your System Center Operations Manager Database

Microsoft Lync Server 2013 > Deployment > Health Configuration in Lync Server 2013 >

Topic Last Modified: *2012-10-22*

To use SQL Server 2008 R2 as your back-end database, complete the steps detailed in this topic.

Configuring SQL Server 2008 R2 and SQL Server Reporting Services

Before you begin installing System Center Operations Manager you must make two changes to your SQL Server 2008 R2 and your SQL Server Reporting Services configuration. (These changes are required only if you are using SQL Server 2008 R2 as your Operations Manager database.) First, do the following on the computer that will host your Operations Manager database:

1. Click **Start** and then click **Run**.
2. In the **Run** dialog box, type **C:\Program Files\Microsoft SQL Server\MSRS10_50.ARCHINST\Reporting Services\ReportServer** and then press

ENTER.

3. In the **ReportServer** folder, open the file **rsreportserver.config** in Notepad or any other text editor.
4. Near the beginning of the file you will see a series of "Add Key" nodes. Find the entry that begins **<Add Key="SecureConnectionLevel"** and set the value to **0**:

```
<Add Key="SecureConnectionLevel" Value="0"/>
```

5. Save the file **rsreportserver.config** and then close your text editor.

After updating the Report Server configuration file you must then assign the correct certificate to SQL Server Reporting Services. To do that:

1. Click **Start**, click **All Programs**, click **Microsoft SQL Server 2008 R2**, click **Configuration Tools**, and then click **Reporting Services Configuration Manager**.
2. In the **Reporting Services Configuration Connection** dialog box, make sure that the name of your server appears in the **Server Name** box. Select the SQL Server instance that will host your Operations Manager database (for example, **ARCHINST**) from the **Report Server Instance** drop-down list and then click **Connect**.
3. In Reporting Services Configuration Manager, click **Web Service URL**.
4. On the **Web Service URL** page, select the certificate to be used for your Reporting Services from the **SSL Certificate** dropdown list and then click **Apply**. After a few seconds, you will see a pair of URLs listed under **Report Server Web Service URLs**.
5. Click both of the URLs to verify that you can access SQL Server Reporting Services.
6. Close Reporting Services Configuration Manager.

Creating a System Center Operations Manager database for use with SQL Server 2008 R2

If you want to configure System Center Operations Manager to use a SQL Server 2008 R2 database, you will need to "manually" create the Operations Manager database on the computer running SQL Server 2008 R2. (Again, these steps are not required if you are using UNRESOLVED_TOKEN_VAL(nm-sql-2005) or UNRESOLVED_TOKEN_VAL(nm-sql-2008) as your back-end database.)

To manually create an Operations Manager database do the following:

1. On the System Center Operations Manager 2007 R2 setup media, in the SupportTools\AMD64 folder, double-click **DBCreateWizard.exe**.
2. In the Database Configuration Wizard, on the **Welcome to the Database Configuration Wizard** page, click **Next**.
3. On the **Database Information** page leave all the settings as-is and then click **Next**
4. On the **Management Group Configuration** page type a name for your Management Group (for example, **Lync Server Monitoring**) in the **Management Group name** box and then click **Next**.
5. On the **Operations Manager Error Reports** page click **Next**.
6. On the **Summary** page click **Finish**.

Creating a System Center Operations Manager data warehouse for use with SQL Server 2008 R2

Microsoft Lync Server 2013 ships with three new System Center Operations Manager reports:

- **End to End Scenario Availability Report** This report details the availability/ uptime for key Lync Server services such as registration or presence.
- **Capacity Report** Using performance counter information, this report shows trends for system components such as memory availability and processor usage.
- **Component Report** This report lists the top alert generators grouped by Lync Server component.

In order to use these new reports you must install a System Center Operations Manager data warehouse. (A data warehouse provides for long-term storage of operations data.) To use a data warehouse with SQL Server 2008 R2 you must carry out the following steps on the computer that hosts your SQL Server database:

1. On the System Center Operations Manager setup media, in the Setup \SupportTools\AMD64 folder, double-click **DBCreateWizard.exe**.
2. In the Database Configuration Wizard, on the **Welcome to the Database Configuration Wizard** page, click **Next**.
3. On the **Database Information** page, select **Operations Manager Data Warehouse Database** from the **Database Type** dropdown list and then click **Next**.
4. On the **Summary** page click **Finish**.

Installing the System Center Operations Manager console

The Operations Manager console is the primary tool used to manage System Center Operations Manager. Before you install the Operations Manager console, make sure that you have installed a supported version of SQL Server along with the SQL Server Reporting Service. It is also recommended that you run SQL Server's Reporting Services Configuration Manager to verify that the Reporting Service has been correctly installed and configured.

To install the System Center Operations Manager console:

1. On the System Center Operations Manager setup media, double-click **SetupOM.exe**.
2. In System Center Operations Manager 2007 R2 Setup, click **Check Prerequisites**.
3. In the System Center Operations Manager Prerequisite Viewer, select the System Center components to be installed: (**Server**; **Console**; and **PowerShell**) and then click **Check**. Verify that no blocking issues have been reported and then click **Close**. If a blocking issue has been reported, correct the problem and then click **Check** to re-run the prerequisite testing.
4. In System Center Operations Manager Setup, click **Install Operations Manager**.
5. In the System Center Operations Manager Setup wizard, on the **Welcome to the System Center Operations Manager Setup Wizard** page, click **Next**.
6. On the **End-User License Agreement** page, select **I accept the terms in the license agreement** and then click **Next**.
7. On the **Product Registration** page, type your name in the **User Name** box and name of your organization in the **Organization** box. Type your System Center Operations Manager product key in the **Enter your 25 digit CD Key** box and then click **Next**.
8. On the **Custom Setup** page select the System Center options to be installed and then click **Next**. You should select **Management Server**, **User Interfaces**, and **Web Console** to be installed. **Database** should not be selected and should not be installed.
9. On the **SC Database Server Instance** page, verify that the name of the computer where the Operations Manager databases are installed appears in

the **System Center Database Server** box. Click **Next**.

10. On the **Management Server Action Account** page, select **Domain or Local Computer Account** and then enter the appropriate values in the **User Account**, **Password**, and **Domain or local computer** boxes. Click **Next**.
11. On the **SDK and Config Service Account** page, select **Domain or Local Computer Account** and then enter the appropriate values in the **User Account**, **Password**, and **Domain or local computer** boxes. Click **Next**.
12. On the **Operations Manager Error Reports** page click **Next**.
13. On the **Customer Experience Improvement Program** page click **Next**.
14. On the **Ready to Install the Program** page, click **Install**.
15. On the **Completing the System Center Operations Manager Setup** page, clear the **Backup Encryption Key** and **Start the console checkboxes** and then click **Finish**.
16. In System Center Operations Manager Setup click **Exit**.

Installing System Center Reporting Services

After installing and configuring the System Center Operations Manager console you must then install System Center Reporting Services. If you are using SQL Server 2008 R2 as your Operations Manager back-end database, that means that you must first make a temporary change to the security group associated with SQL Server Reporting Services. If you are using SQL Server 2008 R2, you must do the following:

1. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. In Server Manager, expand **Configuration**, expand **Local Users and Groups**, and then click **Groups**.
3. Locate the following group, where atl-sc-001 represents the name of your computer and ARCHINST represents the SQL Server instance for the System Center database: **SQLServerReportServerUser$atl-sc-001$MSRS10_50.ARCHINST**.
4. Right-click the group and then click **Rename**. Rename the group by deleting **_50** from the group name. For example: **SQLServerReportServerUser$atl-sc-001$MSRS10.ARCHINST**.
5. Close Server Manager.

At this point you are ready to install System Center Reporting Services. To do this:

1. On the System Center Operations Manager 2007 R2 Setup media, double-click **SetupOM.exe**.
2. In System Center Operations Manager 2007 R2 Setup, click **Install Operations Manager Reporting**.
3. In the System Center Operations Manager 2007 R2 Reporting Setup wizard, on the **Welcome to Operations Manager Reporting Setup** page, click **Next**.
4. On the **End-user License Agreement** page select **I accept the terms of the license agreement** and then click **Next**.
5. On the **Product Registration** page, ensure that your name and the name of your organization appear in the **User Name** and **Organization** boxes and then click **Next**.
6. On the **Custom Setup** page, click **Reporting Server** and select **This component, and all dependent components, will be installed on local disk drive**. Click **Data Warehouse** and select **This component will not be available**, and then click **Next**.
7. On the **Connect to the Root Management Server** page, type the name of your Operations Manager root management server in the **Root Management Server** box and then click **Next**.
8. On the **Connect to the Operations Manager Data Warehouse** page, type the SQL Server instance where your data warehouse is located in the **SQL Server Instance** box. (If your data warehouse is located in the Default instance then simply type the server name; for example: atl-sql-001.) Verify that the database name **OperationsManagerDW** appears in the **Name** box,

and that port **1433** appears in the **SQL Server port** box. Click **Next**.

9. On the **SQL Server Reporting Instance** page, select your SQL Server reporting server from the **Enter the SQL Server Reporting Services Server** dropdown list and then click **Next**.
10. On the **Data Warehouse Write Account** page, enter the name and password of the user to be initially assigned write permissions to the data warehouse in the **User Account** and **Password** boxes. Select the user's domain from the **Domain** dropdown list and then click **Next**.
11. On the **Data Reader Account** page, enter the name and password of the user account to be used when SQL Reporting Services queries the data warehouse in the **User Account** and **Password** boxes. Select the account domain from the **Domain** dropdown list and then click **Next**.
12. On the **Operational Data Reports** page, click **Next**.
13. On the **Microsoft Update** page, click **Next**.
14. On the **Ready to Install the Program** page, click **Install**.
15. On the **Completing the Operations Manager Reporting Components Setup Wizard** page, click **Finish**.
16. In System Center Operations Manager 2007 R2 Setup, click **Exit**.

After System Center reporting has been installed you then use the following procedure to reset the name of the security group associated with SQL Server reporting. Again, this procedure is only required if you are using SQL Server:

1. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. In Server Manager, expand **Configuration**, expand **Local Users and Groups**, and then click **Groups**.
3. Locate the following group, where atl-sc-001 represents the name of your computer and ARCHINST represents the SQL Server instance for the archiving and monitoring databases: **SQLServerReportServerUser$atl-sc-001$MSRS10.ARCHINST**.
4. Right-click the group and then click **Rename**. Rename the group by adding **_50** to the end of the group name, right before the SQL Server instance name. For example: **SQLServerReportServerUser$atl-sc-001$MSRS10_50.ARCHINST**.
5. Close Server Manager.

If the System Center Operations Console is open you will need to close the application and then restart it; if you do not do this the **Reporting** tab will not appear in the Operations Console user interface. Note that, after restarting the Operations Console the first time, it could take several minutes before all the Monitoring Reports appear on the **Reporting** tab.

1.4.17 Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Microsoft Lync Server 2013 > Planning > Planning for Exchange Server Integration >

Topic Last Modified: *2012-10-10*

Exchange and Lync Server have a long history of integration and compatibility. This integration is most noticeable within their respective client application. For example, Lync presence information can be reported in Microsoft Outlook; likewise, Lync can use Outlook calendar to automatically update that presence information. (For example, Lync can change your status to Busy any time your calendar shows that you have a meeting scheduled.) Although you do not have to run Exchange in order to run Lync Server (or vice-versa) there's little doubt that using the two products together epitomizes the very definition of the term "better together."

This is especially true with the release of Microsoft Lync Server 2013 and Microsoft Exchange Server 2013. In addition to features, such as unified messaging and IM and presence, that are found in Microsoft Exchange Server 2010 and Microsoft Lync Server 2010, the 2013 releases of the server products include a number of new capabilities. These capabilities include such things as:

- **Lync Archiving Integration**. In Lync Server 2013 administrators still have the option of having instant messaging and Web conferencing transcripts archived to SQL Server (the same way these transcripts were archived in Lync Server 2010). Alternatively, however, administrators can choose to have transcripts archived to Exchange 2013, storing those transcripts in the individual user mailboxes in the same way in which Exchange archives communications. That means a single repository for all your electronic communications (from both Exchange and Lync Server), which makes it much easier to search for and retrieve those archived communications should the need arise.
- **Unified Contact Store**. In Lync Server 2010, users had to maintain separate contact lists in Outlook and Lync; in fact, to ensure that you had the same contacts available in both products you had to maintain duplicate contact lists, one for Outlook and one for Lync. With Lync Server 2013, however, user contacts can be stored in Exchange 2013 and the unified contact store. Using a single contact store enables users to maintain just one set of contacts, with that same set of contacts being available in Lync 2013, Outlook 2013, and Outlook Web Access 2013.
- **High resolution photos**. Lync 2010 could only display small photos of your contacts; that's because those photos were stored in Active Directory, and Active Directory imposes a 48 pixel by 48 pixel size limitation on stored photos. With Lync Server 2013, however, photos can be stored in Microsoft Exchange; that allows for high-resolution photos as large as 648 pixels by 648 pixels. As you might expect, Lync 2013 has been upgraded to allow for the display of these high-resolution photographs.

Keep in mind that these new features require the use of both Lync Server 2013 and Exchange 2013. In addition to that, users who hope to take full advantage of these new capabilities must have accounts on Lync Server 2013 and Exchange 2013, and must be using the latest versions of the client software (e.g., Lync 2013). For example, the unified contact store is not available to users who have been homed on Lync Server 2010; likewise, high-resolution photos cannot be displayed in Lync 2010.

This documentation provides information on integrating Lync Server 2013 and Exchange 2013. including step-by-step information on enabling new features such archiving Integration and the unified contact store. What this documentation does not do is discuss the initial setup and configuration of these two products. For details about deploying Lync Server 2013 see the Lync Server 2013 Tech Center at http://go.microsoft.com/fwlink/p/?LinkId=246127. For details about deploying Exchange 2013 see the Exchange 2013 Tech Center at http://go.microsoft.com/fwlink/p/?LinkId=268528.
Prerequisites for Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Configuring Partner Applications in Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Configuring Microsoft Lync Server 2013 to Use Microsoft Exchange Server 2013 Archiving

Configuring Microsoft SharePoint Server 2013 to Search for Archived Microsoft Lync Server 2013 Data

Configuring Microsoft Lync Server 2013 to Use the Unified Contact Store

Configuring the Use of High-Resolution Photos in Microsoft Lync Server 2013

Configuring Microsoft Exchange Server 2013 Unified Messaging for Microsoft Lync Server 2013 Voicemail

Integrating Microsoft Lync Server 2013 and Microsoft Outlook Web App 2013

1.4.17.1 Prerequisites for Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Prerequisites for Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2012-10-10*

Before you can integrate Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 you must ensure that all the prerequisite steps have been completed. As you might expect, integration cannot take place until both Exchange 2013 and Lync Server 2013 are fully installed and up and running. For details about installing Exchange, see the Exchange 2013 Planning and Deployment documentation at http://go.microsoft.com/fwlink/p/?LinkId=268539. For details about installing Lync Server 2013, see the planning and deployment documentation at http://go.microsoft.com/fwlink/p/?LinkId=254806.

After the servers are up and running you must assign server-to-server authentication certificates to both Lync Server 2013 and Exchange 2013; these certificates allow Lync Server and Exchange to exchange information and to communicate with one another. When you install Exchange 2013, a self-signed certificate with the name Microsoft Exchange Server Auth Certificate is created for you. This certificate, which can be found in the local computer certificate store, should be used for server-to-server authentication on Exchange 2013. For details about assigning certificates in Exchange 2013, see "Configure Mail Flow and Client Access" at http://go.microsoft.com/fwlink/p/?LinkId=268540.

For Lync Server 2013 you can use an existing Lync Server certificate as your server-to-server authentication certificate; for example, your default certificate can also be used as the OAuthTokenIssuer certificate. Lync Server 2013 allows you to use any Web server certificate as the certificate for server-to-server authentication provided that:

- The certificate includes the name of your SIP domain in the Subject field.
- The same certificate is configured as the OAuthTokenIssuer certificate on all of your Front End Servers.
- The certificate has a length of at least 2048 bits.

For details about server-to-server authentication certificates for Microsoft Lync Server 2013, see Assigning a Server-to-Server Authentication Certificate to Microsoft Lync Server 2013.

After the certificates have been assigned you must then configure the autodiscover service on Exchange 2013. In Exchange 2013, the autodiscover service configures user profiles and provides access to Exchange services when users log on to the system. Users present the autodiscover service with their email address and password; in turn, the services provide the user with information such as:

- Connection information for both internal and external connectivity to Exchange 2013.
- The location of the user’s Mailbox server.
- URLs for Outlook features such as free/busy information, Unified Messaging, and the offline address book.

- Outlook Anywhere server settings.

The autodiscover service must be configured before you can integrate Lync Server 2013 and Exchange 2013. You can verify whether or not the autodiscover service has been configured by running the following command from the Exchange Management Shell and checking the value of the AutoDiscoverServiceInternalUri property:

```
Get-ClientAccessServer
```

If this value is blank, you must assign a URI to the autodiscover service. Typically this URI will look similar to this:

```
https://autodiscover.litwareinc.com/autodiscover/autodiscover.xml
```

You can assign the autodiscover URI by running a command similar to this:

```
Get-ClientAccessServer | Set-ClientAccessServer -AutoDiscoverServiceInternalUri "
```

For details about the autodiscover service, see "Understanding the Autodiscover Service" at http://go.microsoft.com/fwlink/p/?LinkId=268542.

After the autodiscover service has been configured you must then modify the Lync Server OAuth configuration settings; this ensures that that Lync Server knows where to find the autodiscover service. To modify the OAuth configuration settings in Lync Server 2013, run the following command from within the Lync Server Management Shell. When running this command, be sure that you specify the URI to the autodiscover service running on your Exchange server, and that you use **autodiscover.svc** to point to the service location instead of **autodiscover.xml** (which points to the XML file used by the service):

```
Set-CsOAuthConfiguration -Identity global -ExchangeAutodiscoverUrl "https://autod
```

Note:

The Identity parameter in the preceding command is optional; that's because Lync Server only allows you to have a single, global collection of OAuth configuration settings. Among other things, that means that you can configure the autodiscover URL by using this slightly-simpler command:
Set-CsOAuthConfiguration–ExchangeAutodiscoverUrl "https://autodiscover.litwareinc.com/autodiscover/autodiscover.svc"
If you are unfamiliar with the technology, OAuth is a standard authorization protocol used by a number of major websites. With OAuth, user credentials and passwords are not passed from one computer to another. Instead, authentication and authorization is based on the exchange of security tokens; these tokens grant access to a specific set of resources for a specific amount of time.

In addition to configuring the autodiscover service, you must also create a DNS record for the service that points to your Exchange server. For example, if your autodiscover service is located at autodiscover.litwareinc.com you will need to create a DNS record for autodiscover.litwareinc.com that resolves to the fully qualified domain name of your Exchange server (for example, atl-exchange-001.litwareinc.com).

1.4.17.2 Configuring Partner Applications in Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Configuring Partner Applications in Microsoft Lync Server 2013 and Microsoft Exchange Server 2013

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2012-11-12*

Server-to-server authentication typically involves three entities: the two servers that need to communicate with one another, and a third-party security token server. If two servers (for example, Server A and Server B) need to communicate, then both of those servers typically start by contacting a token server and obtain a mutually-trusted security token. Server A then present that security token to Server B (and vice-versa) as a way to guarantee both its authenticity and its trustworthiness.

However, that's a general rule. Lync Server 2013, Microsoft Exchange Server 2013, and Microsoft SharePoint Server 2013 do not need to use a third-party token server when communicating with one another; that's because these server products can create security tokens that can be accepted by one another without the need for a separate token server. (This capability is only available in Lync Server 2013, Exchange 2013, and SharePoint Server 2013. If you need to set up server-to-server authentication with other servers, including other Microsoft server products, then you will need to do so by using a third-party token server.)

In order to set up server-to-server authentication between Lync Server and Exchange you must do two things: 1) you must assign the appropriate certificates to each server; and, 2) you must configure each server to be a partner application of the other server: that means you must configure Lync Server 2013 to be a partner application for Exchange 2013, and you must configure Exchange 2013 to be a partner application for Lync Server 2013.

Configuring Lync Server 2013 to be a Partner Application for Exchange 2013

The easiest way to configure Lync Server 2013 to be a partner application with Exchange 2013 is to run the Configure-EnterprisePartnerApplication.ps1 script, a Windows PowerShell script that ships with Exchange 2013. To run this script, you must provide the URL for the Lync Server authentication metadata document; this will typically be the fully qualified domain name of the Lync Server 2013 pool followed by the suffix /metadata/json/1. For example:

```
https://atl-cs-001.litwareinc.com/metadata/json/1
```

To configure Lync Server as a partner application, open the Exchange Management Shell and run a command similar to this (assuming that Exchange has been installed on drive C: and that it uses the default folder path):

```
"C:\Program Files\Microsoft\Exchange Server\V15\Scripts\Configure-EnterprisePartn
```

After configuring the partner application it is recommended that you stop and restart Internet Information Services (IIS) on your Exchange mailbox and client access servers. You can restart IIS by using a command similar to this, which restarts the service on the computer atl-exchange-001:

```
iisreset atl-exchange-001
```

This command can be run from within the Exchange Management Shell or from any other command window run under administrator privileges.

Configuring Exchange 2013 to be a Partner Application for Lync Server 2013

After you have configured Lync Server 2013 to be a partner application for Exchange 2013, you must then configure Exchange to be a partner application for Lync Server. This can be done by using the Lync Server Management Shell and specifying the authentication metadata document for Exchange; this will typically be the URI of the Exchange autodiscover service followed by the suffix /metadata/json/1. For example:

```
https://autodiscover.litwareinc.com/autodiscover/metadata/json/1
```

In Lync Server, partner applications are configured by using the New-CsPartnerApplication cmdlet. In addition to specifying the metadata URI you should also set the application trust level to Full; this will allow Exchange to represent both itself and any authorized user in the realm. For example:

```
New-CsPartnerApplication -Identity Exchange -ApplicationTrustLevel Full -Metadata
```

Alternatively, you can create a partner application by copying and modifying the script code found in the Lync Server 2013 server-to-server authentication documentation. See the article Managing Server-to-Server Authentication (Oauth) and Partner Applications for more information.

If you have successfully configured partner applications for both Lync Server and Exchange that means that you have also successfully configured server-to-server authentication between the two products. Lync Server 2013 includes a Windows PowerShell cmdlet, Test-CsExStorageConnectivity, that enables you to verify that server-to-server authentication has been correctly configured and that the Lync Server Storage Service can connect to Exchange 2013. The cmdlet does this by connecting to the mailbox of an Exchange 2013 user, writing an item into the Conversation History folder for that user, and then, optionally, deleting that item.

To test the integration of Lync Server 2013 and Exchange 2013, run a command similar to this from within the Lync Server Management Shell:

```
Test-CsExStorageConnectivity -SipUri "sip:kenmyer@litwareinc.com"
```

In the preceding command, the SipUri represents the SIP address of a user with an account on Exchange 2013; your command will fail in this is not a valid user account.

If the test succeeds and connectivity has been established, you can then proceed to configure optional features such as archiving integration and the unified contact store.

1.4.17.3 Configuring Microsoft Lync Server 2013 to Use Microsoft Exchange Server 2013 Archiving

Configuring Microsoft Lync Server 2013 to Use Microsoft Exchange Server 2013 Archiving

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2012-10-04*

Microsoft Lync Server 2013 gives administrators the option of having instant messaging and Web conferencing transcripts archived to a user's Microsoft Exchange Server 2013 mailbox rather than a SQL Server database. If you enable this option, transcripts are written to the Purges folder in the user's mailbox. The Purges folder is a hidden folder found in the Recoverable Items folder. Although this folder is not visible to end-users, the folder is indexed by the Exchange search engine and can be discovered by using Exchange mailbox search and/or Microsoft SharePoint Server 2013. Because information is stored in the same folder used by the Exchange In-Place Hold feature (responsible for archiving email and other Exchange communications), administrators can use a single tool to search for all the electronic communications archived for a user.

In order to archive transcripts to Exchange 2013 you must begin by configuring server-to-server authentication between the two servers. After server-to-server authentication is in place you can then carry out the following tasks in Microsoft Lync Server 2013 (note that, depending on your setup and configuration, you might not need to complete all of these tasks):

1. Enable Exchange archiving by modifying your Lync Server archiving configuration settings. This step is required for all deployments.
2. Enable archiving for internal and/or external communications for your users. This step is required for all deployments.
3. Configure the ExchangeArchivingPolicy property for each user. This step is only required in Lync Server and Exchange are located in different forests.

Step 1: Enabling Exchange Archiving

Archiving in Lync Server is primarily managed by using the archiving configuration settings. When you install Lync Server 2013 you are automatically given a single, global collection of these settings. (Administrators can optionally create new collections of archiving settings at the site scope.) By default, archiving is not enabled in the global settings, nor is Exchange archiving enabled in these settings. In order to use Exchange archiving administrators must configure both the EnableArchiving and the EnableExchangeArchiving properties in these configuration settings. The EnableArchiving property can be set to one of three possible values:

- **None**. Archiving is disabled. This is the default value. If EnableArchiving is set to None then nothing will be archived in either your Lync Server archiving database or in Exchange 2013.
- **ImOnly**. Only instant message transcripts are archived. If Exchange archiving is enabled these transcripts will be archived in Exchange 2013. If Exchange archiving is disabled then these transcripts will be archived to Lync Server.
- **ImAndWebConf**. Both instant message transcripts and Web conferencing transcripts are archived. If Exchange archiving is enabled these transcripts will be archived in Exchange 2013. If Exchange archiving is disabled then these transcripts will be archived to Lync Server.

The EnableExchangeArchiving property is a Boolean value: set EnableExchangeArchiving to True ($True) to enable Exchange archiving or set EnableExchangeArchiving to False ($False) to disable Exchange archiving. For example, this command enables the archiving of instant messaging transcripts and also enables Exchange archiving:

```
Set-CsArchivingConfiguration -Identity "global" -EnableArchiving ImOnly -EnableEx
```

To disable Exchange archiving, use a command similar to the following, which enables instant messaging archiving but disables archiving to Exchange (in other words, transcripts will be archived to Lync Server):

```
Set-CsArchivingConfiguration -Identity "global" -EnableArchiving ImOnly -EnableEx
```

Note:

If the EnableArchiving property is set to None then Lync Server will not archive instant messaging and Web conferencing transcripts at all. In that case, the server will simply ignore the value configured for EnableExchangeArchiving.

Exchange archiving can also be enabled (or disabled) by using the Lync Server Control Panel. To do that, complete the following procedure:

1. In Control Panel, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
2. On the **Archiving Configuration** tab, double-click the collection of archiving

settings to be modified (for example, the **Global** collection).

3. In the **Edit Archiving Setting** pane, click the **Archiving setting** dropdown list and select either **Archive IM sessions** (to archive just instant messaging sessions) or **Archive IM and web conferencing sessions** (to archive both instant messaging and Web conferencing sessions).
4. After choosing the items to be archived, select the **Exchange Server integration** checkbox to enable Exchange archiving. To disable Exchange archiving, clear this checkbox.

Note:

The **Exchange Server integration** checkbox will not be available if the **Archiving setting** is set to **Disable archiving**. You must enable archiving first and then enable Exchange archiving.

If Lync Server 2013 and Exchange 2013 are located in the same forest then archiving for individual users (or at least for users who have email accounts on Exchange 2013) is managed by using Exchange In-Place Hold policies. If you have users who are homed on a previous version of Exchange then archiving for those users will be managed by using Lync Server archiving policies. Note that only users with accounts on Exchange 2013 can have their Lync transcripts archived to Exchange.

If Lync Server 2013 and Exchange 2013 are located in different forests then archiving for individual users is managed by configuring the ExchangeArchivingPolicy property for each individual user account. See Step 3 for more information.

Step 2: Enabling the Archiving of Internal and/or External Communications

After you have enabled archiving (and Exchange archiving) you must then modify the appropriate archiving policies to ensure that user sessions are actually archived. Note that simply enabling archiving (Step 1) does not cause Lync Server to begin archiving instant messaging and Web conferencing transcripts. Instead, you must use archiving policies to enable internal and/or external archiving. When you install Lync Server 2013 you also install a single, global archiving policy that contains two properties:

- **ArchiveInternal**. When set to True ($True) indicates that internal communication sessions involving only users who have Active Directory accounts in your organization) will be archived.
- **ArchiveExternal**. When set to True ($True) indicates that internal communication sessions (sessions involving at least one user who does not have an Active Directory account in your organization) will be archived.

By default, both of these property values are set to False, meaning that neither internal nor external communication sessions are archived. To modify the global policy, you can use the Lync Server Management Shell and the Set-CsArchivingPolicy cmdlet. This command enables the archiving of both internal and external communication sessions:

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $True -ArchiveExternal
```

Alternatively, you can use the New-CsArchivingPolicy to create a new policy at either the site scope or the per-user scope. For example, this command creates a new per-user archiving policy named RedmondArchivingPolicy:

```
New-CsArchivingPolicy -Identity "RedmondArchivingPolicy" -ArchiveInternal $True -
```

If you create a per-user policy you will then need to assign that policy to the appropriate users. For example:

```
Grant-CsArchivingPolicy -Identity "Ken Myer" -PolicyName  "RedmondArchivingPolicy
```

Archiving policies can also be managed by using the Lync Server Control Panel. Within the Control Panel, click **Monitoring and Archiving** and then click **Archiving Policy**. To modify an existing policy, double-click the policy (e.g., Global) and then, in the **Edit Archiving Policy** pane, select or clear the **Archive internal communications** and the **Archive external communications** checkboxes as needed. To create a new archiving policy, click **New** and then select either **Site policy** or **User policy**. If you create a new user policy then you must access the appropriate user accounts (from the **Users** tab) and assign those users the new policy.

Step 3: Configuring the ExchangeArchivingPolicy Property

If Lync Server 2013 and Exchange 2013 are located in different forests then it is not enough to simply enable Exchange archiving in the archiving configuration settings; that will not result in instant messaging and Web conferencing transcripts being archived in Exchange. Instead, you must also configure the ExchangeArchivingPolicy property on each of the relevant Lync Server user accounts. This property can be set to one of four possible values:

1. Uninitialized. Indicates that archiving will be based on the In-Place Hold settings configured for the user's Exchange mailbox; if In-Place Hold has not been enabled on the user's mailbox then the user will have his or her messaging and Web conferencing transcripts archived in Lync Server.
2. **UseLyncArchivingPolicy**. Indicates that the user's instant messaging and Web conferencing transcripts should be archived in Lync Server rather than in Exchange.
3. **NoArchiving**. Indicates that the user's instant messaging and Web conferencing transcripts should not be archived at all. Note that this setting overrides any Lync Server archiving policies assigned to the user.
4. **ArchivingToExchange**. Indicates that the user's instant messaging and Web conferencing transcripts should be archived to Exchange regardless of the In-Place Hold settings that have (or have not) been assigned to the user's mailbox.

For example, to configure a user account so that instant messaging and Web conferencing transcripts are always archived to Exchange you can use a command similar to this from the Lync Server Management Shell:

```
Set-CsUser -Identity "Ken Myer" -ExchangeArchivingPolicy ArchivingToExchange
```

If you want to set the same archiving policy for a group of users (for example, all the users homed on a specified Registrar pool) you can use a command similar to this:

```
Get-CsUser -Filter {RegistrarPool -eq "atl-cs-001.litwareinc.com"} | Set-CsUser -
```

Note that you must use the Lync Server Management Shell (and Windows PowerShell) in order to configure value of the ExchangeArchivingPolicy property. This property is not exposed to administrators in the Lync Server Control Panel.

If you would like to view a list of all the users who have been assigned a specific archiving policy then you can use a command similar to the following, which returns the Active Directory display name of all the users who have had the ExchangeArchivingPolicy property set to Uninitialized:

```
Get-CsUser | Where-Object {$_.ExchangeArchivingPolicy -eq "Uninitialized"} | Sele
```

Likewise, this command returns the display name of the users who have not have the ExchangeArchivingPolicy property set to UseLyncArchivingPolicy:

```
Get-CsUser | Where-Object {$_.ExchangeArchivingPolicy -ne "UseLyncArchivingPolicy
```

1.4.17.4 Configuring Microsoft SharePoint Server 2013 to Search for Archived Microsoft Lync Server 2013 Data

Configuring Microsoft SharePoint Server 2013 to Search for Archived Microsoft Lync Server 2013 Data

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2013-02-04*

One of the major advantages to storing instant messaging and Web conferencing transcripts in Microsoft Exchange Server 2013 instead of Microsoft Lync Server 2013 is the fact that storing data in the same location enables administrators to use a single tool to search for archived Exchange data and/or archived Lync Server data. Because all the data is stored in the same place (Exchange) any tool that can search for archived Exchange data can also search for archived Lync Server data.

One tool that makes it easy to search for archived data is Microsoft SharePoint Server 2013. If you would like to use SharePoint to search for Lync Server data, you must first complete all the steps involved in configuring Exchange archiving in Lync Server. After Exchange 2013 and Lync Server 2013 have been successfully integrated you must then install the Exchange Web Services Managed API Version 2.0 on your SharePoint Server; the setup program for that API can be downloaded from the Microsoft Downloads Center (http://go.microsoft.com/fwlink/p/?LinkId=258305). The downloaded file (EWSManagedAPI.msi) can be saved to any folder on your SharePoint server.

After the file has been downloaded complete the following procedure on the SharePoint server:

1. Open a command window by clicking **Start**, clicking **All Programs**, clicking **Accessories**, right-clicking **Command Prompt**, and then clicking **Run as administrator**.
2. In the command window, use the **cd** command to change the current directory to the folder where the file EWSManagedAPI.msi has been saved. For example, if you have saved the file to C:\Downloads type the following command in the command window and then press ENTER:
   ```
   cd C:\Downloads
   ```
3. To install the API, type the following command then press ENTER:
   ```
   msiexec /I EwsManagedApi.msi addlocal="ExchangeWebServicesApi_Feature,
   ```
4. After the API has been installed, reset IIS by typing the following command and pressing ENTER:
   ```
   iisreset
   ```

After Exchange Web Services has been installed you must then configure server-to-server authentication between SharePoint Server 2013 and Exchange 2013. To do this, first open the SharePoint 2013 Management Shell and run the following set of command:

```
New-SPTrustedSecurityTokenIssuer -Name "Exchange" -MetadataEndPoint "https://auto
$service = Get-SPSecurityTokenServiceConfig
$service.HybridStsSelectionEnabled = $True
$service.AllowMetadataOverHttp = $False
$service.AllowOAuthOverHttp = $False
$service.Update()
```

Note:

Be sure and use the URI for your autodiscover service. Do not use the sample URI https://autodiscover.litwareinc.com/autodiscover/metadata/json/1.

After you have created the token issuer and configured the token service, run these commands, making sure to substitute the URL of your SharePoint site for the sample URL http://atl-sharepoint-001:

```
$exchange = Get-SPTrustedSecurityTokenIssuer "Exchange"
$app = Get-SPAppPrincipal -Site "https://atl-sharepoint-001" -NameIdentifier $exc
$site = Get-SPSite  "https://atl-sharepoint-001"
Set-SPAppPrincipalPermission -AppPrincipal $app -Site $site.RootWeb -Scope "SiteS
```

To configure server-to-server authentication for Exchange 2013, open the Exchange Management Shell and run a command similar to this (assuming that Exchange has been installed on drive C: and that it uses the default folder path):

```
"C:\Program Files\Microsoft\Exchange Server\V15\Scripts\Configure-EnterprisePartn
```

After configuring the partner application it is recommended that you stop and restart Internet Information Services (IIS) on all your Exchange mailbox and client access servers. You can restart IIS by using a command similar to this, which restarts the service on the computer atl-exchange-001:

```
iisreset atl-exchange-001
```

This command can be run from within the Exchange Management Shell or from any other command window.

Next, run a command similar to the following, which gives the specified user (in this example, kenmyer) the right to do discovery on Exchange:

```
Add-RoleGroupMember "Discovery Management" -Member "kenmyer"
```

After server-to-server authentication has been established between Exchange and SharePoint your next step is to create an eDiscovery site in SharePoint. That can be done by running commands similar to these from the SharePoint Management Shell:

```
$template = Get-SPWebTemplate | Where-Object {$_.Title -eq "eDiscovery Center"}
New-SPSite -Url "https://atl-sharepoint-001/sites/discovery" -OwnerAlias "kenmyer
```

Note:

"eDiscovery" is short for "electronic discovery," and typically refers to the process of looking through electronic archives for items that can be "reasonably calculated to lead to admissible evidence" in a court of law.

When the new site is ready, the next step is to configure Exchange 2013 to act as a result source for SharePoint. You can do that by completing the following procedure from the SharePoint 2013 Central Administration page:

1. On the Central Administration page click **Manage Service Applications** and then click **Search Service Application**.
2. On the Search Service Application: Search Administration page click **Result Sources** and then click **New Result Source**.
3. In the **New Result Source** pane enter a name for the new result source (for example, **Microsoft Exchange**) in the **Name** box. Select **Exchange** as the result source **Protocol**, and then enter the web services source URL for your Exchange server in the **Exchange Source URL** box. The source URL should look similar to this: https://atl-exchange-001.litwareinc.com/ews/exchange.asmx
4. Make sure that **Use Autodiscover** is not selected, and then click **OK**.

Finally, create a new eDiscovery case and a new eDiscovery set by completing the following procedure from the SharePoint Discovery site (for example, https://atl-sharepoint-001/sites/discovery):

1. On the Site Contents page click **Create a new case**.
2. On the Site Contents: New SharePoint Site page, enter the user's email alias (for example, **kenmyer**) in the **Title** box, then add that same URL to the **Web Site Address** box. That will result in a URL similar to this: https://atl-sharepoint-001/sites/eDiscovery/kenmyer
3. Click **Create**.
4. When the eDiscovery set page appears, click **new item** under **Identity and Preserve: Discovery Sets**.
5. On the New: Discovery Set page, enter the user's email alias in the **Discovery Set Name** box. Enter **eDiscovery Lync*** in the **Filter** box and then click **Add & Manage Sources**.
6. On the Add & Manage Sources page, enter the user's email alias in the first textbox under **Mailboxes**. Click the check mailbox icon located next to the textbook to verify that SharePoint can connect to the specified mailbox.
7. Click **OK**.
8. On the eDiscovery set page, click **Save** to save the new eDiscovery set.

At this point you can search the specified mailbox (kenmyer) and/or enable In-Place holds the same way you would for any other SharePoint content or result source.

1.4.17.5 Configuring Microsoft Lync Server 2013 to Use the Unified Contact Store

Configuring Microsoft Lync Server 2013 to Use the Unified Contact Store

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2013-01-16*

The unified contact store enables users to maintain a single contacts list and then have those contacts available in multiple applications, including Microsoft Lync 2013, Microsoft Outlook 2013, and Microsoft Outlook Web App 2013. When you enable the unified contact store for a user that user's contacts are not stored in Microsoft Lync Server 2013 and then retrieved using the SIP protocol. Instead, his or her contacts are stored in Microsoft Exchange Server 2013 and are retrieved by using Exchange Web Services.

Note:

Technically, contact information is stored in a pair of folders found in the user's Exchange 2013 mailbox. The contacts themselves are stored in a folder named Lync Contacts which is visible to end users; metadata about the contacts are stored in a subfolder that is not visible to end users.

Enabling the Unified Contact Store for a User

If you have already configured server-to-server authentication between Lync Server 2013 and Exchange 2013 then you have also enabled the use of the unified contact store; no additional server configuration is required. However, additional user account configuration is required in order to move a user's contacts into the unified contact store. By default, user contacts are kept in Lync Server and not in the unified contact store.

Access to the unified contact store is managed by using Lync Server user services policies.

User server policies have only a single property (UcsAllowed); this property is used to determine the location where a user's contacts are stored. If a user is managed by a user services policy where UcsAllowed has been set to True ($True) then the user's contacts will be stored in in the unified contact store. If the user is managed by a user services policy where UcsAllowed has been set to False ($False) then his or her contacts will be stored in Lync Server.

When you install Lync Server 2013 a single user services policy (configured at the global scope) is installed as well. The UcsAllowed value in this policy is set to True, meaning that, by default, user contacts will be stored in the unified contact store (assuming this has been deployed and configured). If you want to migrate all of your user contacts to the unified contact store you do not have to do anything at all.

If you would prefer not to migrate all your contacts to the unified contact store you can disable the unified contact store for all users by setting the UcsAllowed property in the global policy to False:

```
Set-CsUserServicesPolicy -Identity global -UcsAllowed $False
```

After you have disabled the unified contact store in the global policy you can then create a per-user policy that enables the use of the unified contact store; this allows you to have some users keep their contacts in the unified contact store while other users continue to keep their contacts in Lync Server. You can create a per-user user services policy by using a command similar to this:

```
New-CsUserServicesPolicy -Identity "AllowUnifiedContactStore" -UcsAllowed $True
```

After you have created the new policy you must then assign that policy to any user who should have access to the unified contact store. Per-user policies can be assigned to users by using commands similar to this:

```
Grant-CsUserServicesPolicy -Identity "Ken Myer" -PolicyName "AllowUnifiedContactS
```

After the policy has been assigned Lync Server will begin to migrate the user's contacts to the unified contact store. After migration is complete, the user will then have his or her contacts stored in Exchange rather than Lync Server. If the user happens to be logged on to Lync 2013 at the time migration completes, a message box will appear and he or she will be asked to log off of Lync and then log back on in order to finalize the process. Users who have not been assigned this per-user policy will not have their contacts migrated to the unified contact store. That’s because those users are being managed by the global policy, and use of the unified contact store has been disabled in the global policy.

You can verify that a user's contacts have successfully been migrated to the unified contact store by running the Test-CsUnifiedContactStore cmdlet from within the Lync Server Management Shell:

```
Test-CsUnifiedContactStore -UserSipAddress "sip:kenmyer@litwareinc.com" -TargetFq
```

If Test-CsUnifiedContactStore succeeds that means that the contacts for the user sip:kenmyer@litwareinc.com have been migrated to the unified contact store.

Rolling Back the Unified Contact Store

If you need to remove a user's contacts from the unified contact store (for example, if the user needs to be rehomed on Microsoft Lync Server 2010 and thus can no longer use the unified contact store) you must do two things. First, you must assign the user a new user services policy, one that prohibits storing contacts in the unified contact store. (That is, a policy where the UcsAllowed property has been set to $False.) If you do not have such a policy you can create one using a command similar to this:

```
New-CsUserServicesPolicy -Identity NoUnifiedContactStore -UcsAllowed $False
```

You can then assign this new per-user policy (NoUnifiedContactStore) by using a command like this:

```
Grant-CsUserServicesPolicy -Identity "Ken Myer" -PolicyName NoUnifiedContactStore
```

The preceding command assigns the new policy to the user Ken Myer, and also prevents Ken's contacts from being migrated to the unified contact store.

Note:

In some cases you can achieve the same net effect by simply unassigning the user's current user services policy. For example, suppose Ken Myer has a per-user user services policy the enables the unified contact store, but your global policy prohibits the use of the unified contact store. In that case, you could unassign Ken's per-user services policy. When you do that, Ken will automatically be managed by the global policy, and thus will no longer have access to the unified contact store.
To unassign a previously-assigned per-user policy, use the same command as shown before, but this time set the PolicyName parameter to a null value:
Grant-CsUserServicesPolicy –Identity "Ken Myer" –PolicyName $Null

The terminology "prevents Ken's contacts from being migrated to the unified contact store" is important to keep in mind when working with the unified contact store. Simply assigning Ken a new user services policy will not move his contacts out of the unified contact store. When a user logs on to Lync Server 2013, the system checks the user's user services policy to see whether his or her contacts should be kept in the unified contact store. If the answer is yes (that is, if the UcsAllowed property is set to $True) then those contacts will be migrated to the unified contact store (assuming that those contacts are not already in the unified contact store). If the answer is no, then Lync Server simply ignores the user's contacts and moves on to its next task. That means that Lync Server will not automatically move a user's contacts from out of the unified contact store, regardless of the value of the UcsAllowed property.

That also means that, after assigning the user a new user services policy, you must then run the Invoke-CsUcsRollback cmdlet in order to move the user's contacts out of Exchange 2013 and back to Lync Server 2013. For example, after assigning Ken Myer a new user services policy you can then move his contacts out of the unified contact store by using the following command:

```
Invoke-CsUcsRollback -Identity "Ken Myer"
```

If you change the user services policy but do not run the Invoke-CsUcsRollback cmdlet Ken's contacts will not be removed from the unified contact store. What if you run Invoke-CsUcsRollback but do not change Ken Myer's user services policy? In that case, Ken's contacts will be temporarily removed from the unified contact store. The fact that this removal is temporary is important to keep in mind. After Ken's contacts have been removed from the unified contact store, Lync Server 2013 will wait 7 days and then check to see which user services policy has been assigned to Ken. If Ken is still assigned a policy that enables the user of the unified contact store, then his contacts will automatically be moved back to into the contact store. To permanently remove contacts from the unified contact store you must change the user services policy in addition to running the Invoke-CsUcsRollback cmdlet.

1.4.17.6 Configuring the Use of High-Resolution Photos in Microsoft Lync Server 2013

Configuring the Use of High-Resolution Photos in Microsoft Lync Server 2013

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2012-10-22*

Microsoft Lync Server 2010 provided the ability for users to view photos of their contacts (and to make their own photos available to others). Typically these photos were stored as part of the user's thumbnailPhoto attribute in Active Directory. That placed a serious limitation on the size and resolution of the photos: the thumbnailPhoto attribute can only hold a photograph with a maximum size of 48 pixels by 48 pixels.

In Microsoft Lync Server 2013, however, photos can be stored in a user's Microsoft Exchange Server 2013 mailbox; that allows for photo sizes up to 648 pixels by 648 pixels. In addition to that, Exchange 2013 can automatically resize these photos for use in different products as needed. Typically that means three different photo sizes and resolutions:

- 48 pixels by 48 pixels, the size used for the Active Directory thumbnailPhoto attribute. If you upload a photo to Exchange 2013 Exchange will automatically create a 48 pixel by 48 pixel version of that photo and update the user's thumbnailPhoto attribute. Note, however, that the reverse is not true: if you manually update the thumbnailPhoto attribute in Active Directory the photo in the user's Exchange 2013 mailbox will not automatically be updated.
- 96 pixels by 96 pixels, for use in Microsoft Outlook 2013 Web App, Microsoft Outlook 2013, Microsoft Lync Web App, and Lync 2013.
- 648 pixels by 648 pixels for use in Lync 2013 and Microsoft Lync Web App.

Note:

If you have the resources, it is recommended that you upload 648x648 photos; that provides the maximum resolution and optimal picture quality in any of the Office 2013 applications. Each JPEG photo with a size of 648x648 and a depth of 24 bits results in a file size of approximately 240 kilobytes. That means you will need approximately 1 megabyte of disk space for every 4 user photos.

High-resolution photos, which are accessed by using Exchange Web Services, can be uploaded by users who are running Outlook 2013 Web App; users are only allowed to update their own photo. Administrators, however, can update the photo for any user by using the Exchange Management Shell and a series of Windows PowerShell commands similar to the following:

```
$photo = ([Byte]] $(Get-Content -Path "C:\Photos\Kenmyer.jpg" -Encoding Byte -Rea
Set-UserPhoto -Identity "Ken Myer" -PictureData $photo -Confirm:False
Set-UserPhoto -Identity "Ken Myer" -Save -Confirm:False
```

The first command in the preceding example uses the Get-Content cmdlet to read the contents of the file C:\Photos\Kenmyer.jpg and store that data in a variable named $photo. In the second command, the Exchange cmdlet Set-UserPhoto is used to upload the photo and attach that photo to Ken Myer's user account.

Note:

In this example, Ken Myer's Active Directory display name is used as the user account Identity. You can also reference a user account by using other identifiers such as the user's SMTP address or his or her User Principal Name. See the documentation for the Set-UserPhoto cmdlet at http://go.microsoft.com/fwlink/p/?LinkId=268536 for more information

Uploading the photo does not equate to assigning that photo to Ken Myer's user account. Instead, uploading the photo simply results in a preview of that photo to be displayed on the Outlook Web App Options page. To actually assign that photo to the user account the user must click **Save** on the Options page or the administrator must execute the third command in the example. That third command uses the Save parameter to assign the photo to Ken Myer's user account:

```
Set-UserPhoto -Identity "Ken Myer" -Save -Confirm:False
```

To verify that the new photo has been assigned to the user account, Ken Myer can log on to Lync 2013, select **Options**, and then select **My Picture**. The newly-uploaded photo should be displayed as Ken's personal photo. Alternatively, administrators can verify the photo for any user by starting Internet Explorer and navigating to a URL similar to this:

```
https://atl-mail-001.litwareinc.com/ews/Exchange.asmx/s/GetUserPhoto?email=kenmye
```

If the administrator can view the photo using Internet Explorer but the user cannot view his or her photo in Lync 2013, that typically indicates a connectivity problem with Exchange Web Services or with the Exchange autodiscover service.

1.4.17.7 Configuring Microsoft Exchange Server 2013 Unified Messaging for Microsoft Lync Server 2013 Voicemail

Configuring Microsoft Exchange Server 2013 Unified Messaging for Microsoft Lync Server 2013 Voicemail

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2013-02-04*

Microsoft Lync Server 2013 enables you to have voicemail messages stored in Microsoft Exchange Server 2013; those voicemail messages will then appear as email messages in your users' Inboxes. This capability was also found in the 2010 editions of Lync Server and Exchange; however, the process of configuring this "unified messaging" has been simplified in in the 2013 editions thanks to the introduction of the UM Call Router component. This component is installed on the Exchange 2013 Client Access server, and all calls to Exchange unified messaging (such as a voicemail) are first routed through the Call Router and then are redirected to the appropriate Mailbox server.

If you have already configured server-to-server authentication between Lync Server 2013 and Exchange 2013 then you are ready to setup unified messaging. To do so, you must first create and assign a new unified messaging dial plan on your Exchange server. For example, these two commands (run from within the Exchange Management Shell) configure a new 3-digit dial plan for Exchange:

```
New-UMDialPlan -Name "RedmondDialPlan" -VoIPSecurity "Secured" -NumberOfDigitsInE
Set-UMDialPlan "RedmondDialPlan" -ConfiguredInCountryOrRegionGroups "Anywhere,*,*
```

In the first command in the example, the VoIPSecurity parameter, and the parameter value "Secured" indicate that the signaling channel is encrypted by using Transport Layer Security (TLS). The URIType "SipName" indicates that messages will be sent and received using the SIP protocol, and the CountryOrRegionCode of 1 indicates that the dial plan applies to the US.

In the second command, the parameter value passed to the ConfiguredInCountryOrRegionGroups parameter specifies the in-country groups that can be used with this dial plan. The parameter value "Anywhere,*,*,*" sets the following:

- Group name ("Anywhere")
- AllowedNumberString (*, a wildcard character indicating that any number string is allowed)

- DialNumberString (*, a wildcard character indicating that any dialed number is allowed)
- TextComment (*, a wildcard character indicating that any text command is allowed)

Note:

Creating a new dial plan will also create a Default Mailbox Policy.

After creating and configuring the new dial plan you must add the new dial plan to your unified messaging server and then modify the startup mode of that server; in particular, you must set the startup mode to "Dual". You can perform both of these tasks from within the Exchange Management Shell:

```
Set-UmService -Identity "atl-exchangeum-001.litwareinc.com" -DialPlans "RedmondDi
```

After the unified messaging server has been configured you should next run the Enable-ExchangeCertificate cmdlet to ensure that your Exchange certificate is applied to the unified messaging service:

```
Enable-ExchangeCertificate -Server "atl-umserver-001.litwareinc.com" -Thumbprint
```

After the certificate has been correctly assigned you must then stop and restart the MsExchangeUM service on the unified messaging server. This service must be stopped and restarted any time you change the startup mode.

After finishing configuration of the unified messaging server you can then configure the UM Call Router:

```
Set-UMCallRouterSettings -Server "atl-exchange-001.litwareinc.com" -UMStartupMode
Enable-ExchangeCertificate -Server "atl-umserver-001.litwareinc.com" -Thumbprint
```

Because the startup mode has changed you must stop and restart the MsExchangeUMCR service on the computer hosting the UM Call Router.

To complete the unified messaging setup, you then need to create a UM mailbox policy and then use that policy to enable users for unified messaging. You can create a mailbox policy by using a command similar to this:

```
New-UMMailboxPolicy -Name "RedmondMailboxPolicy" -AllowedInCountryOrRegionGroups
```

And you can enable a user for unified messaging by using a command similar to this:

```
Enable-UMMailbox -Extensions 100 -SIPResourceIdentifier "kenmyer@litwareinc.com"
```

In the preceding command, the Extensions parameter represents the telephone extension number for the user. In this example, the user has the extension number 100.

After you have enabled his mailbox, the user kenmyer@litwareinc.com should be able to use Exchange unified messaging. You can verify that the user can connect to Exchange UM by running the Test-CsExUMConnectivity cmdlet from within the Lync Server Management Shell:

```
$credential = Get-Credential "litwareinc\kenmyer"
Test-CsExUMConnectivity -TargetFqdn "atl-cs-001.litwareinc.com" -UserSipAddress "
```

If you have a second user who has been enabled for unified messaging you can use the Test-CsExUMVoiceMail cmdlet to verify that this second user can leave a voicemail message for the first user.

```
$credential = Get-Credential "litwareinc\pilar"
Test-CsExUMVoiceMail -TargetFqdn "atl-cs-001.litwareinc.com" -ReceiverSipAddress
```

1.4.17.8 Integrating Microsoft Lync Server 2013 and Microsoft Outlook Web App 2013

Integrating Microsoft Lync Server 2013 and Microsoft Outlook Web App 2013

Planning > Planning for Exchange Server Integration > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2013-02-03*

In addition to integrating with Microsoft Outlook 2013, Microsoft Lync Server 2013 can be fully integrated with Microsoft Outlook Web App 2013; among other things, this adds instant messaging and presence to Outlook Web App, and enables your unified contact list to be shared between Outlook Web App and Microsoft Lync 2013. In order to integrate Lync Server 2013 and Outlook Web App, you must first verify that the Unified Communications Managed API 4.0 Runtime has installed in your Microsoft Exchange Server 2013 backend server. You can do this by looking for the existence of the following registry value:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA \InstantMessaging\ImplementationDLLPath

The ImplementationDLLPath should point to the folder location for the file Microsoft.Rtc.Internal.Ucweb.dll. If it does not, or if the registry value does not exist, then you should download and install the UCMA Runtime setup program from the Microsoft Download Center at http://www.microsoft.com/en-us/download/details.aspx?id=34992. Information on how to install the UCMA Runtime can be found on that same web page.

Backward Compatibility

Lync Server 2013 can be integrated with the Microsoft Exchange Server 2010 versions of both unified messaging and Outlook Web App. For more information, see the article Deploying On-Premises Exchange UM to Provide Lync Server 2010 Voice Mail at http://technet.microsoft.com/en-us/library/gg398768.aspx. If you integrate with Exchange 2010 you will not have Lync Server specific features such as the unified contact store and Lync-to-Exchange archiving.

Microsoft Lync 2013 can also be used in conjunction with Exchange 2010 and Outlook 2010. Once again, however, new functionality such as the unified contact store and high-resolution photos will not be available to Lync 2013 users. These new capabilities require both Lync Server 2013 and Exchange 2013.

Creating a Trusted Application Pool for Outlook Web App

If you have installed the Microsoft Exchange Unified Messaging Call Router service and the Microsoft Exchange Unified Messaging service on the same computer then there is no need to create a trusted application pool for Outlook Web App. (This assumes that the server in question is hosting a SipName UM dial plan.) If you are using a single computer to host both of these services then you can skip to the section of this document titled **Enabling Instant Messaging on Outlook Web App**.

Lync Server 2013 can autodiscover any Exchange servers that host a SipName UM dial plan; these servers are automatically added to the Lync Server Known Servers List. There is no need to create a trusted application pool and add these servers to the Known Servers List. In fact, doing so will cause Outlook Web App integration to stop working.

Note:

This is due to the fact that the Lync Server topology will now have two entries for the same computer: the autodiscovered entry, and the manually-added entry. To fix the problem, and to get Outlook Web App working again, use Windows PowerShell to remove the trusted pool and trusted application entries for the server. See the help topics for the Remove-CsTrustedApplicationPool and Remove-CsTrustedApplication cmdlets for more information.

If these two services are running on separate computers then, after you have verified that the Unified Communications Managed API 4.0 Runtime has been installed, you must create a Lync Server trusted application pool and a trusted application associated with Outlook Web App; that will add the server to the Known Servers List. To do that, first run a command similar to this from within the Lync Server Management Shell:

```
New-CsTrustedApplicationPool -Identity atl-owa-001.litwareinc.com -Registrar atl-
```

In the preceding command, atl-owa-001.litwareinc.com is the fully qualified domain name of the Outlook Web App pool; this must be the same name that appears in the Subject Name and Subject Alternative Name (SAN) fields of the certificate that provides access to Outlook Web App. Likewise, atl-cs-001.litwareinc.com is the fully qualified domain name of the Lync Server 2013 pool that will host the new trusted application pool. Note, too that the specified site, Redmond, represents the SiteID of the Lync Server site. The SiteID is not necessarily the same as the site's DisplayName; you can retrieve SiteIDs for your Lync Server sites by running the following command from the Lync Server Management Shell:

```
Get-CsSite | Select-Object DisplayName, SiteID
```

After creating the trusted application pool, use a command similar to the following to configure an application Identity and a port for Outlook Web App:

```
New-CsTrustedApplication -ApplicationId OutlookWebApp -TrustedApplicationPoolFqdn
```

In the preceding command, the ApplicationID is simply a friendly identifier used to distinguish trusted applications. The ApplicationID can be any text string that does not include blank spaces or other prohibited characters. (To ensure that you create a valid identifier, it is recommended that you use only letters and numbers when specifying an ApplicationId.) The value assigned to the Port parameter is also left to the administrator's discretion: this can be any available network port.

After creating the trusted application you must run the following command to enable the changes to your Lync Server topology:

```
Enable-CsTopology
```

Note that you must also add your Exchange client access and mailbox server to all of your SIP Uri dial plans. In turn, this will configure the servers as trusted SIP peers with the ExUmRouting topology for Lync Server.

Enabling Instant Messaging on Outlook Web App

With Lync Server correctly configured you can then begin to configure Outlook Web App. The first step in that process is to enable instant messaging on all your Outlook Web App virtual directories on your front end servers. (There is no need to enable instant messaging for the virtual directories on your backend servers. In fact, it is recommended that you do not enable instant messaging on your backend servers.) Instant messaging can be enabled on the client access servers by running the following command from within the Exchange Management Shell:

```
Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -InstantMessagingEnabled $True
```

Note:

By default, instant messaging is enabled when you install Outlook Web App; that is, the InstantMessagingEnabled property is set to True. However, you must still run the preceding command in order to set the instant messaging type to OCS. By default, InstantMessagingType is set to None.

Next you must add the following two lines to Outlook Web App Web.config file (this file is typically located in the folder C:\Program Files\Microsoft\Exchange Server\V15 \ClientAccess\Owa). These two lines should be added under the <AppSettings> node in the Web.config file, and this procedure should be carried out only on the backend servers where Outlook Web App has been installed:

```
<add key="IMCertificateThumbprint" value="EA5A332496CC05DA69B75B66111C0F78A110D22
<add key="IMServerName" value="atl-cs-001.litwareinc.com"/>
```

In the preceding example, the value for IMCertificateThumbprint must be the thumbprint for the Exchange 2013 certificate that is installed on your backend servers. You can retrieve that information by running the following command from the Exchange Management Shell:

```
Get-ExchangeCertificate
```

Note, too that the value assigned to IMServerName is the fully qualified domain name of the Lync Server pool where you created the trusted application pool for Outlook Web App.

The certificate that you use for Outlook Web App must be a certificate that is trusted by Lync Server. One way to ensure that the certificate will be trusted by both Lync Server and Exchange is to use your internal certificate authority to create a certificate on the mailbox server, making sure that the server FQDN is used for the subject name and that this FQDN appears in the certificate alternate name field. After the certificate has been created it can then be imported to your backend servers. The net result is that the same certificate is used for two purposes: 1) communication between Exchange unified messaging and Lync Server; and, 2) the integration between Outlook Web App and Lync Server.

After you have updated the Web.config file you should then run the following command on the Exchange backend server in order to recycle the Outlook Web App pool:

```
C:\Windows\System32\Inetsrv\Appcmd.exe recycle apppool /apppool.name:"MSExchangeO
```

If the recycle operation succeeds you will see the following message in the Exchange Management Shell:

```
"MSExchangeOWAAppPool" successfully recycled
```

Configuring Outlook Web App Mailbox Policies

At this point you can use the following command to configure instant messaging on the appropriate Outlook Web App mailbox policy (or policies). For example, this command, run on one of your mailbox servers, enables instant messaging on the Default policy:

```
Set-OwaMailboxPolicy -Identity "Default" -InstantMessagingEnabled $True -InstantM
```

And this command enables instant messaging for all your Outlook Web App mailbox policies:

```
Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -InstantMessagingEnabled $True -Insta
```

After the mailbox policy has been enabled then all users managed by that policy will have full integration between Lync Server and Outlook Web App, provided that:

- The user has a mailbox on Exchange 2013.
- The user has been enabled for Lync Server 2013.
- The user has a valid SIP proxy address.

Disabling Instant Messaging in Outlook Web App

As noted previously, instant messaging is enabled by default in Outlook Web App. That means that, if you do not integrate Outlook Web App with Lync Server, users will see blank presence icons and an error message each time they log on to Outlook Web App. To prevent this problem, use the following Exchange Management Shell command to disable instant messaging in Outlook web App:

```
Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -InstantMessagingEnabled $False
```

Verifying Integration With Outlook Web App

To verify that instant messaging and presence have been integrated with Outlook Web App, sign on to Outlook Web App 2013. In the upper right-hand corner of the screen, you will see your Exchange display name. If there is a presence icon next to your name (for example, a green icon indicating that your current status is Available) that indicates that you have successfully integrated Lync Server and Outlook Web App.

After the initial sign-on to Outlook Web App, check to see if an event with the Event ID 112 (and the source MSExchange OWA) has been written to the event log on the mailbox server. This event indicates that the Instant Messaging Endpoint Manager was successfully initialized. If instant messaging does not appear to be working then, on the mailbox server, look for log files in the folder C:\Program Files\Microsoft\Exchange server \V15\Logging\OWA\InstantMessaging. If either the Logging or the InstantMessaging folders do not exist that indicates that integration has failed. In that case, you can use SIPStack tracing on Lync Server (All Levels and All Flags) to try and determine why integration failed.

1.4.17.9 Configuring the Personal Contacts Store on Client Computers

Configuring the Personal Contacts Store on Client Computers

Microsoft Lync Server 2013 > Deployment > Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 >

Topic Last Modified: *2012-10-10*

If you are integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 then it is recommended that you configure the Lync personal contact store on all your client computers; in particular, you should configure Lync to use Exchange as the personal contact store, and, at the same time, ensure that users are not able to override that decision. This can be done by creating and configuring a Registry value on each client computer.

To configure this value on a single computer, complete the following procedure:

1. On the client computer, click Start and then click Run.
2. In the Run dialog box, type regedit and then press ENTER.
3. In Registry Editor, expand HKEY_LOCAL_MACHINE, expand Software, expand Policies, and then expand Microsoft.
4. Right-click Communicator, point to New, and then click DWORD (32-bit) Value.
5. After the new value is created, type PersonalContactStoreOverride and then press ENTER to rename the value.
6. Verify that the value of PersonalContactStoreOverride is set to 0 and then close Registry Editor.

If you need to make this same change on multiple computers you can do so by creating a custom Group Policy object. For details, see the Group Policy documentation at http://go.microsoft.com/fwlink/p/?LinkId=268543.

1.5 Lync Server 2013 Hybrid

Lync Server 2013 Hybrid

Microsoft Lync Server 2013 >

Topic Last Modified: *2013-02-18*

This section describes hybrid configurations for Lync Server 2013, including hybrid Lync Server 2013 deployments and Hybrid Voice deployments.

Overview of Hybrid Deployments

Planning for Hybrid Deployments

Configuring Hybrid Deployments

1.5.1 Overview of Hybrid Deployments

Overview of Hybrid Deployments

Microsoft Lync Server 2013 > Lync Server 2013 Hybrid >

Topic Last Modified: *2013-02-18*

A hybrid deployment is a deployment in which some users are homed on-premises and some users are homed online, but the users share the same domain, such as contoso.com. In Lync Server 2013, you can configure two types of hybrid deployments.

- **Hybrid Lync Server** An on-premises Lync Server configured for hybrid with Lync Online.
- **Hybrid Voice** On-premises Lync Server configured for hybrid with Hosted Voice services.

You can configure your on-premises deployment for hybrid with Lync Online, by using Active Directory Synchronization to keep your on-premises and online users synchronized. You can also configure hybrid deployments for integration with other Microsoft Office 365 applications, including Exchange Online and SharePoint Online. This section guides you through deploying the applications required for a Lync Server hybrid deployment, and then configuring your deployment to enable it.

About Hybrid Deployments

For information about configuring your on-premises Lync Server deployment for hybrid with Lync Online or for Hybrid Voice, see the following topics:

Planning for Hybrid Deployments

Configuring Hybrid Deployments

For more information about Lync Online, see Lync Online at http://go.microsoft.com/fwlink/p/?LinkId=282396.

1.5.2 Planning for Hybrid Deployments

Planning for Hybrid Deployments

Microsoft Lync Server 2013 > Lync Server 2013 Hybrid >

Topic Last Modified: *2013-02-19*

This section provides information about planning for hybrid deployments.

- Planning for Lync Server 2013 Hybrid Deployments
- Supported Lync Server 2013 Hybrid Configurations
- Planning for Hybrid Voice

1.5.2.1 Planning for Hybrid Deployments

Planning for Lync Server 2013 Hybrid Deployments

Microsoft Lync Server 2013 > Lync Server 2013 Hybrid > Planning for Hybrid Deployments >

Topic Last Modified: *2013-02-22*

You should consider the following requirements for users and your network infrastructure while planning for a hybrid deployment.

Requirements

You must have the following available in your environment in order to implement and configure a Lync Server 2013 hybrid deployment.

- An Office 365 tenant running Lync Online 2013.
- An Active Directory Federation Services (AD FS) Server running Windows 2008 R2 SP1 or the latest service pack. For additional system requirements for AD FS, see Active Directory Federation Services 2.0 at http://go.microsoft.com/fwlink/p/?LinkId=151338.
- Lync Server 2013 on-premises deployment.
- A Directory Synchronization server. For details about Directory Synchronization, see Directory Synchronization Tool at http://go.microsoft.com/fwlink/p/?LinkID=231010.

Lync Client Support

There are some differences in the features supported in Lync clients, as well as the features available in on-premises and online environments. Before you decide where you want to home users in your organization, you can view the client support for the various configurations of Lync Server. For details about client support, see the following topics:

- Lync Online client comparison tables at http://go.microsoft.com/fwlink/p/?LinkId=281902.
- Client Comparison Tables
- Mobile Client Comparison Tables

Topology Requirements

To configure your Lync Server 2013 deployment for hybrid with Lync Online, you need to have one of the following supported topologies:

- Microsoft Office Communications Server 2007 R2 with Lync Server 2013 on-premises. The Lync Server 2013 federation Edge Server and the next hop server from the federation Edge Server must be running Lync Server 2013, and there must be a Central Management Store deployed. The Edge Server and pool must be deployed on-premises.

- Microsoft Lync Server 2010 with Lync Server 2013 on-premises. The federation Edge Server and next hop server from the federation Edge Server must be running either Lync Server 2013 or Microsoft Lync Server 2010 with the latest cumulative updates.

> **Important:**
> If a Lync Server 2013 Director is deployed and is the next hop for the Edge Server, the –ProxyPool parameter must be used with the **Move-CsUser** cmdlet to move users from on-premises to Lync Online. For details, see Move Users to Lync Online.

- A Lync Server 2013 deployment with all servers running Lync Server 2013.

For more information about supported topologies, see Supported Lync Server 2013 Topologies.

Requirements for Federation Allowed/ Blocked Lists

The Allowed domains list includes domains that have a partner Edge fully qualified domain name (FQDN) configured. These are sometimes referred to as *allowed partner servers* or *direct federation partners*. You should be familiar with the difference between Open Federation and Closed Federation, referred to as *partner discovery* and *allowed partner domain list*, respectively, in on-premises deployments.

The following requirements must be met to successfully configure a hybrid deployment:

- Domain matching must be configured the same for your on-premises deployment and your Office 365 tenant. If partner discovery is enabled on the on-premises deployment, then open federation must be configured for your online tenant. If partner discovery is not enabled, then closed federation must be configured for your online tenant.
- The Blocked domains list in the on-premises deployment must exactly match the Blocked domains list for your online tenant.
- The Allowed domains list in the on-premises deployment must exactly match the Allowed domains list for your online tenant.
- Federation must be enabled for the external communications for the online tenant, which is configured by using the Lync Online Control Panel.

DNS Settings

When creating DNS SRV records for hybrid deployments, the records, _sipfederationtls._tcp.<domain> and _sip._tls.<domain>, should point to the on-premises Access Proxy.

Firewall Considerations

Computers on your network must be able to perform standard Internet DNS lookups. If these computers can reach standard Internet sites, your network meets this requirement.

Depending on the location of your Microsoft Online Services data center, you must also configure your network firewall devices to accept connections based on wildcard domain names (for example, all traffic from *.outlook.com). If your organization’s firewalls do not support wildcard name configurations, you will have to manually determine the IP address ranges that you would like to allow and the specified ports.

Refer to the Help topic Office 365 URLs and IP address ranges at http://go.microsoft.com/fwlink/p/?LinkId=252942.

Port and Protocol Requirements

In addition to the port requirements for internal Lync Server 2013 communication, you must also configure the following ports.

Protocol / Port	Applications
TCP 443	Open inbound • Active Directory Federation Services (federation server role) For more information, see Understanding AD FS Role Services at http://go.microsoft.com/fwlink/p/?LinkId=281899. • Active Directory Federation Services (proxy server role) • Microsoft Online Services Portal • My Company Portal • Outlook Web App • Lync client (communication to Lync Online from on-premises Lync Server)
TCP 80 and 443	Open inbound • Microsoft Online Services Directory Synchronization Tool
TCP 5061	Open inbound/outbound on the Edge Server
PSOM/TLS 443	Open inbound/outbound for data sharing sessions
STUN/TCP 443	Open inbound/outbound for audio, video, application sharing sessions
STUN/UDP 3478	Open inbound/outbound for audio and video sessions
RTP/TCP 50000-59999	Open outbound for audio and video sessions

Note:

If you need to federate with partners running Office Communications Server 2007, you will need to open inbound/outbound RTP/UDP and RTP/TCP ports 50000-59999. For more information about A/V firewall requirements see, Determine External A/V Firewall and Port Requirements. For more information on ports and protocols, see Port Summary - Scaled Consolidated Edge with Hardware Load Balancers.

User Accounts and Data

In a Lync Server 2013 hybrid deployment, any user that you want to home in Lync Online must first be created in the on-premises deployment, so that the user account is created in Active Directory Domain Services (AD DS). You can then move the user to Lync Online, which will move the user’s contact list.

Important:

If the user is created by using the online portal for Office 365, the user account will not be synchronized with on-premises Active Directory, and the user will not exist in the on-premises Active Directory.

You should also consider the following user-related issues when planning for a hybrid deployment.

- **User contacts** The limit for contacts for Lync Online users is 250. Any contacts beyond that number will be removed from the user's contact list.
- **Instant Messaging and Presence** User contact lists, groups, and access control lists (ACLs) are migrated with the user account.
- **Conferencing data, meeting content, and scheduled meetings** This content is not migrated with the user account. Users must reschedule meetings after their accounts are migrated to Lync Online.

User Policies and Features

- In a Lync Server 2013 hybrid environment, users can be enabled for Instant Messaging, voice, and meetings either on-premises or online, but not both simultaneously.
- **Lync Client** Some users may require a new client version when they are moved to Lync Online. For Office Communications Server 2007 R2, users must be moved to a Lync Server 2013 pool prior to migration to Lync Online. For more information about client support, see Lync Online client comparison tables at http://go.microsoft.com/fwlink/p/?LinkId=281902 and Lync Client Requirements and Limitations at http://go.microsoft.com/fwlink/p/?LinkId=281901 .
- **Enterprise Voice** User level call routing capabilities are migrated.
- **On-premises policies and configuration (non-user)** Online and on-premises policies require separate configuration. You cannot set global policies that apply to both.

1.5.2.2 Supported Lync Server 2013 Hybrid Configurations

Supported Lync Server 2013 Hybrid Configurations

Microsoft Lync Server 2013 > Lync Server 2013 Hybrid > Planning for Hybrid Deployments >

Topic Last Modified: *2013-03-12*

You can configure Lync Server 2013 deployments for integration with Microsoft Exchange Server 2013 and SharePoint Server, both on-premises and online. The features listed in the following table are supported with all clients unless otherwise specified. For more information about client support, see Client Comparison Tables and Lync Online client comparison tables at http://go.microsoft.com/fwlink/p/?LinkId=281902.

Integration with Exchange Server

The following table lists the features supported in a Lync Server 2013 hybrid deployment when integrated with Exchange.

	Exchange on-premises	Exchange Online
Lync Server 2013 on-premises	• IM/Presence in Outlook For more information, see IM and Presence • Schedule and join online meetings through Outlook For more information, see Integrating	• IM/Presence in Outlook For more information, see Configuring On-premises Lync Server 2013 Integration with Exchange Online • Schedule and join online meeting

	Microsoft Lync Server 2013 and Microsoft Exchange Server 2013 • IM/Presence in Outlook Web App For more information, see Configuring Microsoft Lync Server 2013 in a Cross-Premises Environment • Schedule and join online meetings through Outlook Web App • IM/Presence in Mobile Clients • Join online meetings in Mobile clients For more information, see Deploying Mobility • Publish status based on Outlook calendar free/busy information • Contact List (via Unified Contact Store) For more information, see Configuring Microsoft Lync Server 2013 to Use the Unified Contact Store **Note:** Lync Server 2013 and Exchange only. A Lync 2013 client is required. • High-resolution Contact Photo in Lync 2013 client and Lync Web App. For more information, see Configuring the Use of High-Resolution Photos in Microsoft Lync Server 2013 **Note:** Lync Server 2013 only • Meeting delegation Supported only when both users are homed online in the same forest, or both are homed on-premises. • Missed Conversations history and Call Logs are written to user’s exchange mailbox • Archiving Content (IM	through Outlook • IM/Presence in OWA For more information, see Integrating Microsoft Lync Server 2013 and Microsoft Outlook Web App 2013 • Schedule and join online meeting from Outlook Web App For more information, see Integrating Microsoft Lync Server 2013 and Microsoft Outlook Web App 2013 • IM/Presence in Mobile Clients • Join online meeting in Mobile clients • Publish status based on Outlook calendar free/busy information • Contact List (via Unified Contact Store). For more information, see Configuring Microsoft Lync Server 2013 to Use the Unified Contact Store **Note:** Lync Server 2013 only. A Lync 2013 client is required. • High-resolution Contact Photo in Lync 2013 client and Lync Web App. For more information, see Configuring the Use of High-Resolution Photos in Microsoft Lync Server 2013. • Meeting delegation Supported only when both users are homed online in the same forest, or both are homed on-premises. • Missed Conversations history and Call Logs are written to user’s exchange mailbox • Archiving Content (IM and Meeting) in Exchange. For more information,

	and Meeting) in Exchange For more information, see Deployment Checklist for Archiving • Search archived content • Voice mail For more information, see Deploying On-Premises Exchange UM to Provide Lync Server 2013 Voice Mail	see Deployment Checklist for Archiving **Note:** Lync Server 2013 only • Search archived content. For more information, see Configure Exchange for SharePoint eDiscovery Center at http://go.microsoft.com/fwlink/p/?LinkId=285448 **Note:** Lync Server 2013 only • Voice mail. For more information, see Providing Lync Server 2013 Users Voice Mail on Hosted Exchange UM
Lync Online	• IM and Presence in Outlook • Schedule and join online meetings through Outlook • IM/Presence in Mobile clients • Missed Conversations history and Call Logs are written to user’s exchange mailbox • High-resolution Contact Photo in Lync 2013 client. **⚠Warning:** Not supported in Lync Web App when users are homed on Lync Online. • Join online meeting in Mobile clients • Publish status based on Outlook calendar free/busy information • Meeting delegation Supported only when both users are homed online in the same forest, or both are homed on-premises. **Note:** Exchange 2013 only	• IM/Presence in Outlook • Schedule and join online meetings through Outlook • IM/Presence in Outlook Web App • Schedule and join online meeting from Outlook Web App • IM/Presence in Mobile Clients • Join online meeting in Mobile clients • Publish status based on Outlook calendar free/busy information • Missed Conversations history and Call Logs are written to user’s exchange mailbox • Contact List (via Unified Contact Store) **Note:** Lync Server 2013 client Required • High-resolution Contact Photo in Lync 2013 client and Lync Web App • Meeting delegation Supported only when both users are homed

		online in the same forest, or both are homed on-premises. • Archiving Content (IM and Meeting) in Exchange • Search archived content • Voicemail

Integration with SharePoint

The following table lists the features supported in a Lync Server 2013 hybrid deployment when integrated with SharePoint.

	SharePoint on-premises	SharePoint Online
Lync Server 2013 on-premises	• Skills search • Presence in SharePoint	• Presence in SharePoint
Lync Online	• Presence in SharePoint	• Presence in SharePoint

1.5.2.3 Planning for Hybrid Voice

Planning for Hybrid Voice

Microsoft Lync Server 2013 > Lync Server 2013 Hybrid > Planning for Hybrid Deployments >

Topic Last Modified: *2013-03-12*

Many enterprises are actively looking to move their enterprise services to the cloud. The move to the cloud does not happen in single deployment step. It is more of a process performed over time in a phased approach eventually leading to a complete transition to the cloud. We refer to this phased approach while some users are still homed on-premise and other users are moved to Lync Online as a hybrid environment.

While planning a transition to the cloud, there needs to be an approach which allows the following:

- Moves existing functionality to the cloud
- Provides time to validate quality, reliability and the security of the cloud offering
- Continues to allow existing on-premise Lync investments to be utilized

To facilitate the transition to the cloud, hybrid voice allows customers to integrate Lync Online with their on-premise PSTN infrastructure:

- For migrating users from Lync on-premise to Lync Online
- For leveraging existing on-premise PBX infrastructure
- For keeping existing carrier relationships

On-Premise Infrastructure Requirements

Server Roles	Supported versions	Notes
Lync pool	Lync Server 2010: October 2012 cumulative updates or later Lync Server 2013	The Lync pool must be configured as the next hop to the Edge Server. A Lync pool consists of an Enterprise Edition pool, Standard Edition

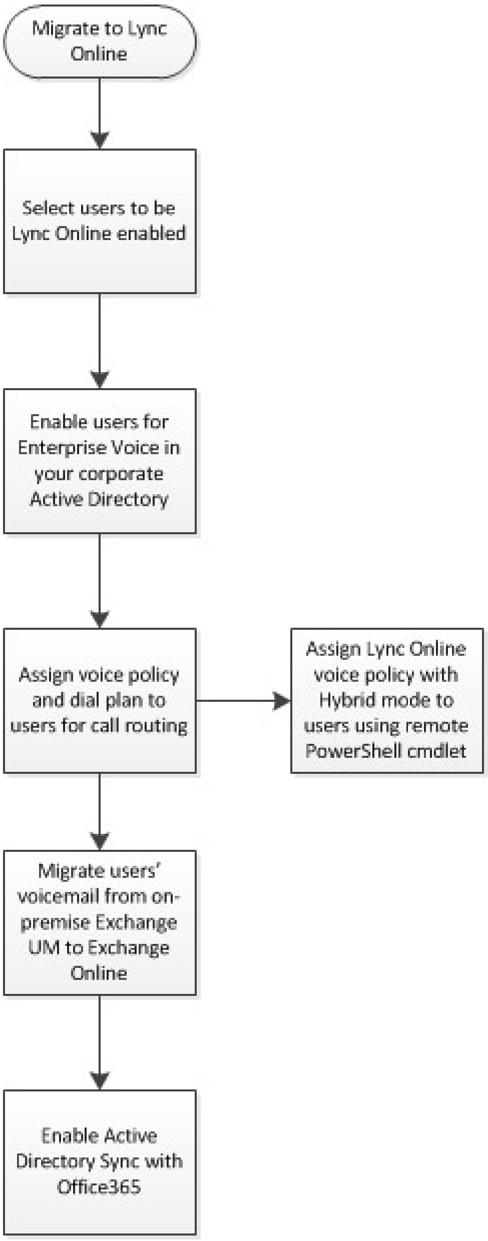
		server or Director
Edge Server	Lync Server 2010: October 2012 cumulative updates or later Lync Server 2013	
Mediation Server	Office Communication Server 2007 R2 Lync Server 2010 Lync Server 2013	E-9-1-1 and Media Bypass for hybrid voice users is only supported with Lync Server 2013Mediation Server.

Feature Summary

Enterprise Voice Functionality	Lync Online Hybrid Voice
Call Hold/Retrieve	yes
Call Transfer	yes
Call Forwarding	yes
Voicemail (Exchange UM Online)	yes
USB Peripherals	yes
Delegation, Team Call	yes
Outside voice – Mobile	yes
Integration with on-premise PBX	yes
Private Line	yes
E-9-1-1	yes
Media bypass	yes
Lync Phone Edition devices	yes
Response Group	no
Call Park	no
Voice Resiliency	no
RCC (remote call control)	no
Analog and common area phones	no
Integration with on-premise Call Center Solutions	no

Deployment Workflow

The following diagram illustrates the workflow to enable users for hybrid voice.


Migrate to Lync Online
Select users to be Lync Online enabled
Enable users for Enterprise Voice in your corporate Active Directory
Assign voice policy and dial plan to users for call routing
Assign Lync Online voice policy with Hybrid mode to users using remote PowerShell cmdlet
Migrate users' voicemail from on-premise Exchange UM to Exchange Online
Enable Active Directory Sync with Office365

1.5.3 Configuring Hybrid Deployments

Configuring Hybrid Deployments

Microsoft Lync Server 2013 > Lync Server 2013 Hybrid >

Topic Last Modified: *2013-02-22*

This section describes the steps necessary for configuring hybrid Lync Server 2013 deployments and Hybrid Voice deployments.

- Configuring an On-premises Deployment for Hybrid with Lync Online
- Configuring Hybrid Voice

⊟Related Sections

Planning for Hybrid Deployments

1.5.3.1 Configuring an On-premises Deployment for Hybrid with Lync Online

Configuring an On-premises Deployment for Hybrid with Lync Online

Microsoft Lync Server 2013 > Lync Server 2013 Hybrid > Configuring Hybrid Deployments >

Topic Last Modified: *2013-02-20*

A hybrid deployment is a deployment in which some users are homed on-premises and some users are homed online, but all users share the same domain, such as user@contoso.com. This section guides you through deploying the applications required for a hybrid deployment, and then configuring your deployment to enable it.

- Overview of the Lync Server 2013 Hybrid Environment
- Steps to Prepare and Deploy Lync Server 2013 Hybrid Environment
- Configure Federation with Lync Online
- Move Users to Lync Online
- Administering Users in a Hybrid Deployment

1.5.3.1.1 Overview of the Lync Server 2013 Hybrid Environment

Overview of the Lync Server 2013 Hybrid Environment

Lync Server 2013 Hybrid > Configuring Hybrid Deployments > Configuring an On-premises Deployment for Hybrid with Lync Online >

Topic Last Modified: *2013-02-19*

Lync Server 2013 hybrid environment refers to a deployment in which there are some users homed to the on-premises Lync Server 2013 and other users homed to Lync Online, but users share the same domain, such as user@contoso.com.

About this Guide

This guide describes the tasks necessary to configure your Lync Server 2013 environment for interoperability with Lync Online, and then to move users from your on-premises deployment to use Lync Online.

Prerequisites

You will need to have the following applications and utilities installed to complete the tasks for configuring a deployment for hybrid. The installers for these files are included on the installation media provided for your deployment, as well as at the links included in the following list.

- Active Directory Federation Services (AD FS) 2.0
- Directory Synchronization tool (DirSync.exe)
- Microsoft Online Services module for Windows PowerShell
- Microsoft Online Services Sign-in Assistant (msoidcli-7.0.msi) is included with the Desktop Setup for Office 365, which can be obtained from the Downloads page linked to from the Admin portal.

Administrator Credentials

When you are asked to provide your administrator credentials, use the username and password provided to you as the administrator account for the Office 365 tenant that was created for you. You will also use these credentials when you configure Active Directory Federation Services (AD FS) 2.0, Directory Synchronization, Single sign-on, and federation.

1.5.3.1.2 Steps to Prepare and Deploy Lync Server 2013 Hybrid Environment

Steps to Prepare and Deploy Lync Server 2013 Hybrid Environment

Lync Server 2013 Hybrid > Configuring Hybrid Deployments > Configuring an On-premises Deployment for Hybrid with Lync Online >

***Topic Last Modified:** 2013-02-22*

The following table lists the steps required to prepare your environment for a hybrid deployment with Microsoft Lync Online and Microsoft Office 365.

Completed?	Step	Description
	Create a tenant account for Office 365 and enable Lync Online	Learn about Office 365 and Lync Online at Office 365. To make sure that your environment is ready for Office 365, see the System Requirements. For details about setting up Office 365, see Getting Started with Office 365 and Set Up Office 365.
	Add your domain and verify ownership	Your domain is sometimes also referred to as your *vanity domain*. You must add your domain to your Office 365 tenant, and then follow the steps to validate the domain with Office 365. This is to confirm that you are the owner of the domain. To add your domain to your Office 365 tenant, follow the steps described at Add your domain to Office 365. Complete all of the steps in each section in the topic, including "Edit DNS records for your Office 365 services."
	Verify environment readiness	You can use the Office 365 Deployment Readiness Tool to identify any issues in your

		Active Directory Domain Services (AD DS) that may cause issues with synchronizing with Office 365. This tool inspects your Active Directory environment, and then provides a report that includes a prerequisite check and an attribute assessment that are specific to the directory synchronization tool requirements. To download the tool, see Microsoft Office 365 Deployment Readiness Tool. For details about using the tool and deploying Office 365, see Microsoft Office 365 Deployment Guide for Enterprises.
	Prepare for Active Directory synchronization	Active Directory synchronization keeps your on-premises Active Directory continuously synchronized with Office 365. This lets you create synchronized versions of each user account and group, and also enables global address list (GAL) synchronization from your local Microsoft Exchange Server environment to Microsoft Exchange Online. To prepare your environment for Active Directory synchronization, follow the steps described in Active Directory synchronization: Roadmap, including setting up single sign-on.
	Create certificates for Active Directory Federation Services (AD FS)	You will need to create the certificates that are used for identity federation with Office 365. For more information, see the “Federation server certificates” section of the Plan for and deploy AD FS for use with single sign-on topic at http://go.microsoft.com/fwlink/p/?LinkId=285376.
	Assign certificates for AD FS	After you create the certificates that are used for

		identity federation with Office 365, you must install and assign them.
	Move pilot users to Lync Online	After you have completed the steps to prepare and configure your environment for Lync Online, you can start moving pilot users to Lync Online. See Move Users to Lync Online.
	Administering users in a hybrid deployment	For details about how to administer users in a hybrid deployment, see Administering Users in a Hybrid Deployment.

1.5.3.1.3 Configure Federation with Lync Online

Configure Federation with Lync Online

See Also

Lync Server 2013 Hybrid > Configuring Hybrid Deployments > Configuring an On-premises Deployment for Hybrid with Lync Online >

Topic Last Modified: *2013-02-19*

Follow the steps in this section to configure interoperability between your on-premises deployment and Lync Online.

Configure Your Edge Service for Federation with Lync Online

Run the following cmdlets:

```
Set-CSAccessEdgeConfiguration -AllowOutsideUsers 1 -AllowFederatedUsers 1 -UseDns
```

```
New-CSHostingProvider -Identity LyncOnline -ProxyFqdn "sipfed.online.lync.com" -E
```

For details about considerations for federation in a hybrid deployment, see Planning for Lync Server 2013 Hybrid Deployments.

⊟See Also

Other Resources

New-CsHostingProvider

1.5.3.1.4 Move Users to Lync Online

Move Users to Lync Online

Lync Server 2013 Hybrid > Configuring Hybrid Deployments > Configuring an On-premises Deployment for Hybrid with Lync Online >

Topic Last Modified: *2013-02-19*

Before you start migrating users to Lync Online, you should backup the user data associated with the account to be moved.

Migrate User Settings to Lync Online

User settings are moved with the user account. Some on-premises settings are not moved with the user account.

Moving Pilot Users to Lync Online

Before you begin to move users to Lync Online, you may want to move a few pilot users to confirm that your environment is correctly configured. You can then verify that Lync features and services function as expected before attempting to move additional users.

To move an on-premises user to your Lync Online tenant, run the following cmdlets in the Lync Server Management Shell, using the administrator credentials for your Microsoft Office 365 tenant. Replace "username@contoso.com" with the information for the user that you want to move.

```
$creds=Get-Credentials
```

```
Move-CsUser -Identity username@contoso.com -Target sipfed.online.lync.com -Creden
```

The format of the URL specified for the **HostedMigrationOverrideUrl** parameter must be the URL to the pool where the Hosted Migration service is running, in the following format:

Https://<Pool FQDN>/HostedMigration/hostedmigrationService.svc. You can determine the URL to the Hosted Migration Service by viewing the URL for the Lync Online Control Panel for your Office 365 tenant account.

To determine the Lync Online Control Panel URL for your Office 365 tenant

1. Login to the Office 365 portal, and then access the Lync Administration Center.
2. Copy the URL in the address bar up to "ync.com." For example, **https://admin.online.lync.com**.
3. Append the following string to the URL: **/HostedMigration/hostedmigrationservice.svc**.
   The resulting URL should look like the following:
   https://admin.online.lync.com/HostedMigration/hostedmigrationservice.svc

Moving Users to Lync Online

You can move multiple users by using the **Get-CsUSer** cmdlet with the –Filter parameter to select the users with a specific property assigned to the user accounts, such as RegistrarPool. You can then pipe the returned users to the **Move-CsUSer** cmdlet, as shown in the following example.

```
Get-CsUser -Filter {UserProperty -eq "UserPropertyValue"} | Move-CsUser -Target s
```

You can also use the –OU parameter to retrieve all users in the specified OU, as shown in the following example.

```
Get-CsUser -OU "cn=hybridusers,cn=contoso.." | Move-CsUser -Target sipfed.online.
```

Verify Lync Online User Settings and

Features

You can verify that the user was moved successfully in the following ways:

- View the status of the user in the Lync Online Control Panel. The visual indicator for on-premises users and online users is different.
- Run the following cmdlet:

```

Get-CsUser -Identity
```

1.5.3.1.5 Administering Users in a Hybrid Deployment

Administering Users in a Hybrid Deployment

Lync Server 2013 Hybrid > Configuring Hybrid Deployments > Configuring an On-premises Deployment for Hybrid with Lync Online >

Topic Last Modified: *2013-02-22*

You can manage user settings and policies for users migrated to Lync Online by using the User Management features available in the Microsoft Office 365 online portal. You must sign in by using a tenant administrator account to perform administration tasks.

Moving Users Back to On-premises

- Run the following cmdlet:

```
$cred=Get-Credentials
Move-CsUser -Identity username@contoso.com -Target localpool.contoso.co
```

The format of the URL specified for the **HostedMigrationOverrideUrl** parameter must be the URL to the pool where the Hosted Migration service is running, in the following format:

Https://<Pool FQDN>/HostedMigration/hostedmigrationService.svc. You can determine the URL to the Hosted Migration Service by viewing the URL for the Lync Online Control Panel for your Office 365 tenant account.

1.5.3.2 Configuring Hybrid Voice

Configuring Hybrid Voice

Microsoft Lync Server 2013 > Lync Server 2013 Hybrid > Configuring Hybrid Deployments >

Topic Last Modified: *2012-06-29*

With Office 365 Lync Online, Microsoft offers customers Lync Server 2013 as an online service. Customers can migrate to Lync Online on their own terms. With an existing deployment of Lync Server on-premises, hybrid voice refers to a customer environment where some users are enabled for Enterprise Voice on-premises (that is, on-premises users) and other users are enabled for hosted Enterprise Voice online (that is, Office 365 users). This hybrid model provides a seamless user experience for users enabled for Enterprise Voice, whether they are enabled on-premises or online. This section guides you through the configuration of Enterprise Voice with Lync Online.

This section assumes that you have already deployed Lync Server on-premises and have enabled users for Enterprise Voice. You have defined at least one gateway peer to provide PSTN connectivity.

This section also assumes that you have configured on-premises Active Directory Federation Services—a Windows Server 2008 service—to federate with the Microsoft Federation Gateway. After Active Directory Federation Services is configured, all Lync Online users whose identities are based on the federated domain can use their existing corporate logon to automatically authenticate to Office 365.

In This Section

- Configure Enterprise Voice to Work with Lync Online
- Configure Online Users for Lync on-premises Enterprise Voice
- Configure Enterprise Voice Applications for Lync Online Users

1.5.3.2.1 Configure Enterprise Voice to Work with Lync Online

Configure Enterprise Voice to Work with Lync Online

Lync Server 2013 Hybrid > Configuring Hybrid Deployments > Configuring Hybrid Voice >

Topic Last Modified: *2013-02-21*

The following steps configure your Enterprise Voice deployment to enable Lync Online users to receive and place calls to the PSTN through your on-premises PSTN gateways.

- Create a Hybrid PSTN Usage
- Create a Hybrid Voice Routing Policy
- Dial Plan for Hybrid Voice Users
- Normalization Rules for Dial Plan

1.5.3.2.1.1 Create a Hybrid PSTN Usage

Create a Hybrid PSTN Usage

Configuring Hybrid Deployments > Configuring Hybrid Voice > Configure Enterprise Voice to Work with Lync Online >

Topic Last Modified: *2013-02-21*

This step creates a usage specifically for your Lync Online users, which is called HybridVoiceUsage. The new PSTN usage must be tag or global scope. You can also use an existing PSTN usage as long as it is tag scope or global scope.

Using Windows PowerShell command-line interface to create a PSTN usage

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. In the Lync Server Management Shell, type the following commands, replacing the placeholders with the correct information for your organization:

   ```
   Set-CSPstnUsage -Usage <String>
   ```

   For example:

   ```
   Set-CSPstnUsage -Usage @{add="HybridVoiceUsage"}
   ```

1.5.3.2.1.2 Create a Hybrid Voice Routing Policy

Create a Hybrid Voice Routing Policy

Configuring Hybrid Deployments > Configuring Hybrid Voice > Configure Enterprise Voice to Work with Lync Online >

Topic Last Modified: *2013-02-21*

This step creates a voice routing policy specifically for your Lync Online users. Perform this procedure at the on-premise central site. If you want to assign an existing voice routing policy to your Lync Online users, skip to Configure Online Users for Lync on-premises Enterprise Voice, and replace the policy tag, HybridVoiceUser, with the name of your voice routing policy.

The voice routing policy is used to route calls to the PSTN through your on-premises PSTN gateway when the Edge Server next hop is a Lync Server 2013 pool or Director. However, if the Edge Server next hop is a Lync Server 2010 pool or Director, then the user's voice policy is used to route calls to the PSTN.

Using Windows PowerShell command-line interface to create a voice routing policy

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. In the Lync Server Management Shell, type the following commands, replacing the placeholders with the correct information for your organization:

   ```
   New-CSVoiceRoutingPolicy -Identity <Tag> -Name <String> -PstnUsages <U
   ```

   For example:

   ```
   New-CSVoiceRoutingPolicy -Identity "tag:HybridVoiceUser" -Name "Hybrid
   ```

1.5.3.2.1.3 Dial Plan for Hybrid Voice Users

Dial Plan for Hybrid Voice Users

Configuring Hybrid Deployments > Configuring Hybrid Voice > Configure Enterprise Voice to Work with Lync Online >

Topic Last Modified: *2012-11-13*

This step creates a dial plan specifically for your Lync Online users. Skip this step if you plan to apply an existing tagged scoped dial plan to your hybrid voice users, instead of creating a new dial plan. Perform this procedure at the on-premise central site.

Using Windows PowerShell command-line interface to create a dial plan

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. In the Lync Server Management Shell, type the following commands, replacing the placeholders with the correct information for your organization:

   ```
   New-CSDialPlan -Identity "tag:HybridVoiceDialplan" -SimpleName "Hybrid
   ```

1.5.3.2.1.4 Normalization Rules for Dial Plan

Normalization Rules for Dial Plan

Configuring Hybrid Deployments > Configuring Hybrid Voice > Configure Enterprise Voice to Work with Lync Online >

Topic Last Modified: *2012-04-28*

Create normalization rules for the dial plan created in the previous section, Dial Plan for Hybrid Voice Users. Skip this step if you plan to apply an existing set of normalization rules to your hybrid voice users, instead of creating new normalization rules. Perform this procedure at the on-premise central site.

Using Windows PowerShell command-line interface to create normalization rules

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. In the Lync Server Management Shell, type the following commands, replacing the placeholders with the correct information for your organization:

   ```
   New-CSVoiceNormalizationRule -Identity <Tag> -Pattern <RegEx String> -
   ```

   For example:

   ```
   New-CSVoiceNormalizationRule -Identity tag:HybridVoiceDialplan/7Digit
   New-CSVoiceNormalizationRule -Identity tag:HybridVoiceDialplan/10Digit
   New-CSVoiceNormalizationRule -Identity tag:HybridVoiceDialplan/11Digit
   ```

1.5.3.2.2 Configure Online Users for Lync on-premises Enterprise Voice

Configure Online Users for Lync on-premises Enterprise Voice

Lync Server 2013 Hybrid > Configuring Hybrid Deployments > Configuring Hybrid Voice >

Topic Last Modified: *2012-04-09*

After creating a voice routing policy and dial plan for your Lync Online users, use the following procedures to enable your Lync Online users for Lync on-premise Enterprise Voice.

- Enable On-Premise Enterprise Voice
- Assign a Voice Routing Policy
- Assign a Dial Plan
- Assign a Lync Online Voice Policy
- Move Voicemail for Lync Online Users to Exchange Online

1.5.3.2.2.1 Enable On-Premise Enterprise Voice

Enable On-Premise Enterprise Voice

Configuring Hybrid Deployments > Configuring Hybrid Voice > Configure Online Users for Lync on-premises Enterprise Voice >

Topic Last Modified: *2012-04-09*

For Lync Online users to place and receive voice calls, they must be enabled for Enterprise Voice on the on-premise Lync Server environment. Perform the following procedures at the central site.

To enable Lync Online users for Enterprise Voice

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Administrator URL to open the Lync Server 2013 Control Panel. For details about the different methods you

can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to enable, and then click **Find**.
5. In the table, click the Lync Online user account that you want to enable for Enterprise Voice.
6. Click Line URI, and assign a unique, normalized TEL URI (for example, tel:+14255550200). This will be the user's phone number.
7. Click Commit.
8. To finish enabling a user for Enterprise Voice, ensure that the user is assigned the user-specific hybrid voice policy and dial plan.

1.5.3.2.2.2 Assign a Voice Routing Policy

Assign a Voice Routing Policy

Configuring Hybrid Deployments > Configuring Hybrid Voice > Configure Online Users for Lync on-premises Enterprise Voice >

Topic Last Modified: *2012-06-28*

The user-specific on-premise Lync voice routing policy, created in the step Create a Hybrid Voice Policy, must be assigned to the Lync Online users. Perform the following procedures at the central site. If you are using an existing voice routing policy, replace the placeholder, HybridVoiceUser, with the name of your voice policy

To assign the user-specific hybrid voice policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Assign an existing voice policy to a user:

   ```
   Grant-CsVoiceRoutingPolicy -Identity <UserIdParameter> -PolicyName <St
   ```

   For example:

   ```
   Grant-CsVoiceRoutingPolicy -Identity "Bob Kelly" -PolicyName HybridVoi
   ```

In this example, the user with the display name Bob Kelly is assigned to the previously created voice policy with the name HybridVoiceUser.

For details about assigning a user-specific voice policy or about running the Grant-CsVoiceRoutingPolicy cmdlet, see the Lync Server Management Shell documentation.

1.5.3.2.2.3 Assign a Dial Plan

Assign a Dial Plan

Configuring Hybrid Deployments > Configuring Hybrid Voice > Configure Online Users for Lync on-premises Enterprise Voice >

Topic Last Modified: *2012-06-28*

To complete the on-premise configuration for Lync Online users enabled for Enterprise Voice, the on-premise administrator must assign an on-premise dial plan to the Lync Online user. Perform the following procedures at the central site.

To assign a dial plan

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Assign a user-specific dial plan:

   ```
   Grant-CsDialPlan -Identity <UserIdParameter> -PolicyName <String>
   ```

   For example:

   ```
   Grant-CsDialPlan -Identity "Bob Kelly" -PolicyName HybridVoiceDialplan
   ```

In this example, the user with the display name Bob Kelly is assigned the previously created user dial plan with the name HybridVoiceDialplan.

For details about assigning a user dial plan or about running the Grant-CsDialPlan cmdlet, see the Lync Server Management Shell documentation.

1.5.3.2.2.4 Assign a Lync Online Voice Policy

Assign a Lync Online Voice Policy

Configuring Hybrid Deployments > Configuring Hybrid Voice > Configure Online Users for Lync on-premises Enterprise Voice >

Topic Last Modified: *2013-02-21*

The Lync Online users must also be assigned a Lync Online voice policy, also referred to as a Hybrid Voice policy. The tenant administrator assigns the Lync Online voice policy to Lync Online users enabled for on-premises Enterprise Voice by remotely using the PowerShell Lync Server Management Shell cmdlet, **Grant-CsVoicePolicy**. Perform the following procedures. "HybridVoice" is the default name of the Lync Online voice policy.

To assign the user-specific hybrid voice policy

1. Start a Windows PowerShell remote session, not a Lync Server Management Shell.

   Note:
   For details about how to start a Windows PowerShell remote session, see Lync Server Windows PowerShell blog article, "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell," at http://go.microsoft.com/fwlink/?LinkId=255876.

2. In the Windows PowerShell, type the following command and then press **Enter**:

   ```
   $PSModuleAutoloadingPreference = "None"
   ```

3. Import the following Windows PowerShell command-line interface modules:

   ```
   Import-Module LyncOnlineConnector, Microsoft.PowerShell.Management, Mi
   ```

4. Provide your Administrator’s credentials:

   ```
   $cred=Get-Credential <Administrator URI>
   ```

   You will be prompted to enter the Administrator’s password.

5. Create a Lync Online session, specifying the URL of your Lync Online Control Panel:

   ```
   $CsSession = New-CsOnlineSession -TargetServer <Lync Online Control Pa
   ```

Note:
To determine the URL of your Lync Online Control Panel, follow the steps in **To determine the Lync Online Control Panel URL for your Office 365 tenant** under Move Users to Lync Online.

6. Import all the commands from the newly created session, $CsSession, into the current session:

```
Import-PsSession -Session $CsSession
```

7. Assign the Lync Online policy to your user specified by its SIP URI:

```
Grant-CsVoicePolicy -Identity <SIP URI> -PolicyName HybridVoice
```

For example:

```
Grant-CsVoicePolicy -Identity dorena@contoso.com -PolicyName HybridVoi
```

1.5.3.2.2.5 Move Voicemail for Lync Online Users to Exchange Online

Move Voicemail for Lync Online Users to Exchange Online

Configuring Hybrid Deployments > Configuring Hybrid Voice > Configure Online Users for Lync on-premises Enterprise Voice >

Topic Last Modified: *2012-06-29*

The final step is to move Lync Online users' Unified Messaging to Exchange Online. For procedures for configuring Unified Messaging for Lync Online users, see Set Up Unified Messaging at http://go.microsoft.com/fwlink/?LinkId=255531.

1.5.3.2.3 Configure Enterprise Voice Applications for Lync Online Users

Configure Enterprise Voice Applications for Lync Online Users

Lync Server 2013 Hybrid > Configuring Hybrid Deployments > Configuring Hybrid Voice >

Topic Last Modified: *2013-02-25*

In a hybrid voice environment where Lync Online users are enabled for Enterprise Voice using Lync on-premise, these Lync Online users do not have access to advanced features such as Media Bypass and E-9-1-1 available to on-premise Enterprise Voice users until the tenant administrator configures the web URL on Lync Online. To enable Lync Online users to benefit from on-premise Enterprise Voice Applications, the tenant administrator must perform the following procedures.

To enable Lync Online users for Enterprise voice applications

1. Select the Lync pool to serve the Lync Online users.
2. Configure the Lync Web Service and CPS is enabled (with configured orbit numbers) on the selected pool.
3. Assign Lync Online the URL of the Web Service of the selected Lync pool by running the following remote Windows PowerShell command-line interface cmdlet. To enable Media Bypass and E-9-1-1 for hybrid voice users, Lync Server 2013 pool is required. If your deployment uses Lync Server 2010, then you must upgrade to Lync Server 2013 to enable Media Bypass and E-9-1-1.

```
Set-CSTenantHybridConfiguration
-HybridConfigServiceInternalURL <on-premise Web Service internal URL c
-HybridConfigServiceExternalURL <on-premise Web Service external URL c
```

1.6 Migration

Migration

Microsoft Lync Server 2013 >

Topic Last Modified: *2012-09-18*

This section explains how to migrate from Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010 to Microsoft Lync Server 2013, from Microsoft Lync Server 2010, Group Chat to Microsoft Lync Server 2013, Persistent Chat Server, and from Microsoft Office Communications Server 2007 R2 Group Chat to Persistent Chat Server.

- Migration from Lync Server 2010 to Lync Server 2013
- Migration from Office Communications Server 2007 R2 to Lync Server 2013
- Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server

1.6.1 Migration from Lync Server 2010 to Lync Server 2013

Migration from Lync Server 2010 to Lync Server 2013

Microsoft Lync Server 2013 > Migration >

Topic Last Modified: *2012-09-17*

The topics in this section guide you through the process of migrating from Lync Server 2010 to Lync Server 2013.

◆**Important:**
This document describes the steps generally required to accomplish each phase of migration. It does not address every possible legacy deployment topology or every possible migration scenario. Therefore, you may not need to perform every step described, or you may need to perform additional steps, depending on your deployment. This document also provides examples of verification steps. These verification steps are provided to help you understand what you need to look for to ensure that each phase completes successfully as you progress through your migration. Tailor these verification steps to your specific migration process.

This guide provides information specific to upgrading your existing deployment. It does not explain how to change your existing topology. This guide does not cover the implementation of new features. When a detailed procedure is documented elsewhere, this guide directs you to the appropriate document or document section.

This document defines terms as specified in the following list.

migration

Moving your production deployment from a previous version of Lync Server 2010 to Lync Server 2013.

upgrade

Installing a newer version of software on a server or client computer.

coexistence

The temporary environment that exists during migration when some functionality has been migrated to Lync Server 2013 and other functionality still remains on a prior version of Lync Server 2010.

interoperability

The ability of your deployment to operate successfully during the period of coexistence.

In This Section

1.6.1.1 Before You Begin the Migration

Before You Begin the Migration

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010 to Lync Server 2013 >

Topic Last Modified: *2012-09-23*

Before you begin, we recommend that you read this document and the following guides to familiarize yourself with deploying the corresponding Lync Server 2013 roles:

- Deploying Lync Server 2013
- Deploying Lync Server 2013 Standard Edition into an Existing Lync Server 2013 Enterprise
- Deploying External User Access
- Deploying Clients and Devices
- Migration Process
- Migration Phases

1.6.1.1.1 Migration Process

Migration Process

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Before You Begin the Migration >

Topic Last Modified: *2012-09-17*

The recommended and supported migration procedure for Lync Server 2013 is side-by-side migration. This topic describes why you should use side-by-side migration and also includes information about coexistence testing.

Side-By-Side Migration

In nearly every migration, you should use the side-by-side migration path. In a side-by-side migration, you deploy a new server with Lync Server 2013 alongside a corresponding server that is running Lync Server 2010, and then transfer operations to the new server. If it becomes necessary to roll back to Lync Server 2010, you have only to shift operations back to the original servers. Be aware that in this situation any new meetings scheduled with upgraded clients will not work, and the clients would also need to be downgraded.

Coexistence Testing

After you have deployed Lync Server 2013 in parallel with Lync Server 2010, the deployment represents a coexistence testing state of Lync Server 2013 and Lync Server 2010. While in this state, it is important to test and ensure that services are started, each site can be administered, and clients can communicate with current and legacy users. Prior to the migration of all users, it is very important that you understand the state of each deployment and ensure that each deployment is functional and working properly. Typically, the coexistence testing phase exists throughout the pilot testing of Lync Server 2013. Legacy users are moved to Lync Server 2013 for a period of time to ensure that application compatibility and features and functions are working properly. After pilot testing, users and applications are moved to the production version of Lync Server 2013, and the legacy pools and applications of Lync Server 2010 are retired.

1.6.1.1.2 Migration Phases

Migration Phases

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Before You Begin the Migration >

Topic Last Modified: *2012-09-17*

In Lync Server 2013, you define sites on your network that contain Lync Server 2013 components. A site is a set of computers that are well-connected by a high-speed, low-latency network, such as a single local area network (LAN) or two networks connected by a high-speed fiber optic network.

A *Front End pool* is a set of Front End Servers that are configured identically and work together to provide services for a common group of users. A pool provides scalability and failover capability to your users. Each server in a pool must run an identical server role or roles. A Standard Edition server, designed for small organizations, also defines a pool and runs on a single server. This enables you to have Lync Server 2013 functionality for a lesser cost, but does not provide a true high-availability solution.

The following phases describe the process of a pool migration from Lync Server 2010 to Lync Server 2013. For multiple sites containing multiple pools, each individual pool should follow this phased approach.

1. Phase 1: Plan Your Migration from Lync Server 2010
2. Phase 2: Prepare for Migration
3. Phase 3: Deploy Lync Server 2013 Pilot Pool
4. Phase 4: Move test users to the Pilot Pool
5. Phase 5: Add Lync Server 2013 Edge Server to Pilot Pool
6. Phase 6: Move from Pilot Deployment into Production
7. Phase 7: Complete Post-Migration Tasks
8. Phase 8: Decommission Legacy Pools

1.6.1.2 Phase 1: Plan Your Migration from Lync Server 2010

Phase 1: Plan Your Migration from Lync Server 2010

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010 to Lync Server 2013 >

Topic Last Modified: *2012-09-29*

This section covers planning topics for migrating from Lync Server 2010 to Lync Server 2013.

In This Section

1.6.1.2.1 User Migration

User Migration

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 1: Plan Your Migration from Lync Server 2010 >

Topic Last Modified: *2012-10-19*

A generally accepted best practice for migrations is to create several test users and use them to conduct systems tests. After you have successfully moved and tested those accounts, you should identify a group of pilot production users and move their accounts and conduct validation tests on them. When you get satisfactory results, you can move the rest of your users to the new deployment.

For additional information on enabling users for Lync Server 2013, see the topic Disable or Re-Enable User Account for Lync Server in the Deploying Lync Server 2013 documentation.

1.6.1.2.2 Migrating Archiving and Monitoring Servers

Migrating Archiving and Monitoring Servers

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 1: Plan Your Migration from Lync Server 2010 >

Topic Last Modified: *2012-10-02*

If you deployed Archiving Server and Monitoring Server in your Lync Server 2010 environment, you can deploy these servers in your Lync Server 2013 environment after you migrate your Front End pools. If archiving and monitoring functionality are critical to your organization, however, you should add archiving and monitoring to your Lync Server 2013 pilot pool before you migrate so that the functionality is available during the migration process.

If you want archiving and monitoring functionality during the migration process, keep the following considerations in mind:

- Archiving data and monitoring data are not moved to the Lync Server 2013 deployment. The data you back up prior to decommissioning the legacy environment will be your history of activity in the Lync Server 2010 environment.
- The Lync Server 2010 version of Archiving Server and Monitoring Server can be associated only with a Lync Server 2010 Front End pool. In Lync Server 2013, Archiving and Monitoring are no longer server roles, but services integrated into the Lync Server 2013 Front End pool.
- During the time that your legacy and Lync Server 2013 deployments coexist, the Lync Server 2010 version of Archiving Server and Monitoring Server gather data for users homed on Lync Server 2010 pools. Archiving and Monitoring in

Lync Server 2013 gather data for users homed on Lync Server 2013 pools.

> **Note:**
> During the phase of migration when you are still using your legacy Edge server with the new Lync Server 2013 pilot pool, the Lync Server 2010 version of Archiving Server continues to gather data for users homed on Lync Server 2010 pools and Archiving in Lync Server 2013 gathers data for users homed on Lync Server 2013 pools.

- If you use a third-party archiving and monitoring solution in conjunction with Archiving and Monitoring in Lync Server 2013, consult with your vendor about when and how you need to integrate the third-party solution with Lync Server 2013.

1.6.1.2.3 Migrating Group Chat Servers

Migrating Group Chat Servers

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 1: Plan Your Migration from Lync Server 2010 >

Topic Last Modified: *2012-09-29*

If you deployed Group Chat Server in your legacy Lync Server 2010 environment, you must deploy Lync Server 2013 Persistent Chat Server. Group Chat Server and Persistent Chat Server can coexist, but content (for example, chat rooms, etc.) is not shared across these servers. To access the legacy Group Chat Server content from Persistent Chat Server, you must migrate the Group Chat Server to Persistent Chat Server. For details on migrating to Persistent Chat Server, see Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server in the Migration documentation.

1.6.1.2.4 Administering Servers after Migration

Administering Servers after Migration

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 1: Plan Your Migration from Lync Server 2010 >

Topic Last Modified: *2012-09-29*

In general, you must use the administrative tool that corresponds to the server version that you want to manage. You cannot install the Lync Server 2010 and the Lync Server 2013 administrative tools on the same computer. Also, the Lync Server 2013 Control Panel is not installed automatically on each server. To install the Lync Server 2013 Control Panel, follow the procedure inside the topic Install Lync Server Administrative Tools in the Deployment documentation.

> **Important:**
> After a Lync Server 2013 pilot pool is deployed, you cannot use Lync Server 2010 Topology Builder or Lync Server 2010 Control Panel to manage any Lync Server 2013 resources. You must use Lync Server 2013 tools to manage Lync Server 2013 and Lync Server 2010 resources.

1.6.1.2.5 Migrating Multiple Sites and Pools

Migrating Multiple Sites and Pools

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 1: Plan Your Migration from Lync Server 2010 >

Topic Last Modified: *2012-09-17*

Lync Server 2013 supports multi-site and multi-pool deployments. The process of migrating multiple pools from Lync Server 2010 to Lync Server 2013 requires the following considerations:

1. After deploying a Lync Server 2013 pilot pool, you need to define a subset of pilot users that will be moved to the Lync Server 2013 pool, and a methodology for validating the functionality of the users. For example, after moving a user to the pilot pool, verify the user's conference policy has moved to Lync Server 2013.
2. After deploying an Edge Server in the pilot pool, you need to validate that external users can communicate with the Lync Server 2013 pool.
3. After transitioning the federated routes from Lync Server 2010 Edge Servers to the pilot Lync Server 2013 Edge Servers, you need to validate that federated users can communicate with the Lync Server 2013 pool.
4. After moving all the users and non-user contact objects, you need to validate that the Lync Server 2010 pool is empty.
5. After verifying that the Lync Server 2010 pool is empty, you can then deactivate the pool.
   For details about how to deactivate the legacy Lync Server 2010 pool and servers, see Phase 8: Decommission Legacy Pools.

1.6.1.2.6 Migrating XMPP Federation

Migrating XMPP Federation

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 1: Plan Your Migration from Lync Server 2010 >

Topic Last Modified: *2012-10-19*

Previous versions of Lync Server and Office Communications Server provided an extensible messaging and presence protocol (XMPP) gateway that could be deployed as a separate server role to allow federating with XMPP deployments. In Lync Server 2013, the XMPP functionality can be deployed as a feature. XMPP functionality is installed in two parts: as an XMPP proxy that runs on the Lync Server 2013 Edge Server, and the XMPP Gateway that runs on the Lync Server 2013 Front End Server.

From a migration perspective, a Lync Server user account can be moved to a Lync Server 2013 pool and continue to use the legacy XMPP gateway. This is possible only when the XMPP federated partner is not configured in Lync Server 2013.

In summary, if Lync Server 2010 has been deployed with the Office Communications Server 2007 R2 XMPP Gateway and XMPP federation has been enabled for legacy Lync Server 2010 users, to migrate the XMPP federation to Lync Server 2013:

1. Deploy a Lync Server 2013 pool.
2. Deploy a Lync Server 2013 Edge server.
3. Move all users to the Lync Server 2013 pool
4. Create XMPP access policies and certificates for the Edge Server.
5. Enable XMPP federation in Lync Server 2013.
6. Update the DNS entries to point to the Lync Server 2013 XMPP Gateway.

1.6.1.3 Phase 2: Prepare for Migration

Phase 2: Prepare for Migration

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010 to Lync Server 2013 >

Topic Last Modified: *2012-09-17*

Before you begin your migration to Lync Server 2013 from Lync Server 2010, follow the steps described in this section.

In This Section

- Apply Lync Server 2010 Updates
- Configure DNS Records for Pilot Pool Deployment
- Run Best Practices Analyzer
- Back Up Systems and Data
- Configure Clients for Migration
- Verify Lync Server 2010 Environment

1.6.1.3.1 Apply Lync Server 2010 Updates

Apply Lync Server 2010 Updates

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-10-19*

Before you migrate to Lync Server 2013, updates must be applied to your Lync Server 2010 environment. For the most up-to-date information about Lync Server 2010, see **Updates Resource Center for Lync** at http://go.microsoft.com/fwlink/p/?linkid=232630.

To install updates for Lync Server 2010, we recommend you follow the **Method 1 Cumulative Server Update Installer** procedure described in the Microsoft Knowledge Base article, "Updates for Lync Server 2010," at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=2493736.

1.6.1.3.2 Configure DNS Records for Pilot Pool Deployment

Configure DNS Records for Pilot Pool Deployment

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-09-29*

Prior to deploying the Lync Server 2013 pilot pool, you must update the DNS Host A entries for the pilot pool. To successfully complete this procedure, you should be logged on to the server or domain as a member of the Domain Admins group or a member of the DnsAdmins group.

To configure DNS Host A records

1. On the Domain Name System (DNS) server, click **Start**, click **Administrative Tools**, and then click **DNS**.
2. In the console tree for your domain, expand **Forward Lookup Zones**, and

then right-click the domain in which Lync Server 2013 will be installed.
3. Click **New Host (A or AAAA)**.
4. Click **Name**, type the host name for the Lync Server 2013 pool (the domain name is assumed from the zone that the record is defined in and does not need to be entered as part of the A record).
5. Click **IP Address**, type the IP address for the Front End pool.
6. Click **Add Host**, and then click **OK**.
7. When you are finished, click **Done**.

1.6.1.3.3 Run Best Practices Analyzer

Run Best Practices Analyzer

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-03-21*

The Lync Server 2010 Best Practices Analyzer tool gathers configuration information from an Lync Server 2010 deployment and determines whether the configuration is set according to Microsoft best practices. You can install the tool on a client computer that runs Microsoft .NET Framework 3.5 Service Pack 1, or directly on the server that runs Lync Server 2010. We recommend that you install and run this tool on a client computer. The Lync Server 2010 Administrative Tools should also be installed locally on the client computer so that the Best Practices Analyzer can collect a full set of data.

You can download the Lync Server 2010 Best Practices Analyzer from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?linkid=246173 .

1.6.1.3.4 Back Up Systems and Data

Back Up Systems and Data

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-09-18*

Before you begin the migration to Lync Server 2013, we strongly recommend that you perform a full system backup and document your existing system, including an inventory of user accounts that are homed on each pool, so that you can roll back to Lync Server 2010 if it becomes necessary. Multiple tools and programs are available for backing up and restoring data, settings, and systems.

For details and procedures, see Backing Up and Restoring Lync Server 2010 .

1.6.1.3.5 Configure Clients for Migration

Configure Clients for Migration

See Also

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-09-24*

This topic contains the recommended client deployment steps you should take before migrating to Lync Server 2013. These configuration changes should be made on Lync

Server 2010.

⊟To configure clients before migration

1. Deploy the most recent server, client, and device updates (hotfixes) for Lync Server 2010. For the most up-to-date information about Lync Server 2010, see Updates Resource Center for Lync at http://go.microsoft.com/fwlink/p/?linkid=232630.
2. On Lync Server 2010, use Client Version Filtering to only allow clients with the most current updates installed.

Concepts

New and Changed Settings for Lync 2013
Client Interoperability in Lync 2013

Other Resources

Planning for Clients and Devices in Lync Server 2013

1.6.1.3.6 Verify Lync Server 2010 Environment

Verify Lync Server 2010 Environment

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 2: Prepare for Migration >

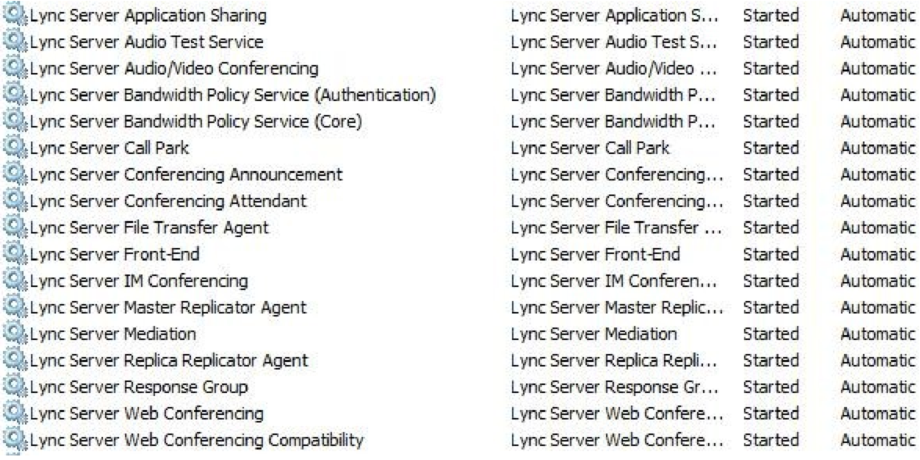
Topic Last Modified: *2012-10-19*

Before deploying Lync Server 2013 in a coexistence state with Lync Server 2010, you need to verify that Lync Server 2010 services have been configured and started. It is important to identify key services and features that exist in your legacy environment, prior to deploying a Lync Server 2013 pilot pool. Before deploying Microsoft Lync Server 2013 XMPP in a coexistence state with a legacy XMPP deployment, you need to verify the legacy XMPP services have been configured and started, and identify which federated partner the legacy XMPP configuration is supporting. Verifying your legacy Lync Server 2010 deployment entails the following:

- Verifying the Lync Server 2010 services are started
- Reviewing the topology and users in Lync Server 2010.
- Verifying the federation and Edge server settings.
- Verifying XMPP services and federated partners.

Verify Lync Server 2010 Services are started

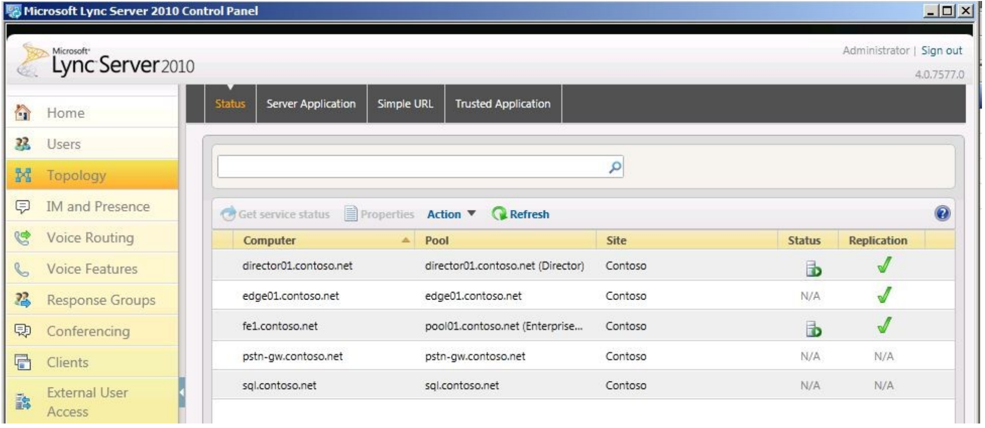
1. From the Lync Server 2010 Front End Server, navigate to the Administrative Tools\Services applet.
2. Verify that the following services are running on the Front End Server:



Lync Server Application Sharing	Lync Server Application S...	Started	Automatic
Lync Server Audio Test Service	Lync Server Audio Test S...	Started	Automatic
Lync Server Audio/Video Conferencing	Lync Server Audio/Video ...	Started	Automatic
Lync Server Bandwidth Policy Service (Authentication)	Lync Server Bandwidth P...	Started	Automatic
Lync Server Bandwidth Policy Service (Core)	Lync Server Bandwidth P...	Started	Automatic
Lync Server Call Park	Lync Server Call Park	Started	Automatic
Lync Server Conferencing Announcement	Lync Server Conferencing...	Started	Automatic
Lync Server Conferencing Attendant	Lync Server Conferencing...	Started	Automatic
Lync Server File Transfer Agent	Lync Server File Transfer ...	Started	Automatic
Lync Server Front-End	Lync Server Front-End	Started	Automatic
Lync Server IM Conferencing	Lync Server IM Conferen...	Started	Automatic
Lync Server Master Replicator Agent	Lync Server Master Replic...	Started	Automatic
Lync Server Mediation	Lync Server Mediation	Started	Automatic
Lync Server Replica Replicator Agent	Lync Server Replica Repli...	Started	Automatic
Lync Server Response Group	Lync Server Response Gr...	Started	Automatic
Lync Server Web Conferencing	Lync Server Web Confere...	Started	Automatic
Lync Server Web Conferencing Compatibility	Lync Server Web Confere...	Started	Automatic

Review the Lync Server 2010 topology in Lync Server Control Panel

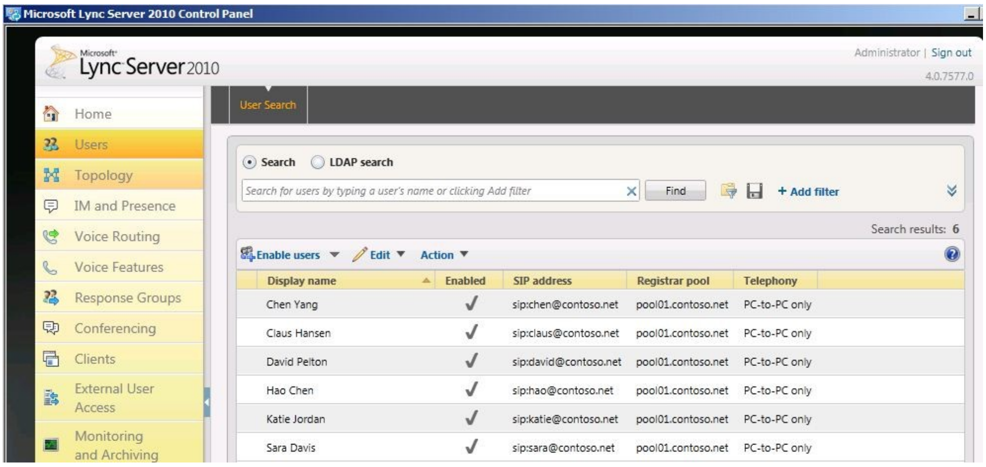
1. Log on to the Front End Server with an account that is a member of the RTCUniversalServerAdmins group or a member of the CsAdministrator or CsUserAdministrator administrative role.
2. Open the Lync Server Control Panel.
3. Select **Topology**. Verify that the various servers in your Lync Server 2010 deployment are listed.



Computer	Pool	Site	Status	Replication
director01.contoso.net	director01.contoso.net (Director)	Contoso		✓
edge01.contoso.net	edge01.contoso.net	Contoso	N/A	✓
fe1.contoso.net	pool01.contoso.net (Enterprise...	Contoso		✓
pstn-gw.contoso.net	pstn-gw.contoso.net	Contoso	N/A	N/A
sql.contoso.net	sql.contoso.net	Contoso	N/A	N/A

To review Lync Server 2010 users in Lync Server Control Panel

1. Open the Lync Server Control Panel.
2. Select **Users** and then click **Find**.
3. Verify that the **Registrar Pool** column points to the Lync Server 2010 pool for each user listed.

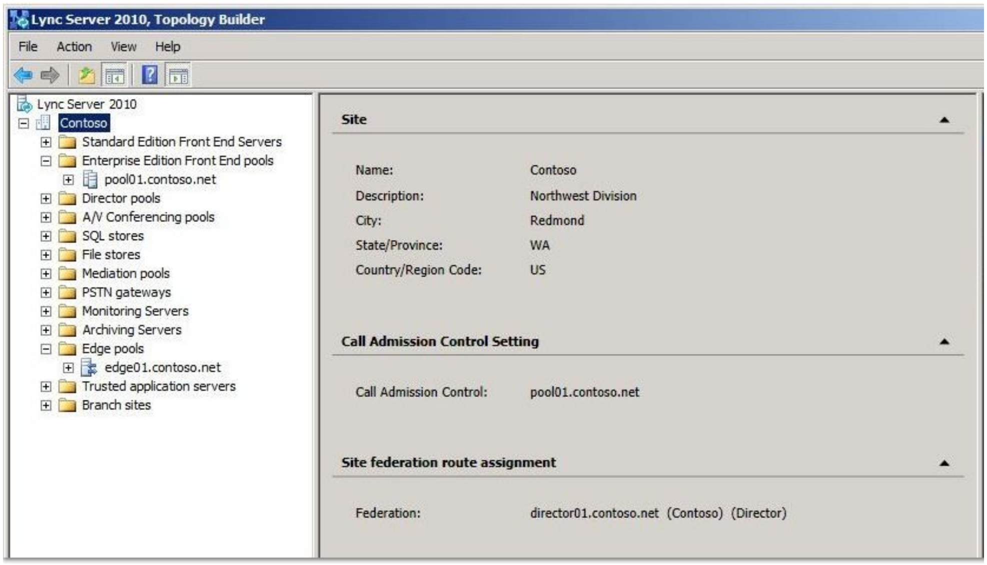


Search results: 6

Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	pool01.contoso.net	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	pool01.contoso.net	PC-to-PC only
David Pelton	✓	sip:david@contoso.net	pool01.contoso.net	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	pool01.contoso.net	PC-to-PC only
Katie Jordan	✓	sip:katie@contoso.net	pool01.contoso.net	PC-to-PC only
Sara Davis	✓	sip:sara@contoso.net	pool01.contoso.net	PC-to-PC only

To verify Lync Server 2010 Edge and Federation Settings

1. Start Topology Builder.
2. Select **Download Topology from existing deployment**.
3. Choose a file name and save the topology with the default .tbxml file type.
4. Expand the Lync Server 2010 node to reveal the various server roles in the deployment.
5. Select the site node and verify if a **Site federation route assignment** value is set.



Site

Name: Contoso
Description: Northwest Division
City: Redmond
State/Province: WA
Country/Region Code: US

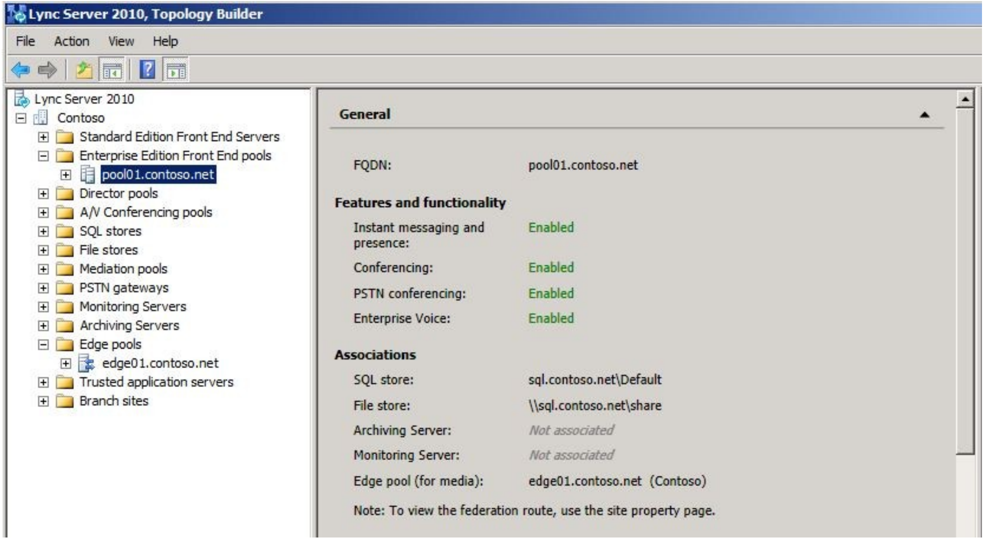
Call Admission Control Setting

Call Admission Control: pool01.contoso.net

Site federation route assignment

Federation: director01.contoso.net (Contoso) (Director)

6. Next, select the Standard Edition Server or Enterprise Edition front end pool. Determine if an Edge pool has been configured for Media below **Associations**.



General

FQDN: pool01.contoso.net

Features and functionality

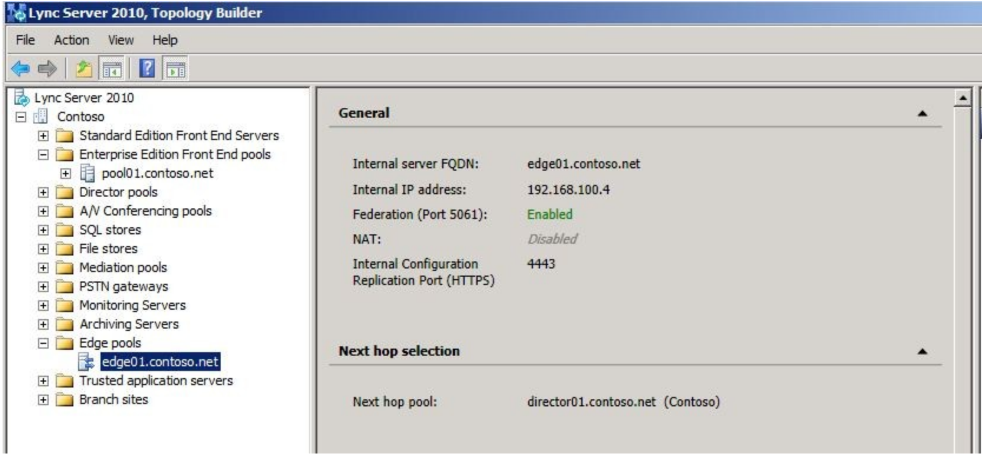
Instant messaging and presence: Enabled
Conferencing: Enabled
PSTN conferencing: Enabled
Enterprise Voice: Enabled

Associations

SQL store: sql.contoso.net\Default
File store: \\sql.contoso.net\share
Archiving Server: *Not associated*
Monitoring Server: *Not associated*
Edge pool (for media): edge01.contoso.net (Contoso)

Note: To view the federation route, use the site property page.

7. Finally, select the Edge pool and identify if a Next hop pool is configured below **Next hop selection**.



General

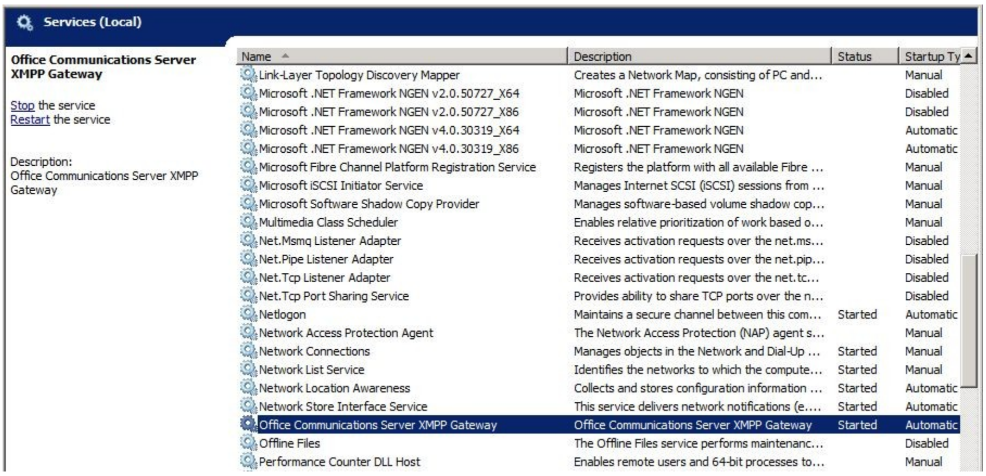
Internal server FQDN: edge01.contoso.net
Internal IP address: 192.168.100.4
Federation (Port 5061): Enabled
NAT: *Disabled*
Internal Configuration Replication Port (HTTPS) 4443

Next hop selection

Next hop pool: director01.contoso.net (Contoso)

Verify legacy XMPP Federated Partner Configuration

1. From the legacy XMPP server, navigate to the Administrative Tools\Services applet.
2. Verify that the Office Communications Server XMPP Gateway service is started.



Office Communications Server XMPP Gateway

Stop the service
Restart the service

Description:
Office Communications Server XMPP Gateway

Name	Description	Status	Startup Ty
Link-Layer Topology Discovery Mapper	Creates a Network Map, consisting of PC and...		Manual
Microsoft .NET Framework NGEN v2.0.50727_X64	Microsoft .NET Framework NGEN		Disabled
Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft .NET Framework NGEN		Disabled
Microsoft .NET Framework NGEN v4.0.30319_X64	Microsoft .NET Framework NGEN		Automatic
Microsoft .NET Framework NGEN v4.0.30319_X86	Microsoft .NET Framework NGEN		Automatic
Microsoft Fibre Channel Platform Registration Service	Registers the platform with all available Fibre ...		Manual
Microsoft iSCSI Initiator Service	Manages Internet SCSI (iSCSI) sessions from ...		Manual
Microsoft Software Shadow Copy Provider	Manages software-based volume shadow cop...		Manual
Multimedia Class Scheduler	Enables relative prioritization of work based o...		Manual
Net.Msmq Listener Adapter	Receives activation requests over the net.ms...		Disabled
Net.Pipe Listener Adapter	Receives activation requests over the net.pip...		Disabled
Net.Tcp Listener Adapter	Receives activation requests over the net.tc...		Disabled
Net.Tcp Port Sharing Service	Provides ability to share TCP ports over the n...		Disabled
Netlogon	Maintains a secure channel between this com...	Started	Automatic
Network Access Protection Agent	The Network Access Protection (NAP) agent s...		Manual
Network Connections	Manages objects in the Network and Dial-Up ...	Started	Manual
Network List Service	Identifies the networks to which the compute...	Started	Manual
Network Location Awareness	Collects and stores configuration information ...	Started	Automatic
Network Store Interface Service	This service delivers network notifications (e....	Started	Automatic
Office Communications Server XMPP Gateway	Office Communications Server XMPP Gateway	Started	Automatic
Offline Files	The Offline Files service performs maintenanc...		Disabled
Performance Counter DLL Host	Enables remote users and 64-bit processes to...		Manual

1.6.1.4 Phase 3: Deploy Lync Server 2013 Pilot Pool

Phase 3: Deploy Lync Server 2013 Pilot Pool

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010 to Lync Server 2013 >

Topic Last Modified: *2012-10-19*

This section covers the steps required to deploy a pilot pool of Lync Server 2013. The deployment of Lync Server 2013 requires using Topology Builder to define your topology and the components you want to deploy, preparing your environment for deployment of the Lync Server 2013 components, publishing your topology design on the first Front End Server, and then installing and configuring Lync Server 2013 software for the components for your deployment. When completed, your Lync Server 2013 pilot pool deployment will coexist with an existing Lync Server 2010 pool.

In This Section

- Prepare Active Directory for Lync Server
- Download Topology From Existing Deployment
- Deploy Lync Server 2013 Pilot Pool
- Verify Pilot Pool Coexistence with Legacy Pool
- Connect Pilot Pool to Legacy Edge Servers
- Configure XMPP Gateway Access Policies and Certificates

1.6.1.4.1 Prepare Active Directory for Lync Server

Prepare Active Directory for Lync Server

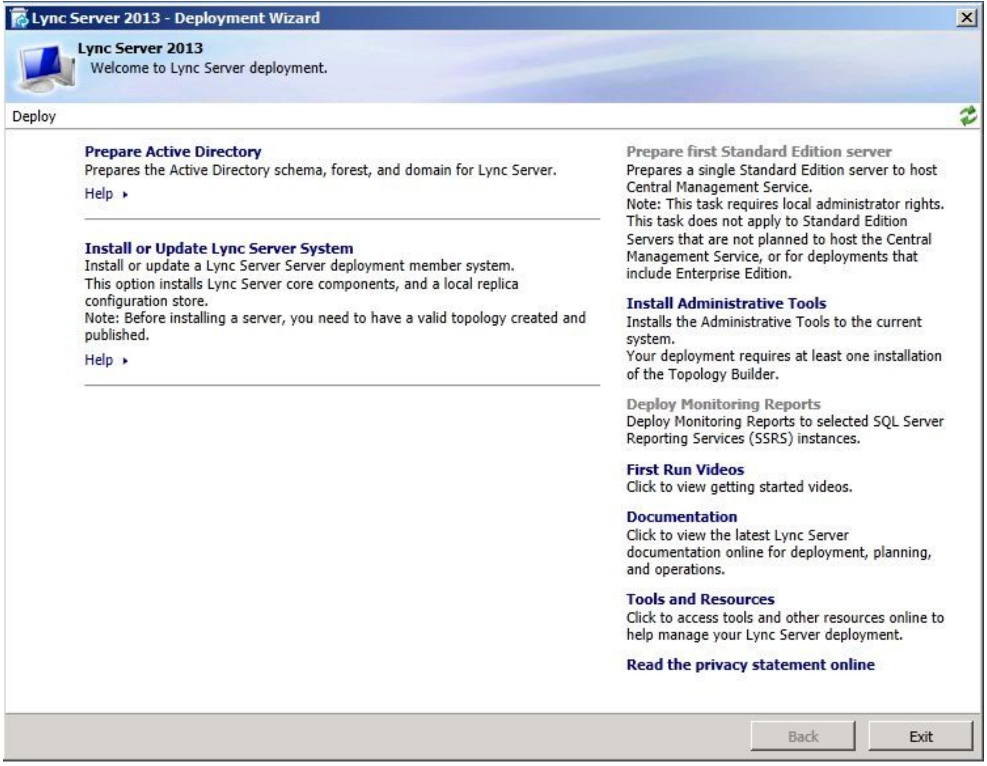
Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

Topic Last Modified: *2012-09-17*

Prior to deploying Lync Server 2013 in a coexistence state with Lync Server 2010, you must perform some additional Active Directory tasks to configure the schema, forest, and domain for Lync Server 2013. The schema extensions add the Active Directory classes and attributes that are required by Lync Server 2013. For additional information, see the topic Preparing Active Directory Domain Services for Lync Server 2013.

To prepare Active Directory for Lync Server 2013

1. On the Lync Server 2013 Front End Server, run Lync Server 2013 Setup.
2. Select **Prepare Active Directory**.



Lync Server 2013 - Deployment Wizard

Lync Server 2013

Welcome to Lync Server deployment.

Deploy

Prepare Active Directory
Prepares the Active Directory schema, forest, and domain for Lync Server.
Help ▸

Install or Update Lync Server System
Install or update a Lync Server Server deployment member system.
This option installs Lync Server core components, and a local replica configuration store.
Note: Before installing a server, you need to have a valid topology created and published.
Help ▸

Prepare first Standard Edition server
Prepares a single Standard Edition server to host Central Management Service.
Note: This task requires local administrator rights.
This task does not apply to Standard Edition Servers that are not planned to host the Central Management Service, or for deployments that include Enterprise Edition.

Install Administrative Tools
Installs the Administrative Tools to the current system.
Your deployment requires at least one installation of the Topology Builder.

Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

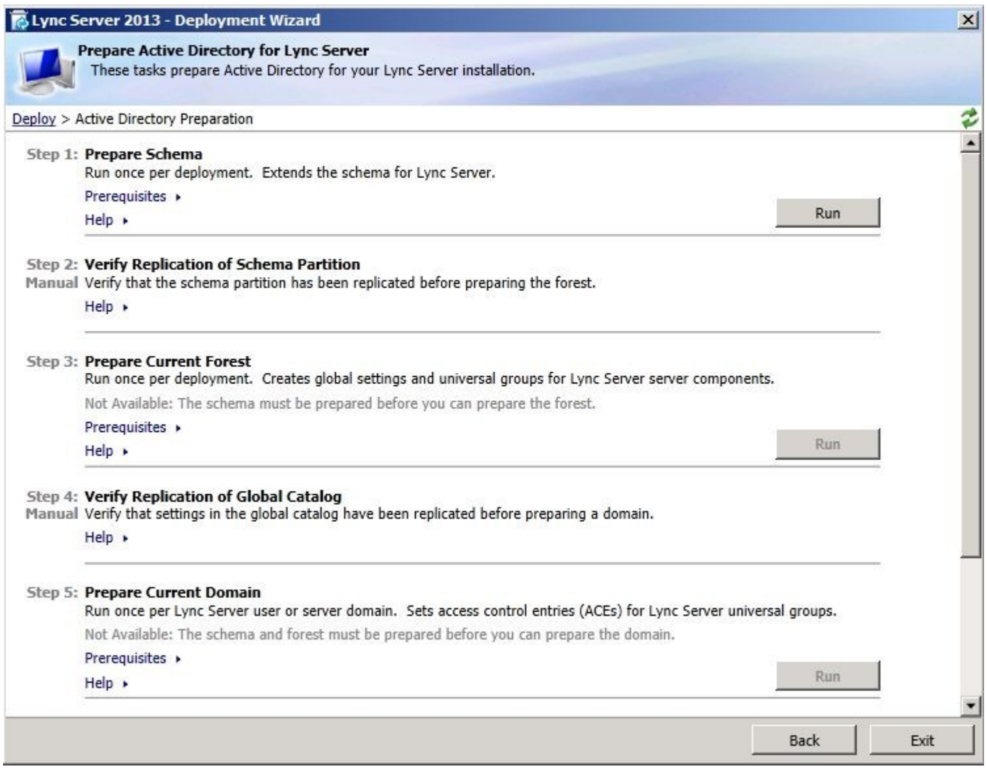
First Run Videos
Click to view getting started videos.

Documentation
Click to view the latest Lync Server documentation online for deployment, planning, and operations.

Tools and Resources
Click to access tools and other resources online to help manage your Lync Server deployment.

Read the privacy statement online

3. Complete steps 1 through 5.



Lync Server 2013 - Deployment Wizard

Prepare Active Directory for Lync Server

These tasks prepare Active Directory for your Lync Server installation.

Deploy > Active Directory Preparation

Step 1: Prepare Schema
Run once per deployment. Extends the schema for Lync Server.

Step 2: Verify Replication of Schema Partition
Manual Verify that the schema partition has been replicated before preparing the forest.

Step 3: Prepare Current Forest
Run once per deployment. Creates global settings and universal groups for Lync Server server components.
Not Available: The schema must be prepared before you can prepare the forest.

Step 4: Verify Replication of Global Catalog
Manual Verify that settings in the global catalog have been replicated before preparing a domain.

Step 5: Prepare Current Domain
Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups.
Not Available: The schema and forest must be prepared before you can prepare the domain.

1.6.1.4.2 Download Topology From Existing Deployment

Download Topology From Existing Deployment

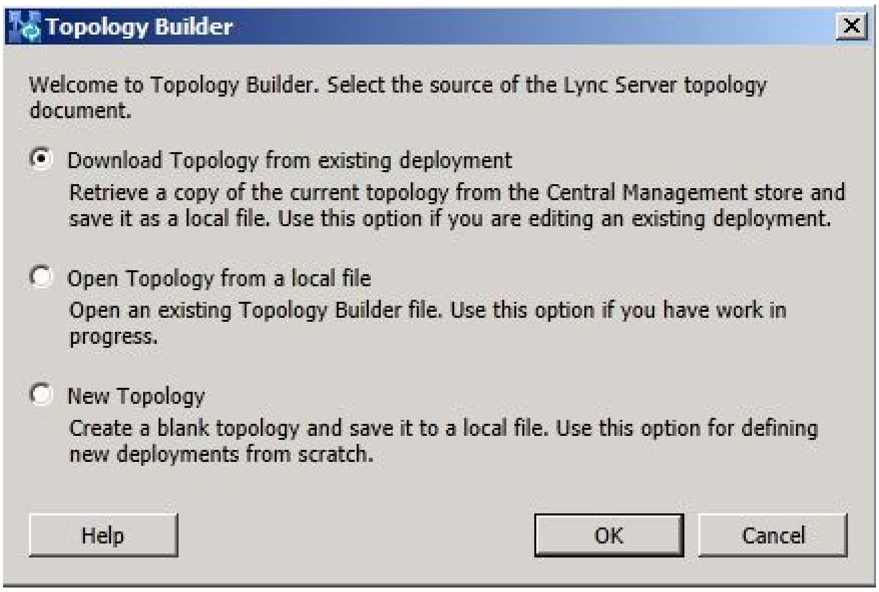
Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

Topic Last Modified: *2012-09-29*

When creating a Lync Server 2013 pool, you will use the Central Management Store that is associated with Lync Server 2010. When you start Topology Builder on first use and subsequent edit sessions, you are prompted for the location where you want Topology Builder to load the current configuration document. Because you already have a Lync Server 2010 topology defined and have established the Central Management store, you should choose to download a topology from an existing deployment. Topology Builder will read the database and retrieve the current definition.

To download a topology from an existing deployment

1. Open the **Lync Server Deployment Wizard**.
2. From the **Lync Server 2013 – Deployment Wizard** page, click **Install Administrative Tools**.
3. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013** , and then click **Lync Server Topology Builder**.
4. Select **Download Topology from existing deployment**.



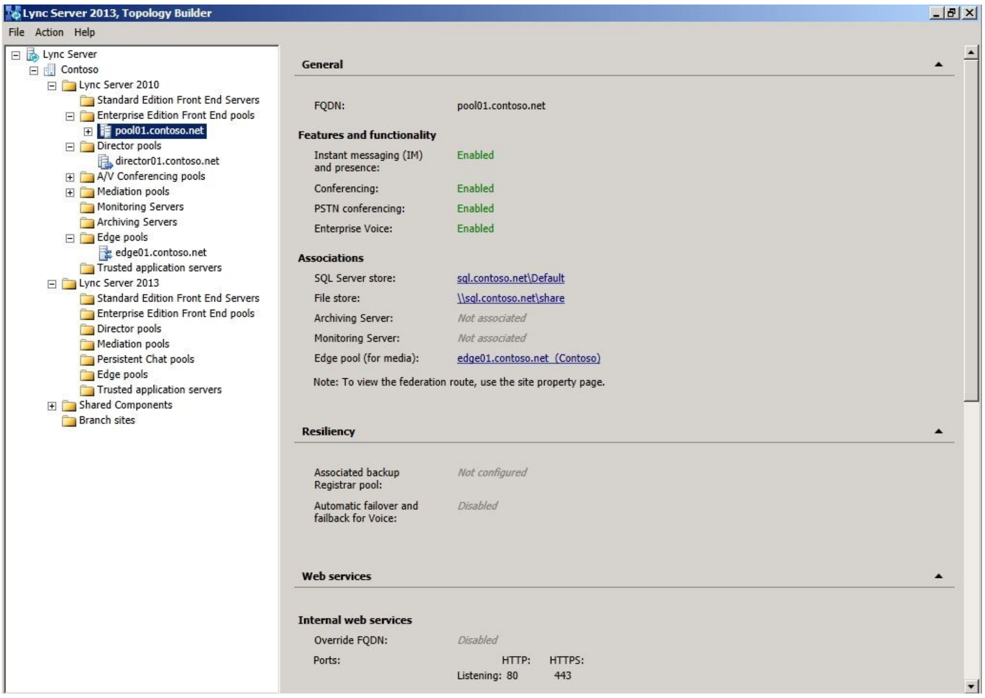
Welcome to Topology Builder. Select the source of the Lync Server topology document.

● Download Topology from existing deployment
Retrieve a copy of the current topology from the Central Management store and save it as a local file. Use this option if you are editing an existing deployment.

○ Open Topology from a local file
Open an existing Topology Builder file. Use this option if you have work in progress.

○ New Topology
Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.

5. Choose a file name and save the topology with the default .tbxml file type.
6. Expand the Lync Server node, as shown, to reveal the various server roles in the deployment.



General

FQDN: pool01.contoso.net

Features and functionality

Instant messaging (IM) and presence: Enabled
Conferencing: Enabled
PSTN conferencing: Enabled
Enterprise Voice: Enabled

Associations

SQL Server store: sql.contoso.net\Default
File store: \\sql.contoso.net\share
Archiving Server: Not associated
Monitoring Server: Not associated
Edge pool (for media): edge01.contoso.net (Contoso)

Note: To view the federation route, use the site property page.

Resiliency

Associated backup Registrar pool: Not configured
Automatic failover and failback for Voice: Disabled

Web services

Internal web services

Override FQDN: Disabled
Ports: HTTP: HTTPS:
Listening: 80 443

1.6.1.4.3 Deploy Lync Server 2013 Pilot Pool

Deploy Lync Server 2013 Pilot Pool

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

Topic Last Modified: *2012-09-29*

One of the first steps required for migration to Lync Server 2013 is to deploy a pilot pool. The pilot pool is where you test coexistence of Lync Server 2013 with your Lync Server 2010 deployment. Coexistence is a temporary state that lasts until you have moved all users and pools to Lync Server 2013.

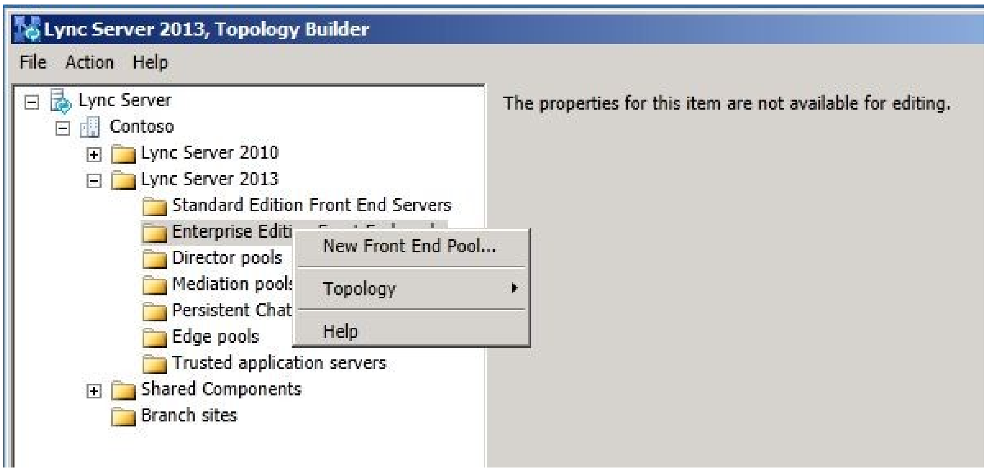
When you deploy a pilot pool, you use the Define New Front End Pool wizard. You should deploy the same features and workloads in your Lync Server 2013 pilot pool that you have in your Lync Server 2010 pool. If you deployed Archiving Server, Monitoring Server, or System Center Operations Manager for archiving or monitoring your Lync Server 2010 environment, and you want to continue archiving or monitoring throughout the migration, you need to also deploy these features in your pilot environment. The version you deployed to archive or monitor your Lync Server 2010 environment will not capture data in your Lync Server 2013 environment.

Note:

The following procedure discusses features and settings you should consider as part of your overall pilot pool deployment process. This section only highlights key points you should consider as part of your pilot pool deployment. For detailed steps, refer to the Deploying Lync Server 2013 deployment guide.

To deploy a Lync Server 2013 pilot pool

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Expand the tree until you reach **Lync Server 2013 Enterprise Edition Front End pools**.
3. Right click **Enterprise Edition Front End pools**, and select **New Front End Pool**.

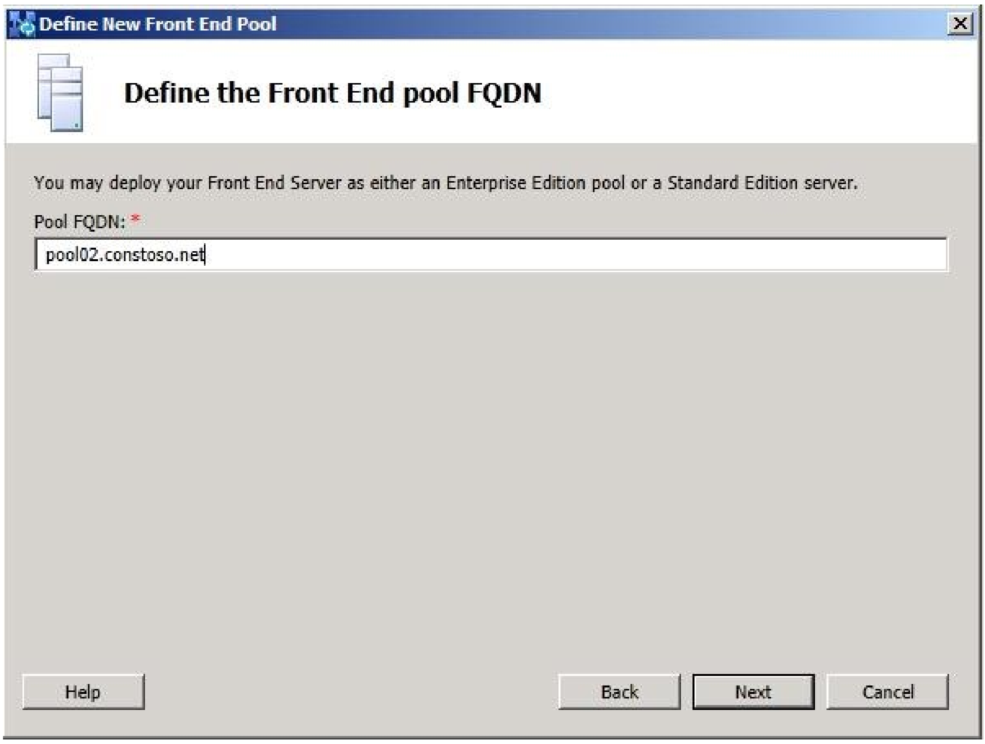


The properties for this item are not available for editing.

4. Enter the pool FQDN. When you define your pilot pool, you can choose to deploy an Enterprise Edition Front End pool or a Standard Edition server. Lync Server 2013 does not require that your pilot pool features match what was deployed in your legacy pool.

Warning:

The pool or server fully qualified domain name (FQDN) that you define for the pilot pool must be unique. It cannot match the name of the currently deployed Lync Server 2010 pool, or any other servers currently deployed.



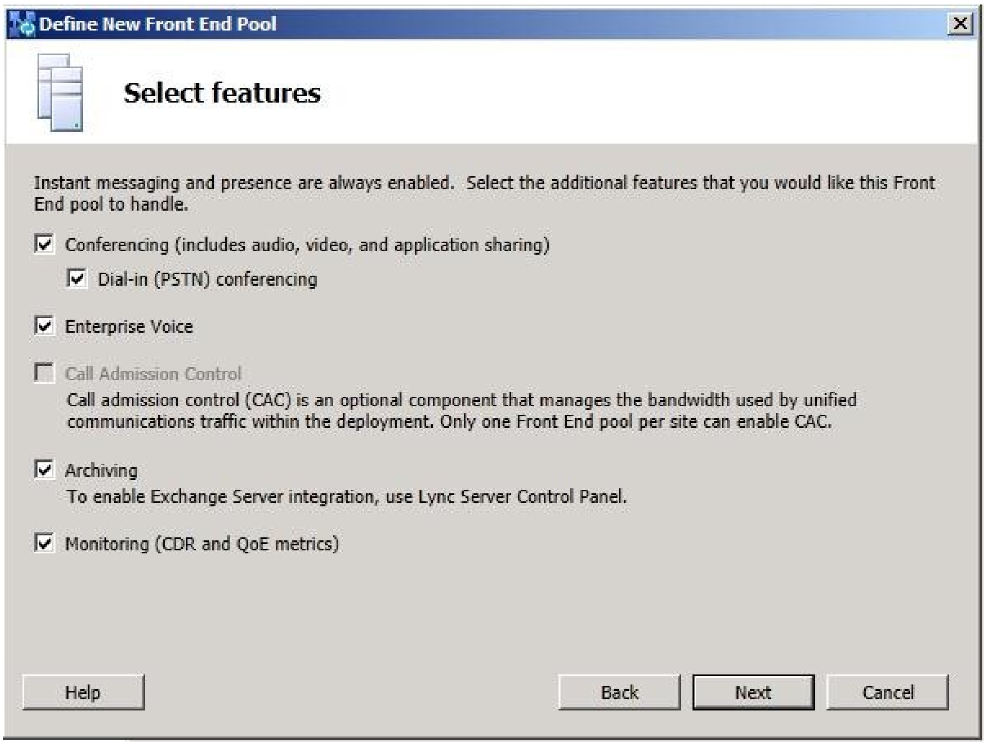
Define the Front End pool FQDN

You may deploy your Front End Server as either an Enterprise Edition pool or a Standard Edition server.

Pool FQDN: *

pool02.constoso.net

5. On the **Select features** page, select the check boxes for the features that you want on this Front End pool. For example, if you are deploying only instant messaging (IM) and presence features, you would select the Conferencing check box to allow multiparty IM, but would not select the Dial-in (PSTN) conferencing, Enterprise Voice, or Call Admission Control check boxes, because they represent voice, video, and collaborative conferencing features. For additional information on selecting features, see Define and Configure a Front End Pool or Standard Edition Server in the Deployment documentation.



Define New Front End Pool

Select features

Instant messaging and presence are always enabled. Select the additional features that you would like this Front End pool to handle.

☑ Conferencing (includes audio, video, and application sharing)

☑ Dial-in (PSTN) conferencing

☑ Enterprise Voice

□ Call Admission Control

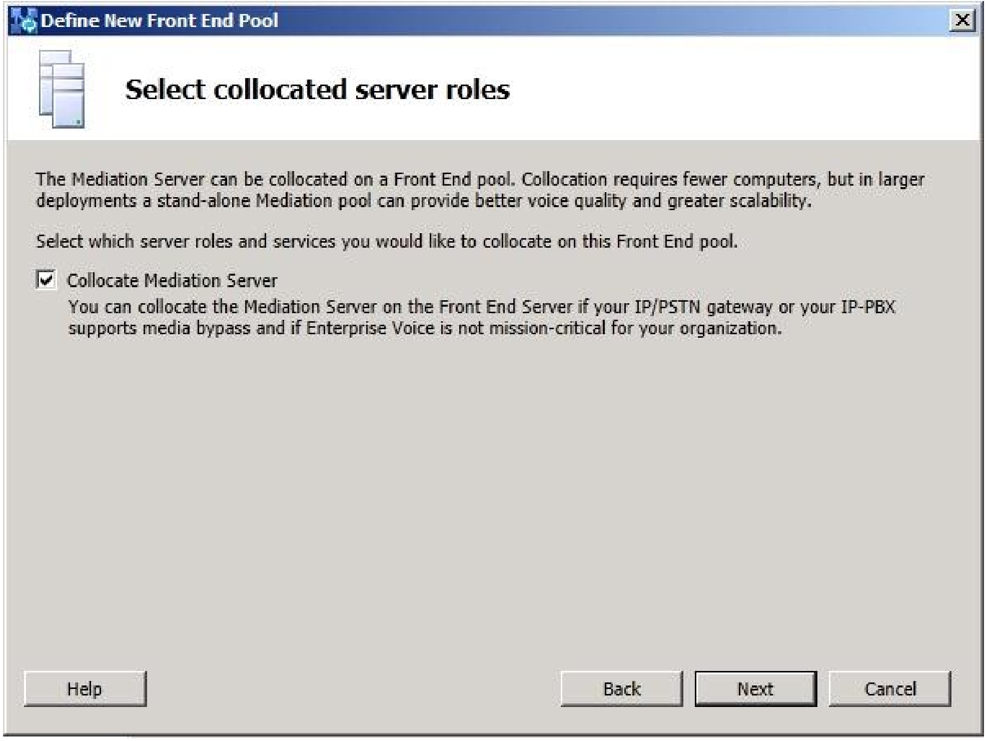
Call admission control (CAC) is an optional component that manages the bandwidth used by unified communications traffic within the deployment. Only one Front End pool per site can enable CAC.

☑ Archiving

To enable Exchange Server integration, use Lync Server Control Panel.

☑ Monitoring (CDR and QoE metrics)

6. On the **Select collocated server roles** page, we recommend you collocate the Mediation Server in Lync Server 2013. When merging a legacy topology with Lync Server 2013, we require that you first collocate the Lync Server 2013 Mediation Server. After merging the topologies and configuring the Lync Server 2013 Mediation Server, you can decide to keep the collocated Mediation Server or change it to a stand-alone server in your Lync Server 2013 deployment.



Define New Front End Pool

Select collocated server roles

The Mediation Server can be collocated on a Front End pool. Collocation requires fewer computers, but in larger deployments a stand-alone Mediation pool can provide better voice quality and greater scalability.

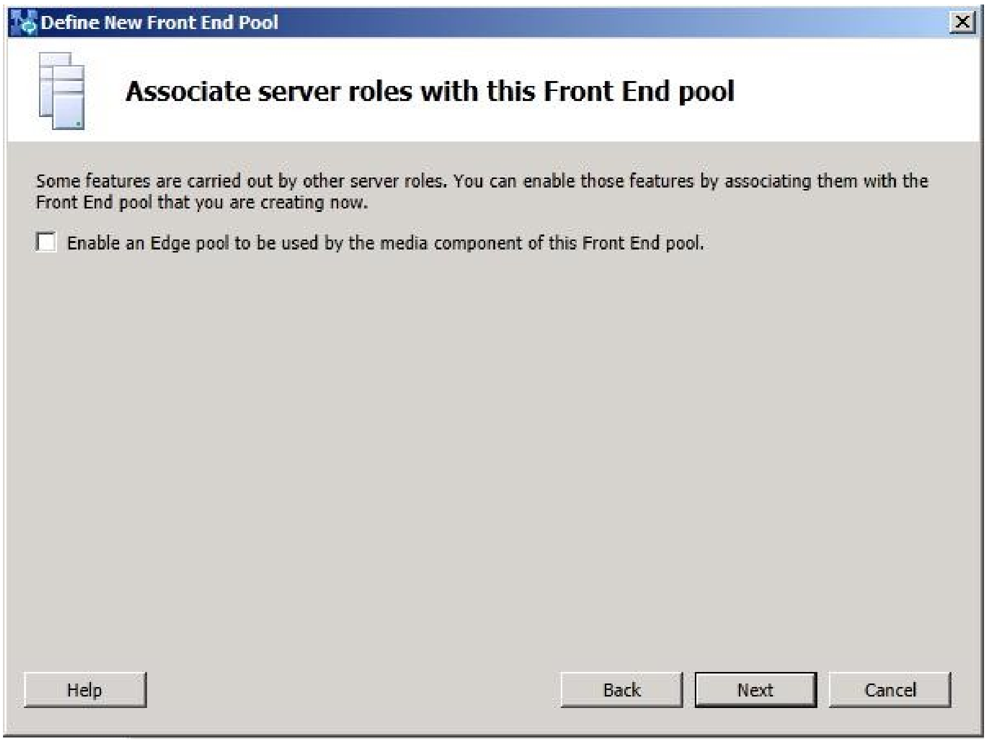
Select which server roles and services you would like to collocate on this Front End pool.

☑ Collocate Mediation Server

You can collocate the Mediation Server on the Front End Server if your IP/PSTN gateway or your IP-PBX supports media bypass and if Enterprise Voice is not mission-critical for your organization.

7. On the **Associate server roles with this Front End pool** page, during pilot

pool deployment, do not choose the **Enable an Edge pool to be used by the media component of this Front End pool** option. This is a feature you will enable and bring online in a later phase of migration. Keep this setting cleared for now.



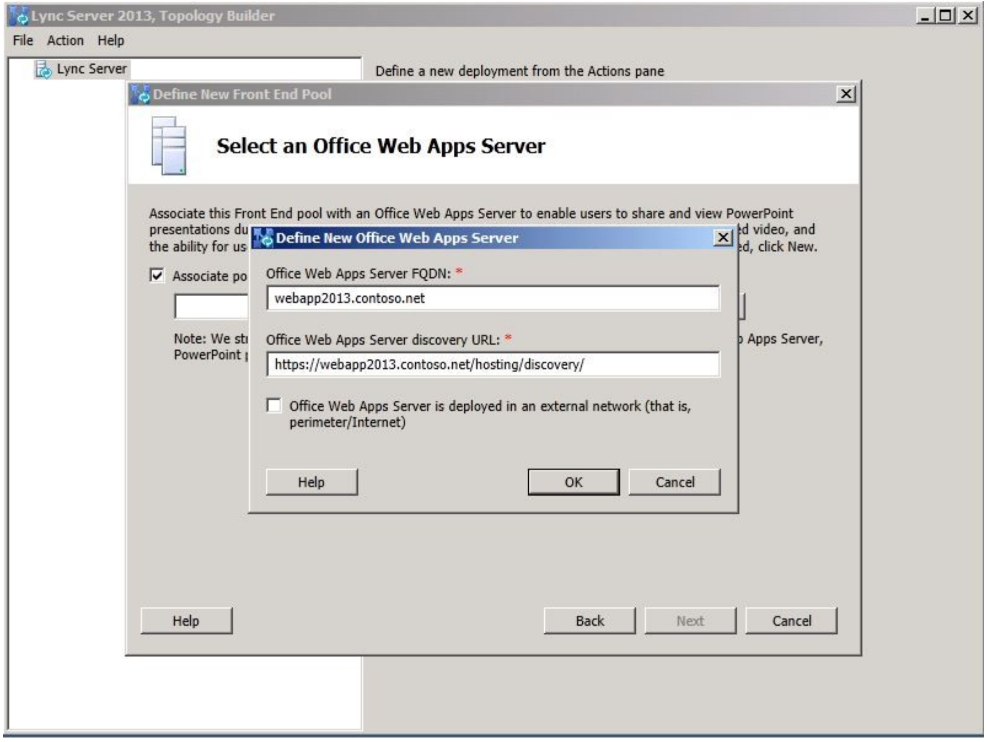
Define New Front End Pool

Associate server roles with this Front End pool

Some features are carried out by other server roles. You can enable those features by associating them with the Front End pool that you are creating now.

☐ Enable an Edge pool to be used by the media component of this Front End pool.

8. On the **Select an Office Web Apps Server** page, click **New**, and specify the FQDN of the application server.



Lync Server 2013, Topology Builder

Define a new deployment from the Actions pane

Define New Front End Pool

Select an Office Web Apps Server

Associate this Front End pool with an Office Web Apps Server to enable users to share and view PowerPoint presentations du… …d video, and the ability for us… …d, click New.

☑ Associate po…

Note: We st… …Apps Server, PowerPoint …

Define New Office Web Apps Server

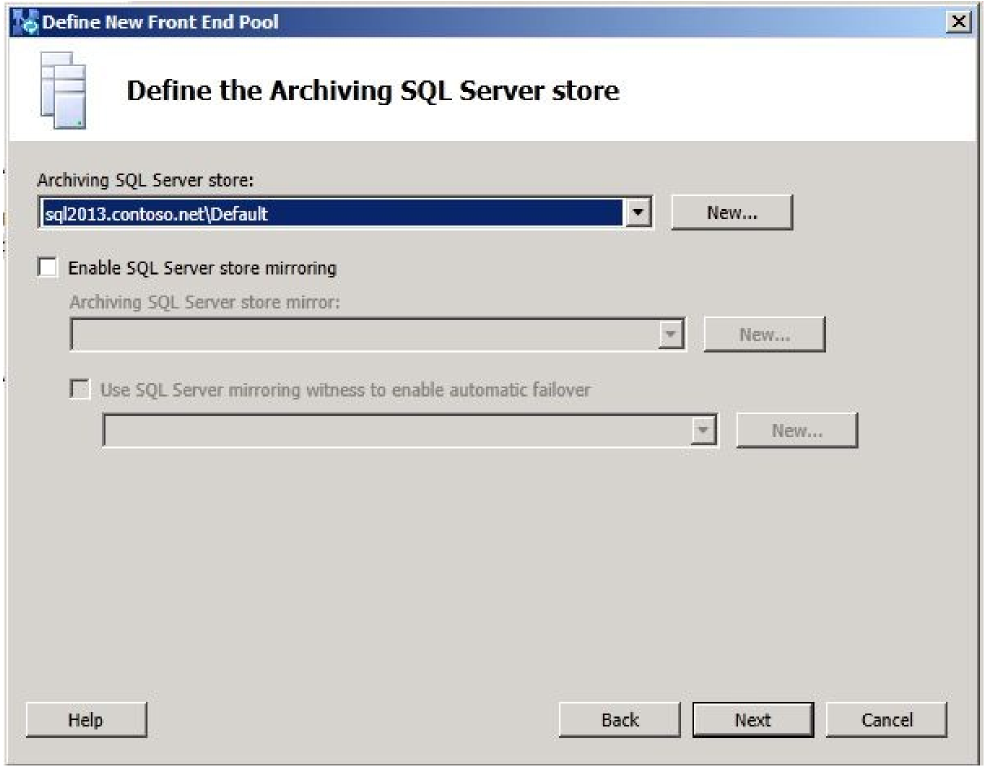
Office Web Apps Server FQDN: *
webapp2013.contoso.net

Office Web Apps Server discovery URL: *
https://webapp2013.contoso.net/hosting/discovery/

☐ Office Web Apps Server is deployed in an external network (that is, perimeter/Internet)

9. On the **Define the Archiving SQL Server store** page, when defining the SQL Server store for both Lync Server Archiving and Monitoring, select the SQL

Server instance created earlier for Lync Server 2013.


Define New Front End Pool
Define the Archiving SQL Server store
New...
New...
New...
Help
Back
Next
Cancel

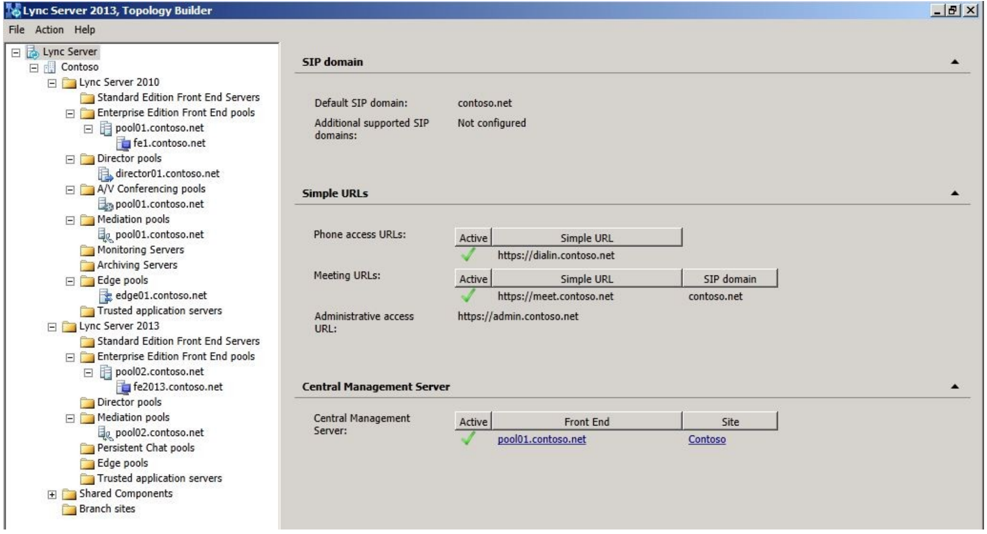
Archiving SQL Server store: sql2013.contoso.net\Default

☐ Enable SQL Server store mirroring

Archiving SQL Server store mirror:

☐ Use SQL Server mirroring witness to enable automatic failover

10.To publish your topology, right-click the **Lync Server** node, and then click **Publish Topology**.



SIP domain

Default SIP domain: contoso.net

Additional supported SIP domains: Not configured

Simple URLs

Phone access URLs:

Active	Simple URL
✓	https://dialin.contoso.net

Meeting URLs:

Active	Simple URL	SIP domain
✓	https://meet.contoso.net	contoso.net

Administrative access URL: https://admin.contoso.net

Central Management Server

Central Management Server:

Active	Front End	Site
✓	pool01.contoso.net	Contoso

11.When the publish process has completed, click **Finish**.

To install a local copy of the configuration store and start the required services, see Setting Up Front End Servers and Front End Pools in the Deployment documentation.

1.6.1.4.4 Verify Pilot Pool Coexistence with Legacy Pool

Verify Pilot Pool Coexistence with Legacy Pool

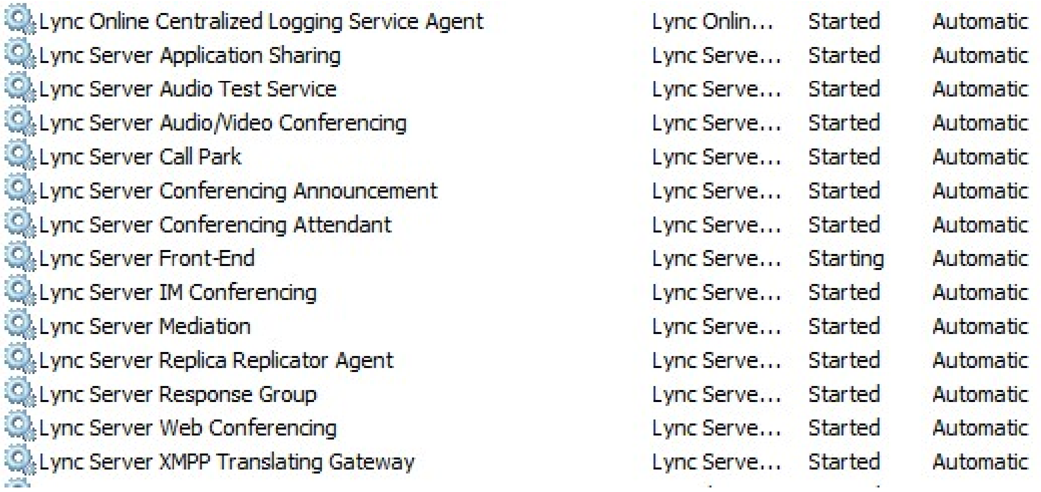
Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

Topic Last Modified: *2012-09-29*

After you deploy the pilot pool, you need to verify the coexistence of the two pools by using the administrative tools to view the pool information. For the Lync Server 2013 pools and legacy pools, you must use the Lync Server 2013 Control Panel and Topology Builder tools.

Verify that Lync Server 2013 services have started

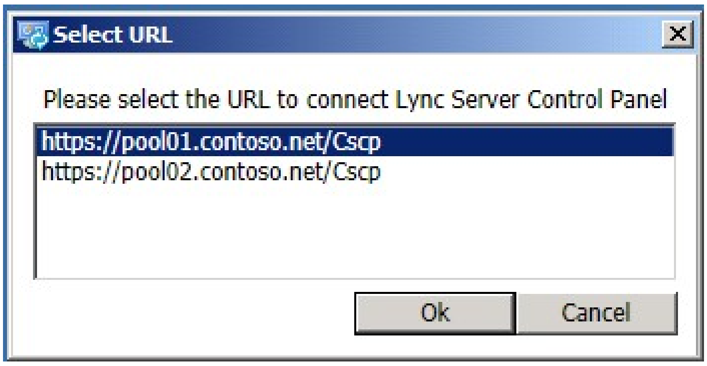
1. From the Lync Server 2013 Front End Server, navigate to the Administrative Tools\Services applet.
2. Verify that the following services are running on the Front End Server:



Lync Online Centralized Logging Service Agent	Lync Onlin...	Started	Automatic
Lync Server Application Sharing	Lync Serve...	Started	Automatic
Lync Server Audio Test Service	Lync Serve...	Started	Automatic
Lync Server Audio/Video Conferencing	Lync Serve...	Started	Automatic
Lync Server Call Park	Lync Serve...	Started	Automatic
Lync Server Conferencing Announcement	Lync Serve...	Started	Automatic
Lync Server Conferencing Attendant	Lync Serve...	Started	Automatic
Lync Server Front-End	Lync Serve...	Starting	Automatic
Lync Server IM Conferencing	Lync Serve...	Started	Automatic
Lync Server Mediation	Lync Serve...	Started	Automatic
Lync Server Replica Replicator Agent	Lync Serve...	Started	Automatic
Lync Server Response Group	Lync Serve...	Started	Automatic
Lync Server Web Conferencing	Lync Serve...	Started	Automatic
Lync Server XMPP Translating Gateway	Lync Serve...	Started	Automatic

Open the Lync Server 2013 Control Panel

From the Front End Server in your Lync Server 2013 deployment, open the Lync Server 2013 Control Panel and select the Lync Server 2010 pool. Repeat the procedure to open the Lync Server 2013 pool.



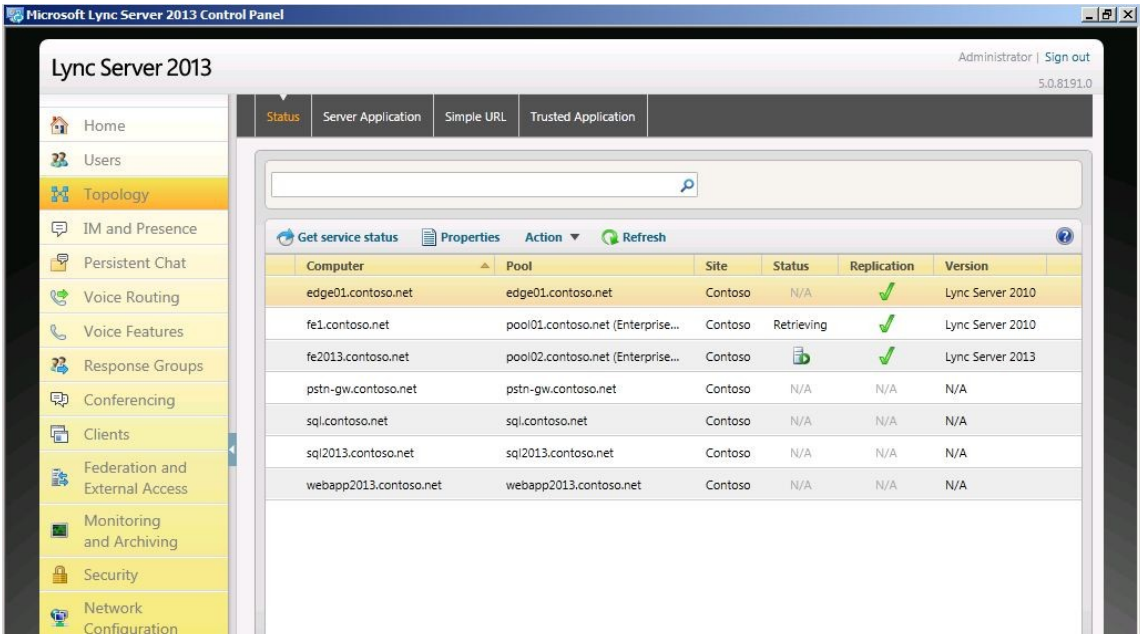
Please select the URL to connect Lync Server Control Panel

https://pool01.contoso.net/Cscp
https://pool02.contoso.net/Cscp

Important:

On Lync Server 2013, you must upgrade Silverlight to Silverlight version 5 prior to using the Lync Server Control Panel.

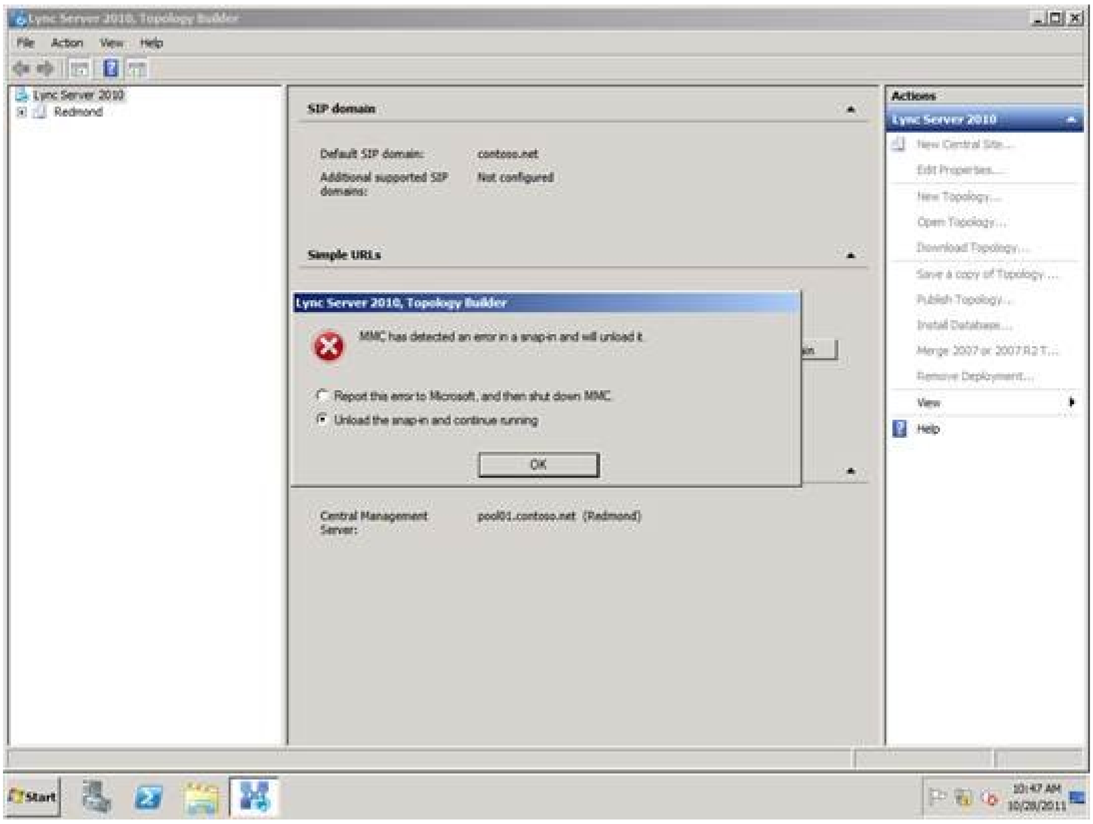
This topology now includes Lync Server 2010 and Lync Server 2013 server roles.



Computer	Pool	Site	Status	Replication	Version
edge01.contoso.net	edge01.contoso.net	Contoso	N/A	✓	Lync Server 2010
fe1.contoso.net	pool01.contoso.net (Enterprise...	Contoso	Retrieving	✓	Lync Server 2010
fe2013.contoso.net	pool02.contoso.net (Enterprise...	Contoso		✓	Lync Server 2013
pstn-gw.contoso.net	pstn-gw.contoso.net	Contoso	N/A	N/A	N/A
sql.contoso.net	sql.contoso.net	Contoso	N/A	N/A	N/A
sql2013.contoso.net	sql2013.contoso.net	Contoso	N/A	N/A	N/A
webapp2013.contoso.net	webapp2013.contoso.net	Contoso	N/A	N/A	N/A

Don’t attempt to open the topology in Lync Server 2010 Topology Builder

If you attempt to open the topology using Lync Server 2010 Topology Builder, you will encounter the error below. The topology can only be viewed using Lync Server 2013 Topology Builder. The Lync Server 2013 Topology Builder must be used to create pools for both Lync Server 2013 and Lync Server 2010.



SIP domain

Default SIP domain: contoso.net

Additional supported SIP domains: Not configured

Simple URLs

Lync Server 2010, Topology Builder

MMC has detected an error in a snap-in and will unload it.

○ Report this error to Microsoft, and then shut down MMC

● Unload the snap-in and continue running

OK

Central Management Server: pool01.contoso.net (Redmond)

1.6.1.4.5 Connect Pilot Pool to Legacy Edge Servers

Connect Pilot Pool to Legacy Edge Servers

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

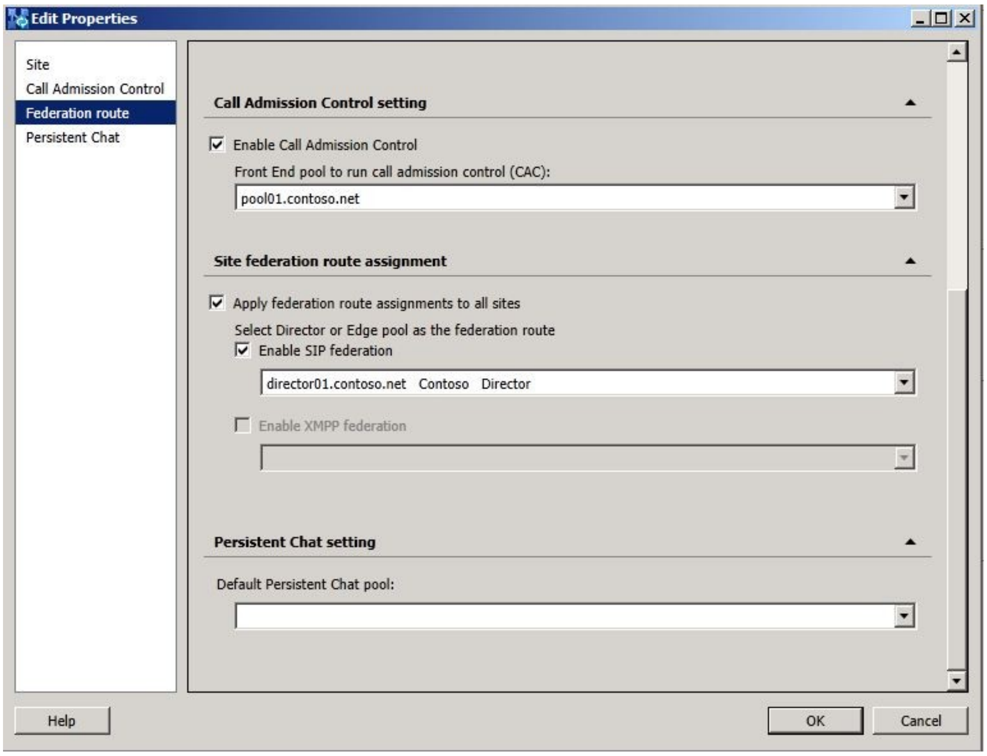
Topic Last Modified: *2012-09-29*

After deploying Lync Server 2013, you need to configure a federation route for your site. In order to use the federated route that is being used by Lync Server 2010, Lync Server 2013 must be configured to use this route.

To enable the Lync Server 2013 site to use the Director and Edge Server of the Lync Server 2010 deployment, use Topology Builder to associate the legacy Edge pool.

To associate the legacy Edge pool by using Topology Builder

1. Open **Topology Builder**.
2. Select your site, which is directly below the **Lync Server** node.
3. On the **Actions** menu, click **Edit Properties**.
4. In the left pane, select **Federation route**.
5. Under **Site federation route assignment**, select **Enable SIP federation**, and then select the Lync Server 2010 Director, or the Lync Server 2010 Edge Server if no Director is listed.



Call Admission Control setting

☑ Enable Call Admission Control

Front End pool to run call admission control (CAC): pool01.contoso.net

Site federation route assignment

☑ Apply federation route assignments to all sites

Select Director or Edge pool as the federation route

☑ Enable SIP federation

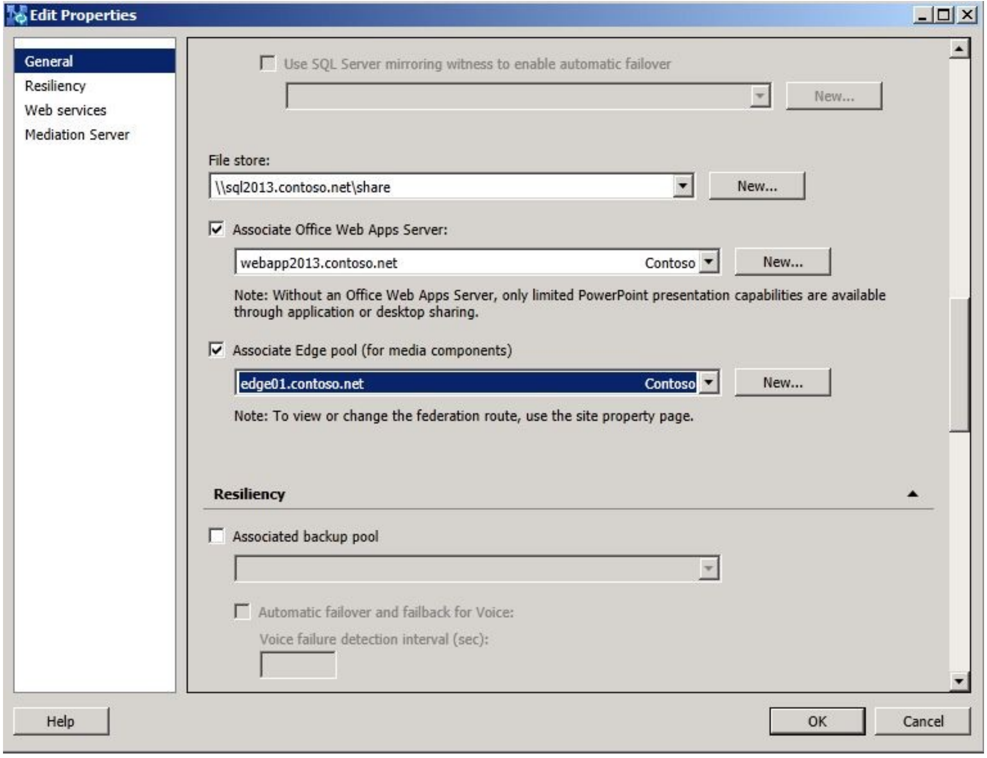
director01.contoso.net Contoso Director

□ Enable XMPP federation

Persistent Chat setting

Default Persistent Chat pool:

6. Click **OK** to close the **Edit Properties** page.
7. In Topology Builder, under the Lync Server 2013 node, navigate to the **Standard Edition server** or **Enterprise Edition Front End pools**, right-click the pool, and then click **Edit Properties**.
8. Under **Associations**, select the check box next to **Associate Edge pool (for media components)**.
9. From the list, select the legacy Edge Server.



□ Use SQL Server mirroring witness to enable automatic failover

File store: \\sql2013.contoso.net\share

☑ Associate Office Web Apps Server: webapp2013.contoso.net Contoso

Note: Without an Office Web Apps Server, only limited PowerPoint presentation capabilities are available through application or desktop sharing.

☑ Associate Edge pool (for media components): edge01.contoso.net Contoso

Note: To view or change the federation route, use the site property page.

Resiliency

□ Associated backup pool

□ Automatic failover and failback for Voice:

Voice failure detection interval (sec):

10. Click **OK** to close the **Edit Properties** page.
11. In **Topology Builder**, select the top-most node, **Lync Server**.
12. From the **Action** menu, click **Publish Topology**, and then click **Next**.
13. When the **Publishing wizard** completes, click **Finish**.

1.6.1.4.6 Configure XMPP Gateway Access Policies and Certificates

Configure XMPP Gateway Access Policies and Certificates

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

***Topic Last Modified:** 2012-10-15*

XMPP federation defines an external deployment based on the eXtensible Messaging and Presence Protocol (XMPP). An XMPP configuration allows Lync users access to XMPP domain users by:

- IM and Presence – person to person only
- Creation of XMPP federated contacts in the Lync client

When you configure policies for support of extensible messaging and presence protocol (XMPP) federated partners, the policies apply to users of XMPP federated domains, but not to users of session initiation protocol (SIP) instant messaging (IM) service providers (for example, Windows Live), or SIP federated domains. You configure an XMPP Federated Partner for each XMPP federated domain that you want to allow your users to add contacts and communicate with. Once the policies are in place, you need to configure the XMPP Gateway certificates.

Note:

To begin the XMPP Gateway migration, you need to deploy the Lync Server 2013 XMPP Gateway, and configure access policies to enable users for Lync Server 2013 XMPP Gateway. All users must be moved to the Lync Server 2013 deployment before you perform these steps. For details, see Configure XMPP Gateway on Lync Server 2013.

⊟Configure an External Access Policy to Enable Users for Lync Server 2013 XMPP Gateway

1. Open Lync Server Control Panel.
2. In the left navigation bar, click **Federation and External Access**, and then click **External Access Policy**.
3. Click **New** and then click **User policy**.
4. Enter a name for the external access user policy.
5. Provide a description for external access user policy.
6. Select **Enable communications with federated users**.
7. Select **Enable communications with XMPP federated users**.
8. Click **Commit** to save your changes to the site or user policy.

1.6.1.5 Phase 4: Move test users to the Pilot Pool

Phase 4: Move test users to the Pilot Pool

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010 to Lync Server 2013 >

***Topic Last Modified:** 2012-09-26*

You can move a single user or groups of users to your new Microsoft Lync Server 2013 deployment using the following two methods: Lync Server Control Panel and Lync Server Management Shell. The topics in this section describe tasks you must complete during pilot deployment, as well as prior to moving your deployment of Lync Server 2013 from a pilot deployment to a production-level deployment.

In This Section

- View Current Users in Lync Server 2010 Pool
- Verify User Replication Has Completed
- Move a single user to the Pilot Pool
- Move multiple users to the Pilot Pool

1.6.1.5.1 View Current Users in Lync Server 2010 Pool

View Current Users in Lync Server 2010 Pool

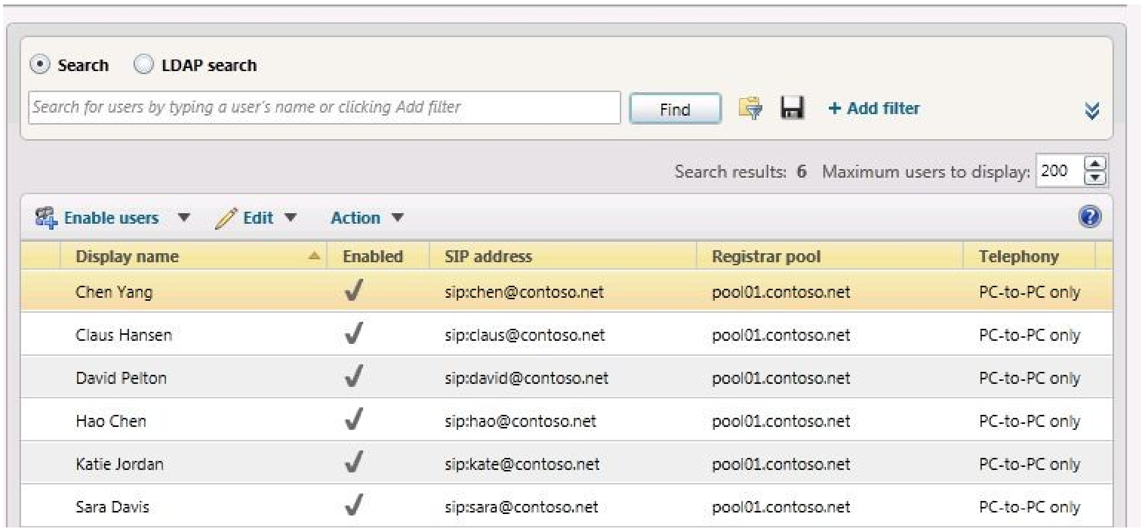
Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 4: Move test users to the Pilot Pool >

Topic Last Modified: *2012-09-26*

Prior to learning the various ways you can move users between pools, we must first determine what users exist in the legacy Lync Server 2010 pool. In the image below, the Registrar pool column identifies six users who are configured for the legacy Lync Server 2010 pool. These are the test users we will move to the Lync Server 2013 pool.

To see the list of users in the Lync Server 2010 pool

1. Log on to the Lync Server 2010 Front End Server with an account that is a member of the RTCUniversalServerAdmins group or a member of the CsAdministrator or CsUserAdministrator administrative role.
2. Open **Lync Server Control Panel**.
3. Click **Users**, click Search, and then click **Find**.


● Search
○ LDAP search
Search for users by typing a user's name or clicking Add filter
Find
+ Add filter
Enable users
Edit
Action

Search results: 6 Maximum users to display: 200

Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	pool01.contoso.net	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	pool01.contoso.net	PC-to-PC only
David Pelton	✓	sip:david@contoso.net	pool01.contoso.net	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	pool01.contoso.net	PC-to-PC only
Katie Jordan	✓	sip:kate@contoso.net	pool01.contoso.net	PC-to-PC only
Sara Davis	✓	sip:sara@contoso.net	pool01.contoso.net	PC-to-PC only

1.6.1.5.2 Verify User Replication Has Completed

Verify User Replication Has Completed

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 4: Move test users to

Topic Last Modified: *2012-09-17*

When running the **Move-CsUser** cmdlet, you may experience a failure because user information between Active Directory Domain Services (AD DS) and the Lync Server 2013 databases are out of sync because the initial replication is incomplete. The time it takes for the successful completion of the Lync Server 2013 User Replicator service's initial synchronization depends on the number of domain controllers that are hosted in the Active Directory forest that hosts the Lync Server 2013 pool. The Lync Server 2013 User Replicator service initial synchronization process occurs when the Lync Server 2013 Front End Server is started for the first time. After that, the synchronization is then based on the User Replicator interval. Complete the following steps to verify user replication has completed before running the **Move-CsUser** cmdlet.

To verify user replication has completed

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Click the **Start** menu, and then click **Run**.
3. Enter **eventvwr.exe** and then click **OK**.
4. In Event Viewer, click **Applications and Services logs** to expand it, and then select Lync Server.
5. In the **Actions** pane click **Filter Current Log**.
6. From the **Event sources** list, click **LS User Replicator**.
7. In **<All Event IDs>** enter **30024** and then click **OK**.
8. In the filtered events list, on the **General** tab, look for an entry that states user replication has completed successfully.

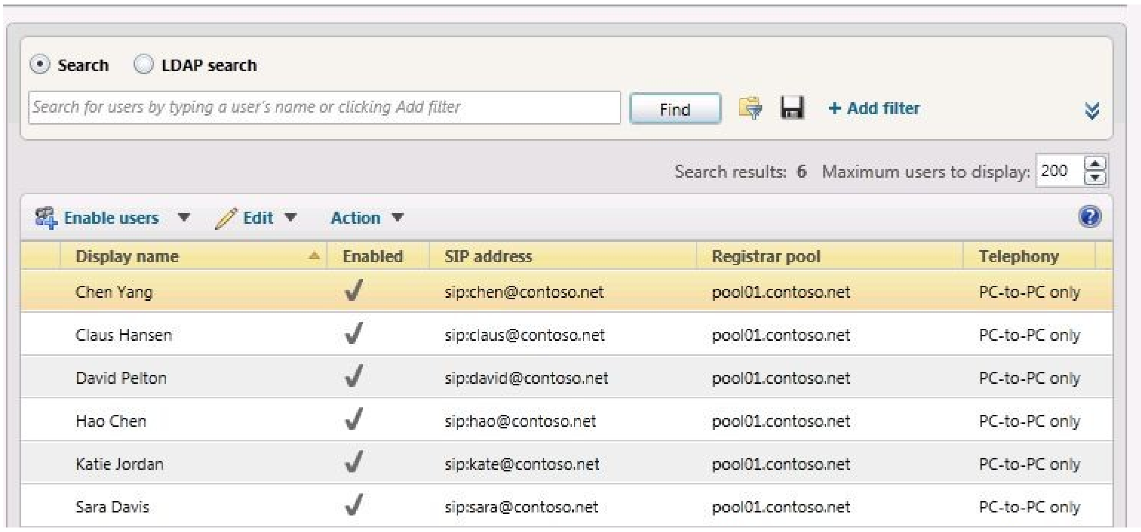
1.6.1.5.3 Move a single user to the Pilot Pool

Move a single user to the Pilot Pool

Topic Last Modified: *2012-09-26*

You can move a user from your Lync Server 2010 pool to your Lync Server 2013 pilot pool using Lync Server 2013 Control Panel or Lync Server 2013 Management Shell. In the example below, in the Registrar pool column, **pool01.contoso.net** is the Lync Server 2010 pool, and all six of these users are connected to this pool. Use the following procedures to move a user to your Lync Server 2013 pool using Lync Server 2013 Control Panel and Lync Server Management Shell.

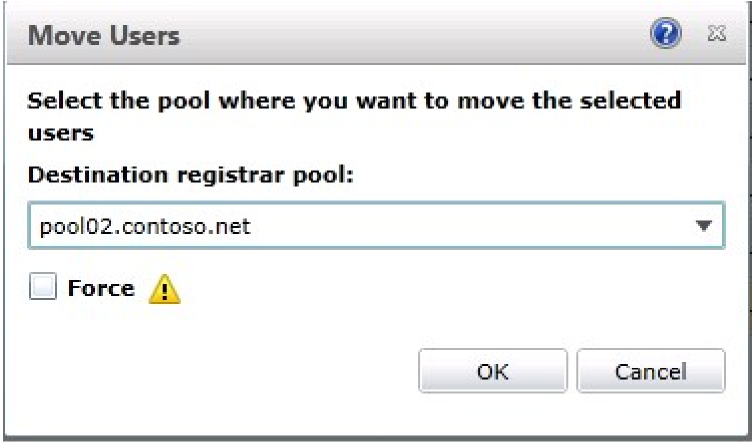
To move a user by using the Lync Server 2013 Control Panel


● Search
○ LDAP search
Search for users by typing a user's name or clicking Add filter
Find
+ Add filter
Enable users
Edit
Action

Search results: 6 Maximum users to display: 200

Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	pool01.contoso.net	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	pool01.contoso.net	PC-to-PC only
David Pelton	✓	sip:david@contoso.net	pool01.contoso.net	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	pool01.contoso.net	PC-to-PC only
Katie Jordan	✓	sip:kate@contoso.net	pool01.contoso.net	PC-to-PC only
Sara Davis	✓	sip:sara@contoso.net	pool01.contoso.net	PC-to-PC only

1. Log on to the Front End Server with an account that is a member of the RTCUniversalServerAdmins group or a member of the CsAdministrator or CsUserAdministrator administrative role.
2. Open **Lync Server Control Panel**.
3. Click **Users**, click Search, and then click **Find**.
4. Select a user that you want to move to the Lync Server 2013 pool. In this example, we will move user Sara Davis.
5. On the **Action** menu, select **Move selected users to pool**.
6. From the drop-down list, select the Lync Server 2013 pool.
7. Click **Action** and then click **Move selected users to pool**. Click **OK**.



Select the pool where you want to move the selected users

Destination registrar pool: pool02.contoso.net

□ Force

8. Verify that the **Registrar pool** column for the user now contains the Lync Server 2013 pool, which indicates that the user has been successfully moved.

To move a user by using the Lync Server 2013 Management Shell

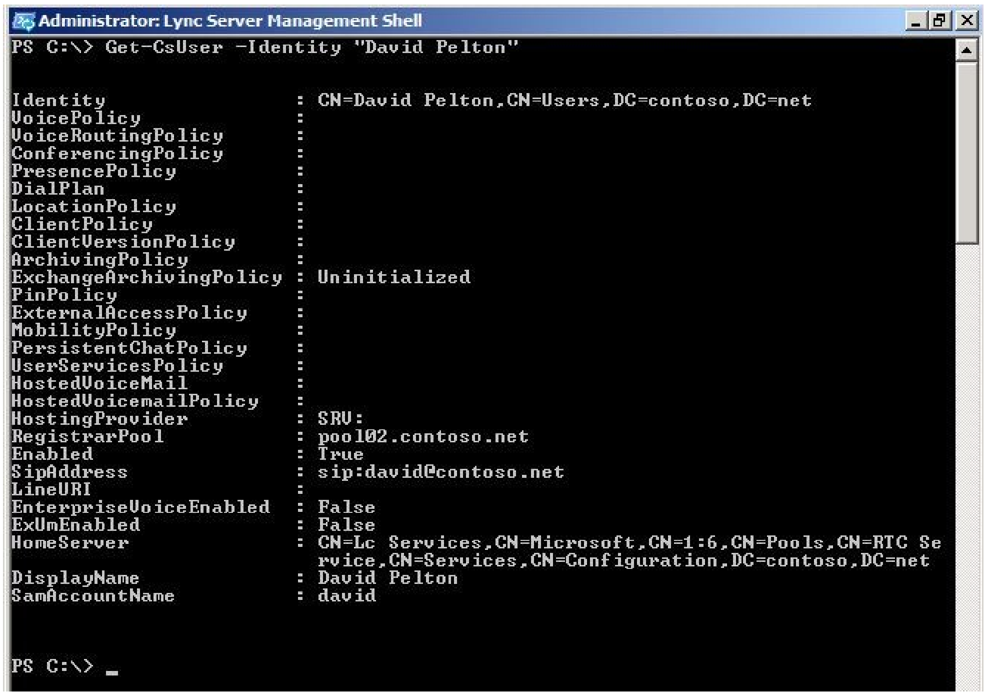
1. Open the Lync Server Management Shell.
2. At the command line, type the following:

```
Move-CsUser -Identity "David Pelton" -Target "pool02.contoso.net"
```

3. Next, at the command line, type the following:

```
Get-CsUser -Identity "David Pelton"
```

4. The **RegistrarPool** identity now points to the Lync Server 2013 pool. The presence of this identity confirms that the user has been successfully moved.



```
PS C:\> Get-CsUser -Identity "David Pelton"


Identity                  : CN=David Pelton,CN=Users,DC=contoso,DC=net
VoicePolicy               :
VoiceRoutingPolicy        :
ConferencingPolicy        :
PresencePolicy            :
DialPlan                  :
LocationPolicy            :
ClientPolicy              :
ClientVersionPolicy       :
ArchivingPolicy           :
ExchangeArchivingPolicy : Uninitialized
PinPolicy                 :
ExternalAccessPolicy      :
MobilityPolicy            :
PersistentChatPolicy      :
UserServicesPolicy        :
HostedVoiceMail           :
HostedVoicemailPolicy     :
HostingProvider           : SRV:
RegistrarPool             : pool02.contoso.net
Enabled                   : True
SipAddress                : sip:david@contoso.net
LineURI                   :
EnterpriseVoiceEnabled    : False
ExUmEnabled               : False
HomeServer                : CN=Lc Services,CN=Microsoft,CN=1:6,CN=Pools,CN=RTC Se
                            rvice,CN=Services,CN=Configuration,DC=contoso,DC=net
DisplayName               : David Pelton
SamAccountName            : david


PS C:\> _
```

Note:

For details about the **Get-CsUser** cmdlet, run: **Get-Help Get-CsUser –Detailed**

1.6.1.5.4 Move multiple users to the Pilot Pool

Move multiple users to the Pilot Pool

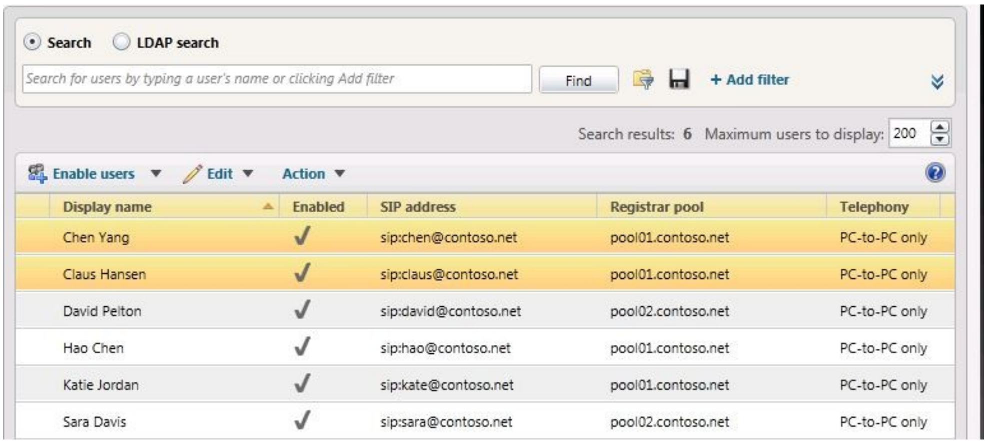
Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 4: Move test users to the Pilot Pool >

Topic Last Modified: *2012-10-02*

You can move multiple users from your Lync Server 2010 pool to your Lync Server 2013 pilot pool using Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

To move multiple users by using the Lync Server 2013 Control Panel

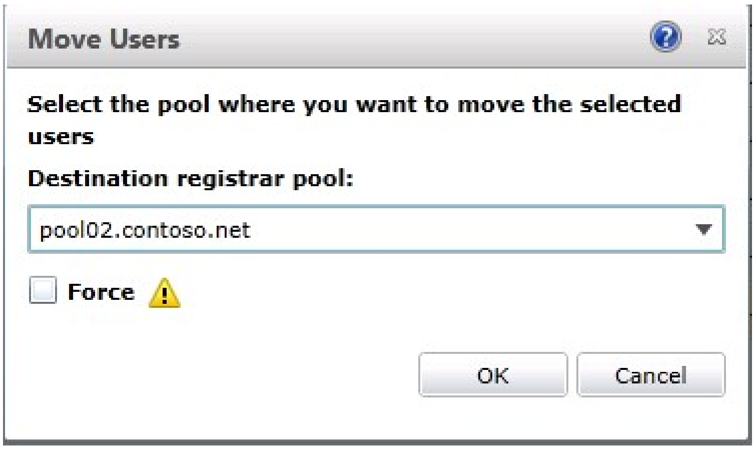
1. Open **Lync Server Control Panel**.
2. Click **Users**, click Search, and then click **Find**.
3. Select two users that you want to move to the Lync Server 2013 pool. In this example, we will move users Chen Yang and Claus Hansen.



Search results: 6 Maximum users to display: 200

Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	pool01.contoso.net	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	pool01.contoso.net	PC-to-PC only
David Pelton	✓	sip:david@contoso.net	pool02.contoso.net	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	pool01.contoso.net	PC-to-PC only
Katie Jordan	✓	sip:kate@contoso.net	pool01.contoso.net	PC-to-PC only
Sara Davis	✓	sip:sara@contoso.net	pool02.contoso.net	PC-to-PC only

4. From the **Action** menu, select **Move selected users to pool**.
5. From the drop-down list, select the Lync Server 2013 pool.
6. Click **Action** and then click **Move selected users to pool**. Click OK.



Move Users

Select the pool where you want to move the selected users

Destination registrar pool:

pool02.contoso.net

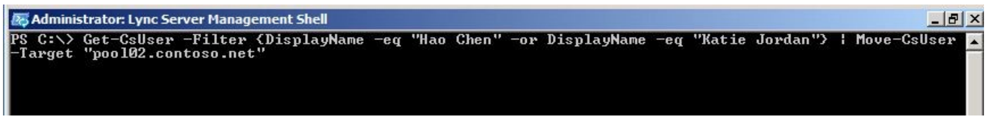
□ Force

7. Verify that the **Registrar pool** column for the users now contains the Lync Server 2013 pool, which indicates that the users have been successfully moved.

To move multiple users by using the Lync Server 2013 Management Shell

1. Open the Lync Server 2013 Management Shell.
2. At the command line, type the following and replace **User1** and **User2** with specific user names you want to move and replace **pool_FQDN** with the name of the destination pool. In this example we will move users Hao Chen and Katie Jordan.

```
Get-CsUser -Filter {DisplayName -eq "User1" -or DisplayName - eq "User
```



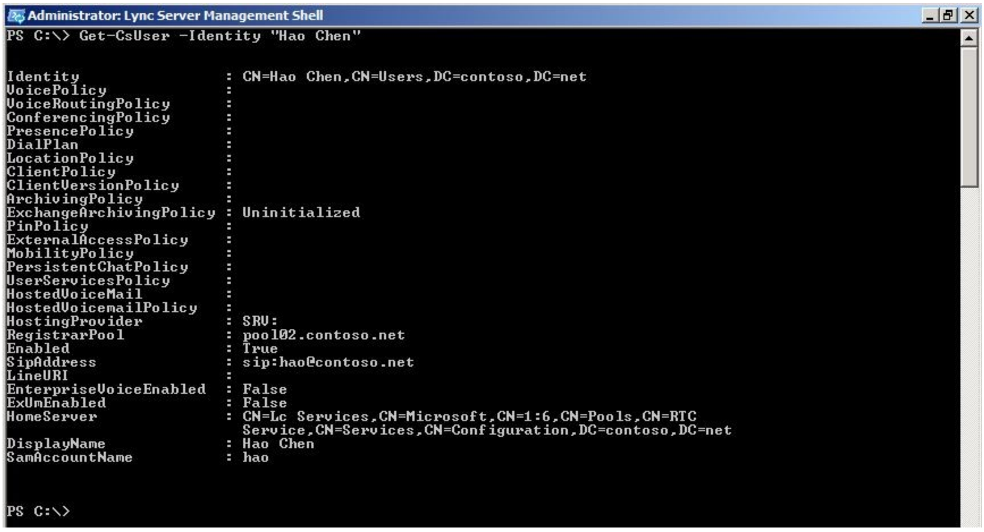
```
PS C:\> Get-CsUser -Filter {DisplayName -eq "Hao Chen" -or DisplayName -eq "Katie Jordan"} | Move-CsUser
-Target "pool02.contoso.net"
```

3. At the command line, type the following

```
Get-CsUser -Identity "User1"
```

4. The **Registrar Pool** identity should now point to the pool you specified as **pool_FQDN** in the previous step. The presence of this identity confirms that

the user has been successfully moved. Repeat step to verify **User2** has been moved.



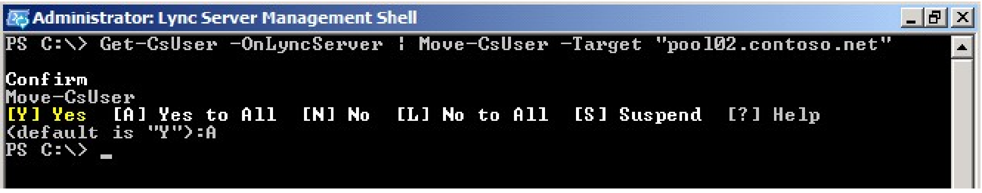
```
PS C:\> Get-CsUser -Identity "Hao Chen"


Identity                  : CN=Hao Chen,CN=Users,DC=contoso,DC=net
VoicePolicy               :
VoiceRoutingPolicy        :
ConferencingPolicy        :
PresencePolicy            :
DialPlan                  :
LocationPolicy            :
ClientPolicy              :
ClientVersionPolicy       :
ArchivingPolicy           :
ExchangeArchivingPolicy   : Uninitialized
PinPolicy                 :
ExternalAccessPolicy      :
MobilityPolicy            :
PersistentChatPolicy      :
UserServicesPolicy        :
HostedVoiceMail           :
HostedVoicemailPolicy     :
HostingProvider           : SRV:
RegistrarPool             : pool02.contoso.net
Enabled                   : True
SipAddress                : sip:hao@contoso.net
LineURI                   :
EnterpriseVoiceEnabled    : False
ExUmEnabled               : False
HomeServer                : CN=Lc Services,CN=Microsoft,CN=1:6,CN=Pools,CN=RTC
                            Service,CN=Services,CN=Configuration,DC=contoso,DC=net
DisplayName               : Hao Chen
SamAccountName            : hao


PS C:\>
```

To move all users at the same time by using the Lync Server 2013 Management Shell

In this example, all users have been returned to the Lync Server 2010 pool (pool01.contoso.net). Using the Lync Server 2013 Management Shell, we will move all users at the same time to the Lync Server 2013 pool (pool02.contoso.net).

1. Open the **Lync Server 2013 Management Shell**.
2. At the command line, type the following:

```
Get-CsUser -OnLyncServer | Move-CsUser -Target "pool_FQDN"
```

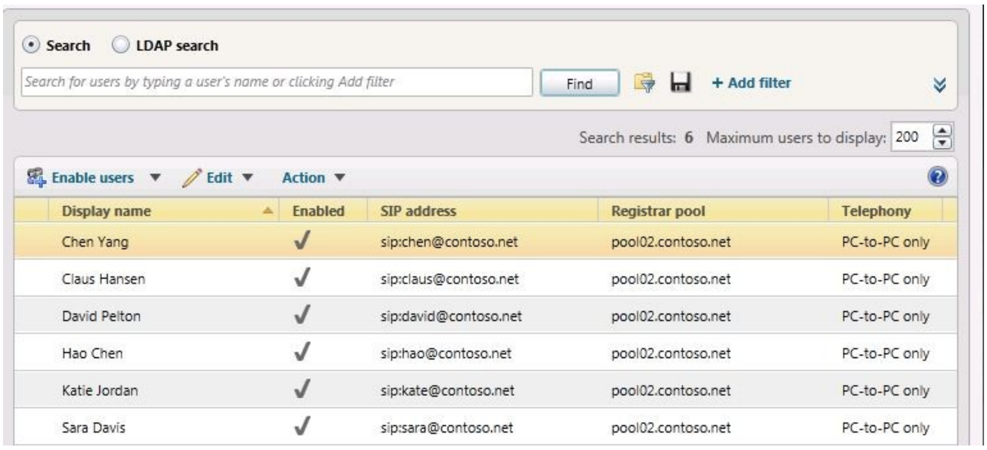


```
PS C:\> Get-CsUser -OnLyncServer | Move-CsUser -Target "pool02.contoso.net"

Confirm
Move-CsUser
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):A
PS C:\> _
```

3. Next, run **Get-CsUser** for one of the pilot users.

```
Get-CsUser -Identity "Hao Chen"
```

4. The **Registrar Pool** identity for each user now points to the pool you specified as “pool_FQDN” in the previous step. The presence of this identity confirms that the user has been successfully moved.
5. Additionally, we can view the list of users in the Lync Server 2013 Control Panel and verify that the Registrar Pool value now points to the Lync Server 2013 pool.


● Search
○ LDAP search
Search for users by typing a user's name or clicking Add filter
Find
+ Add filter
Search results: 6
Maximum users to display: 200
Enable users
Edit
Action

Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	pool02.contoso.net	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	pool02.contoso.net	PC-to-PC only
David Pelton	✓	sip:david@contoso.net	pool02.contoso.net	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	pool02.contoso.net	PC-to-PC only
Katie Jordan	✓	sip:kate@contoso.net	pool02.contoso.net	PC-to-PC only
Sara Davis	✓	sip:sara@contoso.net	pool02.contoso.net	PC-to-PC only

1.6.1.6 Phase 5: Add Lync Server 2013 Edge Server to Pilot Pool

Phase 5: Add Lync Server 2013 Edge Server to Pilot Pool

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010 to Lync Server 2013 >

Topic Last Modified: *2012-09-06*

The topics in this section explain how to add a Lync Server 2013 Edge Server to the pilot pool deployment. The topics provide configuration and verification guidance when running the Deploy New Edge pool wizard.

In This Section

- Deploy Pilot Edge Server
- Verify Configuration Settings

1.6.1.6.1 Deploy Pilot Edge Server

Deploy Pilot Edge Server

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 5: Add Lync Server 2013 Edge Server to Pilot Pool >

Topic Last Modified: *2012-10-19*

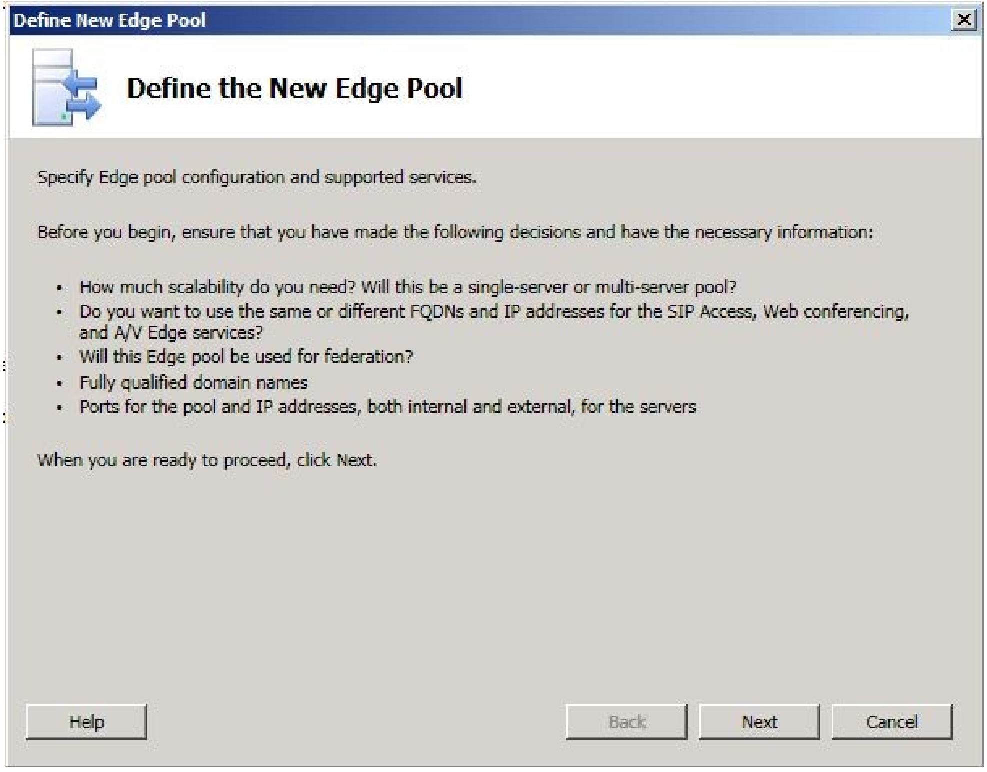
This topic highlights configuration settings you should be aware of prior to deploying your Lync Server 2013 Edge Server. The deployment and configuration processes for Lync Server 2013 are very similar to Lync Server 2010. This section only highlights key points you should consider as part of your pilot pool deployment. For detailed steps, see Deploying External User Access in the Deployment documentation, which describes the deployment process and also gives configuration information for external user access.

As you navigate through the **Define New Edge Pool** wizard, review the key configuration settings shown in the following steps. Note that only a few pages of the **Define New Edge Pool** wizard are shown.

Define an Edge Pool

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.

2. Navigate to the Lync Server 2013 node. Right-click **Edge pools**, and click **New Edge pool**.



Define New Edge Pool

Define the New Edge Pool

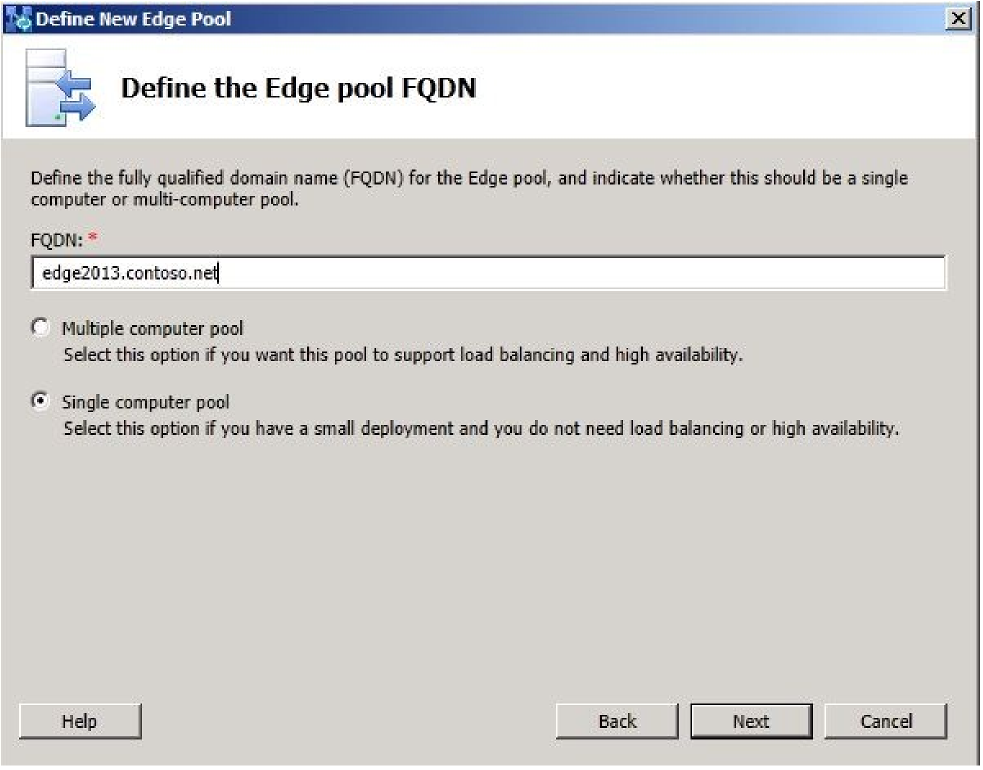
Specify Edge pool configuration and supported services.

Before you begin, ensure that you have made the following decisions and have the necessary information:

- How much scalability do you need? Will this be a single-server or multi-server pool?
- Do you want to use the same or different FQDNs and IP addresses for the SIP Access, Web conferencing, and A/V Edge services?
- Will this Edge pool be used for federation?
- Fully qualified domain names
- Ports for the pool and IP addresses, both internal and external, for the servers

When you are ready to proceed, click Next.

3. An Edge pool can be a **Multiple computer pool** or **Single computer pool**.



Define New Edge Pool

Define the Edge pool FQDN

Define the fully qualified domain name (FQDN) for the Edge pool, and indicate whether this should be a single computer or multi-computer pool.

FQDN: *

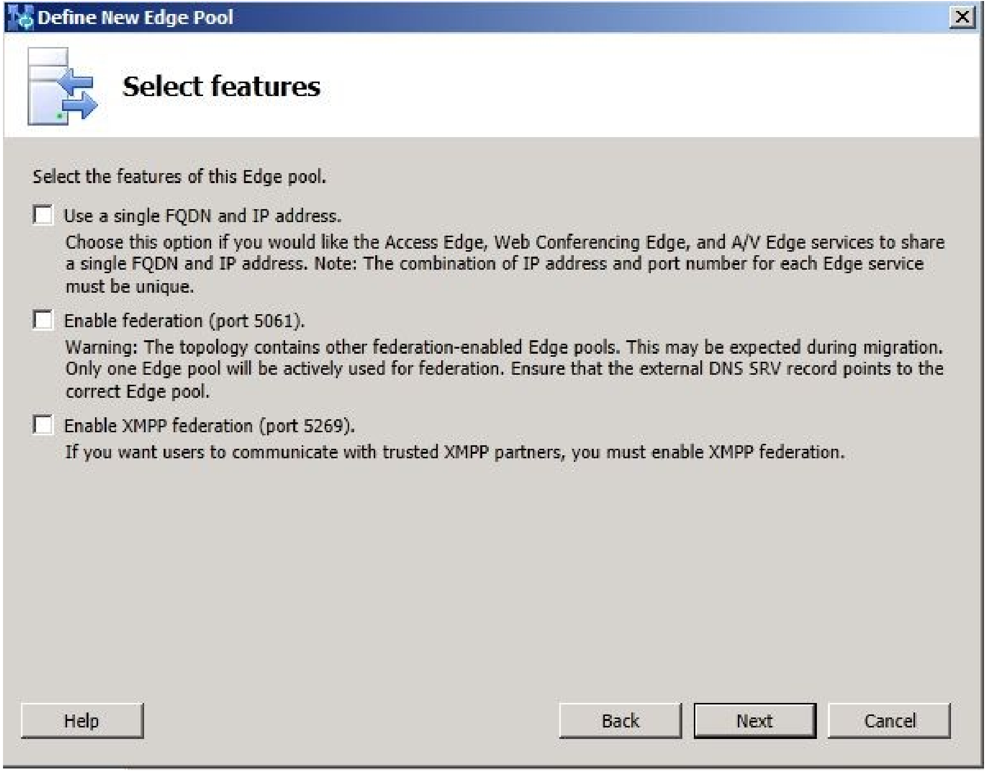
edge2013.contoso.net

○ Multiple computer pool
Select this option if you want this pool to support load balancing and high availability.

● Single computer pool
Select this option if you have a small deployment and you do not need load balancing or high availability.

4. On the **Select features** page, do not enable federation or XMPP federation. Federation and XMPP federation are both currently routed through the legacy Lync Server 2010 Edge Server. These features will be configured in a later

phase of migration.


Define New Edge Pool

Select features

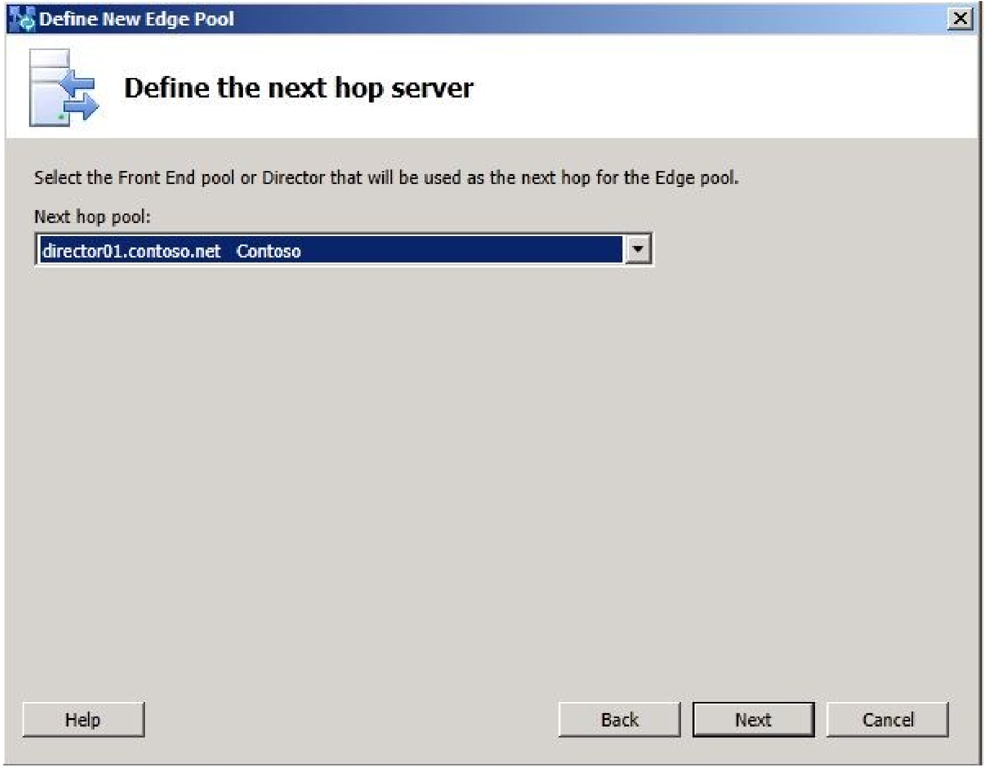
Select the features of this Edge pool.

☐ Use a single FQDN and IP address.
Choose this option if you would like the Access Edge, Web Conferencing Edge, and A/V Edge services to share a single FQDN and IP address. Note: The combination of IP address and port number for each Edge service must be unique.

☐ Enable federation (port 5061).
Warning: The topology contains other federation-enabled Edge pools. This may be expected during migration. Only one Edge pool will be actively used for federation. Ensure that the external DNS SRV record points to the correct Edge pool.

☐ Enable XMPP federation (port 5269).
If you want users to communicate with trusted XMPP partners, you must enable XMPP federation.

5. Next, continue completing the following wizard pages: **External FQDNs**, **Define the internal IP address**, and **Define the external IP address**.
6. On the **Define the next hop** page, select the Director for the next hop of the Lync Server 2010 Edge pool.


Define New Edge Pool

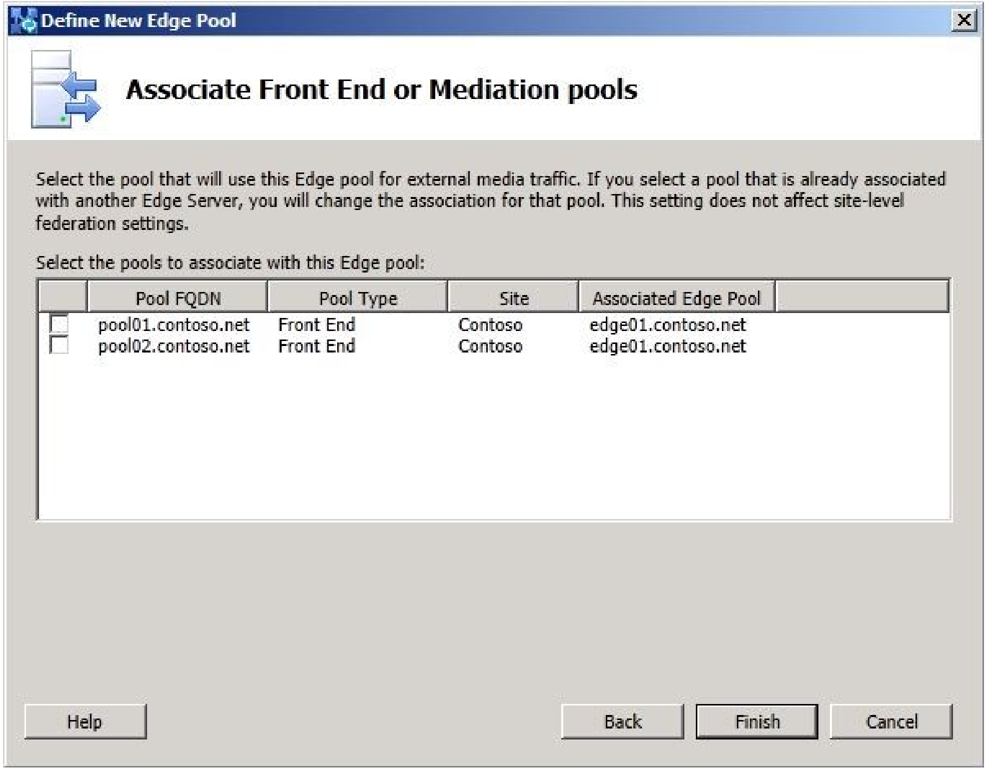
Define the next hop server

Select the Front End pool or Director that will be used as the next hop for the Edge pool.

Next hop pool: director01.contoso.net Contoso

7. On the **Associate Front End or Mediation pools** page, do not associate a

pool with this Edge pool at this time. External media traffic is currently routed through the legacy Lync Server 2010 Edge Server. This setting will be configured in a later phase of migration.



Associate Front End or Mediation pools

Select the pool that will use this Edge pool for external media traffic. If you select a pool that is already associated with another Edge Server, you will change the association for that pool. This setting does not affect site-level federation settings.

Select the pools to associate with this Edge pool:

	Pool FQDN	Pool Type	Site	Associated Edge Pool
□	pool01.contoso.net	Front End	Contoso	edge01.contoso.net
□	pool02.contoso.net	Front End	Contoso	edge01.contoso.net

8. Click **Finish** and then **Publish** the topology.
9. Follow the steps in Install Edge Servers in the Deployment documentation to install the files on the new Edge Server, configure certificates, and start the services.

It’s very important that you follow the guidelines in the topics Deploying External User Access in the Deployment documentation. This section merely provided some guidance on configuration settings when installing these server roles.

You should now have a legacy Lync Server 2010 Edge Server deployed in parallel with a Lync Server 2013 Edge server deployment. Verify that both deployments are running properly, services are started, and you can administer each deployment prior to moving to the next phase.

1.6.1.6.2 Verify Configuration Settings

Verify Configuration Settings

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 5: Add Lync Server 2013 Edge Server to Pilot Pool >

Topic Last Modified: *2012-09-06*

You can validate the replication of configuration information to the Edge server by running the Lync Server 2013 **Get-CsManagementStoreReplicationStatus** cmdlet on the internal computer on which the Central Management store is located, or on any domain joined computer on which Lync Server 2013 Core Components (OcsCore.msi) is installed.

Initial results may indicate the status as "False" instead of "True" for replication. If so, run the **Invoke-CsManagementStoreReplication** cmdlet and allow time for the replication to complete before running the **Get-CsManagementStoreReplicationStatus** again.

1.6.1.7 Phase 6: Move from Pilot Deployment into Production

Phase 6: Move from Pilot Deployment into Production

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010 to Lync Server 2013 >

Topic Last Modified: *2012-10-19*

The topics in this section describe tasks you must complete prior to moving your deployment of Lync Server 2013 from a pilot deployment to a production-level deployment.

- Configure Federation Routes and Media Traffic
- Verify Federation and Remote Access for External Users
- Change Simple URLs after Migration
- Move Remaining Users to Lync Server 2013
- Configure XMPP Gateway on Lync Server 2013

1.6.1.7.1 Configure Federation Routes and Media Traffic

Configure Federation Routes and Media Traffic

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 6: Move from Pilot Deployment into Production >

Topic Last Modified: *2012-10-15*

Federation is a trust relationship between two or more SIP domains that permits users in separate organizations to communicate across network boundaries. After you migrate to your Lync Server 2013 pilot pool, you need to transition from the federation route of your Lync Server 2010 Edge Servers to the federation route of your Lync Server 2013 Edge Servers.

Use the following procedures to transition the federation route and the media traffic route from your Lync Server 2010 Edge Server and Director to your Lync Server 2013 Edge Server, for a single-site deployment.

◆Important:

Changing the federation route and media traffic route requires that you schedule maintenance downtime for the Lync Server 2013 and Lync Server 2010 Edge Servers. This entire transition process also means that federated access will be unavailable for the duration of the outage. You should schedule the downtime for a time when you expect minimal user activity. You should also provide sufficient notification to your end users. Plan accordingly for this outage and set appropriate expectations within your organization.

◆Important:

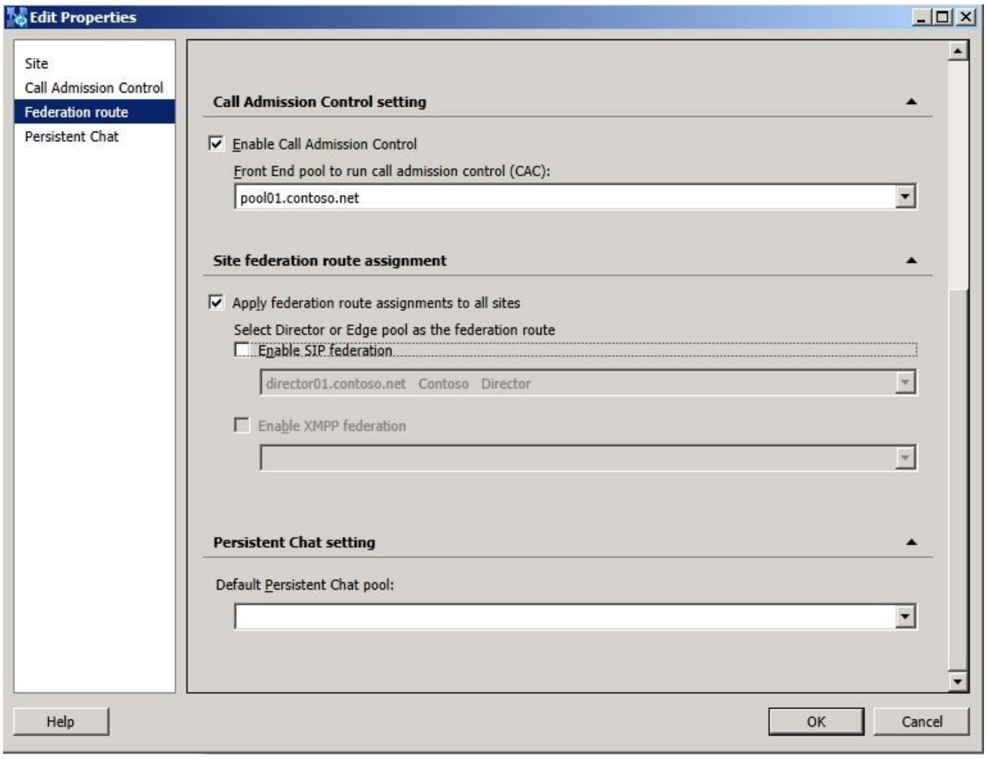
If your legacy Lync Server 2010 Edge Server is configured to use the same FQDN for the Access Edge service, Web Conferencing Edge service, and the A/V Edge service, the procedures in this section are not supported. If the legacy Edge services are configured to use the same FQDN, you must first migrate all your users from Lync Server 2010 to Lync Server 2013, then decommission the Lync Server 2010 Edge Server before enabling federation on the Lync Server 2013 Edge Server.

Important:

If your XMPP federation is routed through a Lync Server 2013 Edge Server, legacy Lync Server 2010 users will not be able to communicate with the XMPP federated partner until all users have been moved to Lync Server 2013, XMPP policies and certificates have been configured, the XMPP federated partner has been configured on Lync Server 2013, and lastly the DNS entries have been updated.

To remove the legacy federation association from Lync Server 2013 sites

1. On the Lync Server 2013 Front End server, open the existing topology in Topology Builder.
2. In the left pane, navigate to the site node, which is located directly below **Lync Server**.
3. Right-click the site and then click **Edit Properties**.
4. In the left pane, select **Federation route**.
5. Under **Site federation route assignment**, clear the **Enable SIP federation** check box to disable the federation route through the legacy Lync Server 2010 environment.



Call Admission Control setting

☑ Enable Call Admission Control

Front End pool to run call admission control (CAC): pool01.contoso.net

Site federation route assignment

☑ Apply federation route assignments to all sites

Select Director or Edge pool as the federation route

☐ Enable SIP federation

director01.contoso.net Contoso Director

☐ Enable XMPP federation

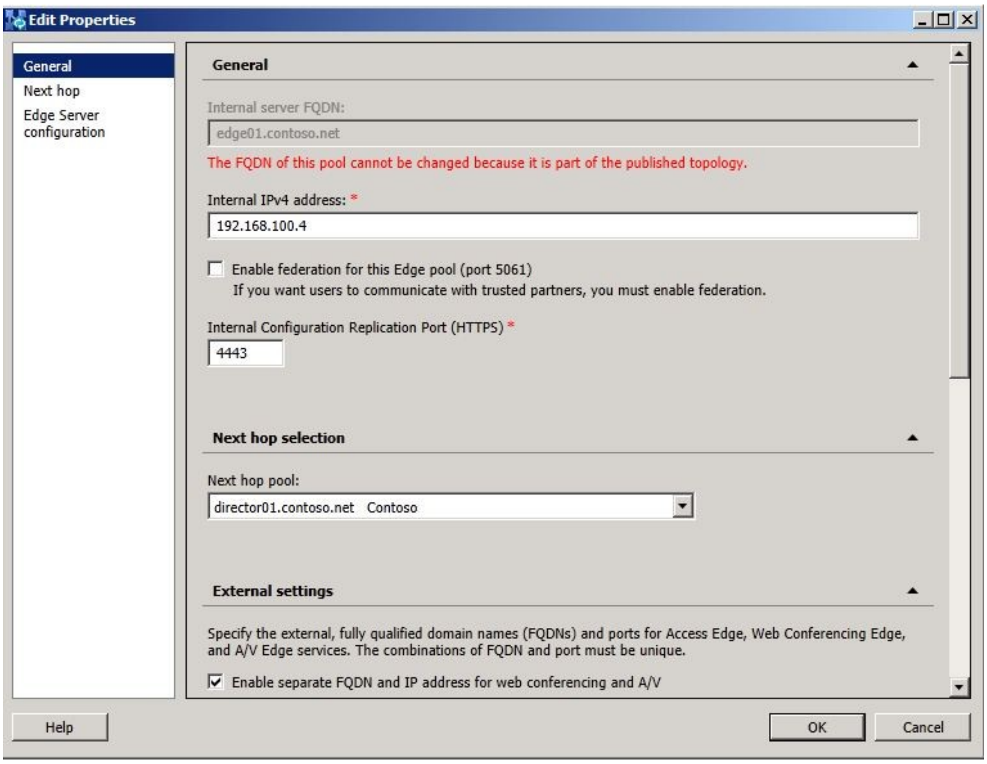
Persistent Chat setting

Default Persistent Chat pool:

6. Click **OK** to close the Edit Properties page.
7. From **Topology Builder**, select the top node **Lync Server**.
8. From the **Action** menu, click **Publish Topology**.
9. Click **Next** to complete the publishing process and then click **Finish** when the publishing process has completed.

To configure the legacy Edge Server as a non-federating Edge Server

1. In the left pane, navigate to the **Lync Server 2010** node and then to the **Edge pools** node.
2. Right-click the Edge server, and then click **Edit Properties**.
3. Select **General** in the left pane.
4. Clear the **Enable federation for this Edge pool (port 5061)** check box entry and select **OK** to close the page.



General

Internal server FQDN:
edge01.contoso.net
The FQDN of this pool cannot be changed because it is part of the published topology.

Internal IPv4 address: *
192.168.100.4

☐ Enable federation for this Edge pool (port 5061)
If you want users to communicate with trusted partners, you must enable federation.

Internal Configuration Replication Port (HTTPS) *
4443

Next hop selection

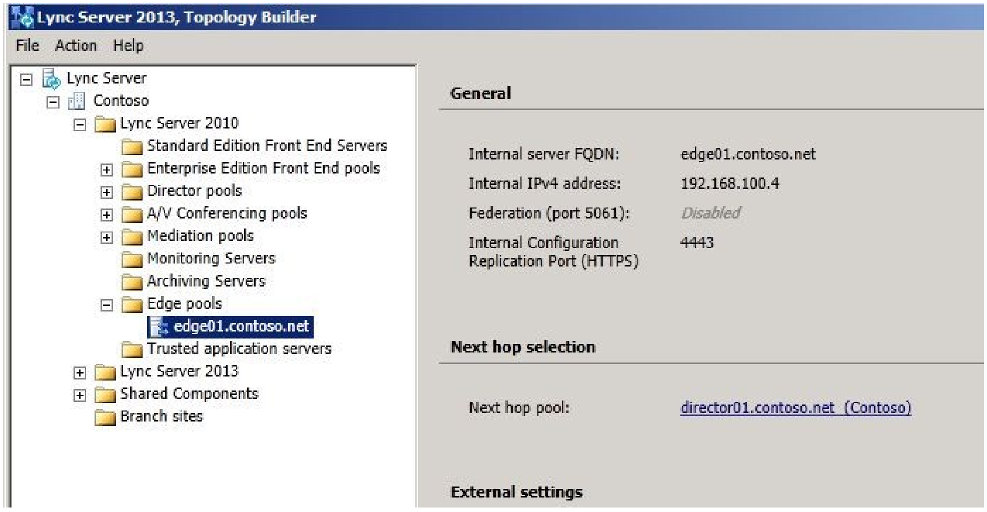
Next hop pool:
director01.contoso.net Contoso

External settings

Specify the external, fully qualified domain names (FQDNs) and ports for Access Edge, Web Conferencing Edge, and A/V Edge services. The combinations of FQDN and port must be unique.

☑ Enable separate FQDN and IP address for web conferencing and A/V

5. From the **Action** menu, select **Publish Topology**, and then click **Next**.
6. When the **Publishing wizard** completes, click **Finish** to close the wizard.
7. Verify federation for the legacy Edge server is disabled.



General

Internal server FQDN: edge01.contoso.net
Internal IPv4 address: 192.168.100.4
Federation (port 5061): *Disabled*
Internal Configuration Replication Port (HTTPS) 4443

Next hop selection

Next hop pool: director01.contoso.net (Contoso)

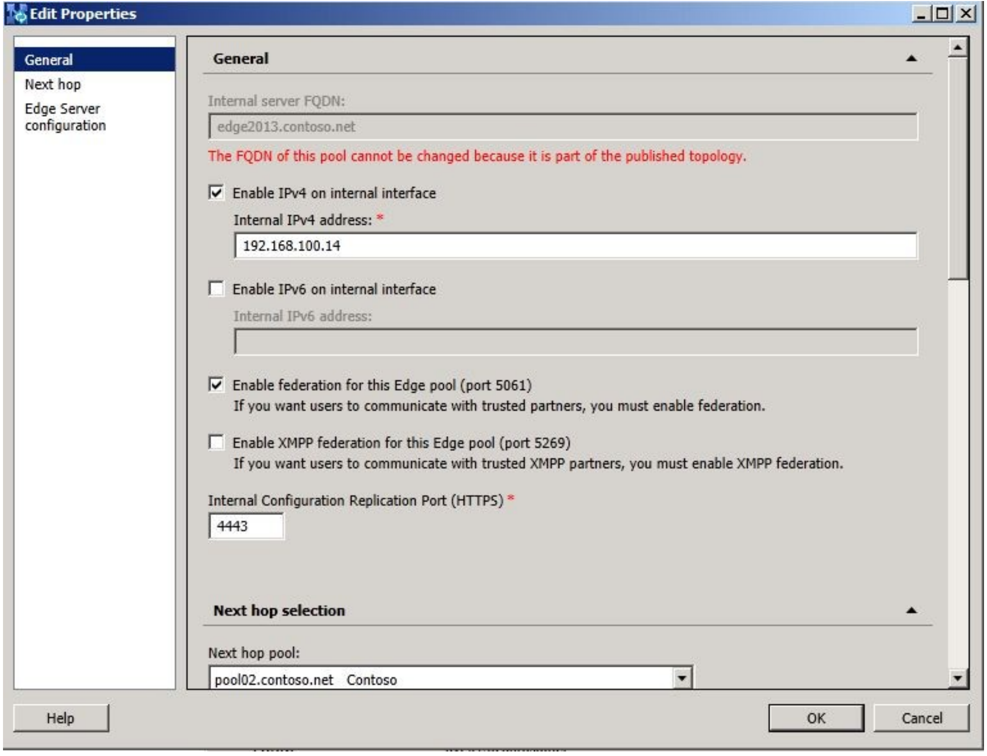
External settings

To configure certificates on the Lync Server 2010 Edge Server

1. Export the external Access Proxy certificate, with the private key, from the legacy Lync Server 2010 Edge Server.
2. On the Lync Server 2013 Edge Server, import the Access Proxy external certificate from the previous step.
3. Assign the Access Proxy external certificate to the Lync Server 2013 external interface of the Edge Server.
4. The internal interface certificate of the Lync Server 2013 Edge Server should be requested from a trusted CA and assigned.

⊟To change Lync Server 2010 federation route to use Lync Server 2013 Edge Server

1. From Topology Builder, in the left pane, navigate to the **Lync Server 2013** node and then to the **Edge pools** node.
2. Right-click the Edge server, and then click **Edit Properties**.
3. Select **General** in the left pane.
4. Select the check box entry for **Enable federation for this Edge pool (port 5061)** and then click **OK** to close the page.



General

Internal server FQDN: edge2013.contoso.net

The FQDN of this pool cannot be changed because it is part of the published topology.

☑ Enable IPv4 on internal interface

Internal IPv4 address: * 192.168.100.14

☐ Enable IPv6 on internal interface

Internal IPv6 address:

☑ Enable federation for this Edge pool (port 5061)
If you want users to communicate with trusted partners, you must enable federation.

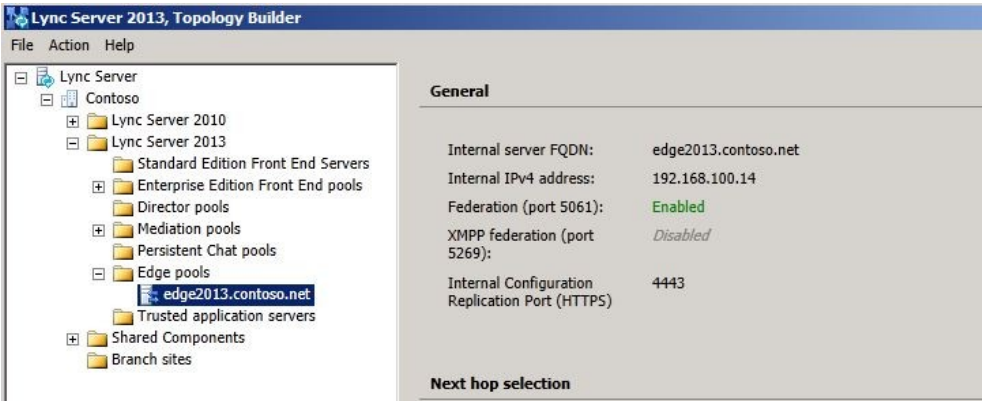
☐ Enable XMPP federation for this Edge pool (port 5269)
If you want users to communicate with trusted XMPP partners, you must enable XMPP federation.

Internal Configuration Replication Port (HTTPS) * 4443

Next hop selection

Next hop pool: pool02.contoso.net Contoso

5. From the **Action** menu, select **Publish Topology**, and then click **Next**.
6. When the **Publishing wizard** completes, click **Finish** to close the wizard.
7. Verify **Federation (port 5061)** is set to **Enabled**.



General

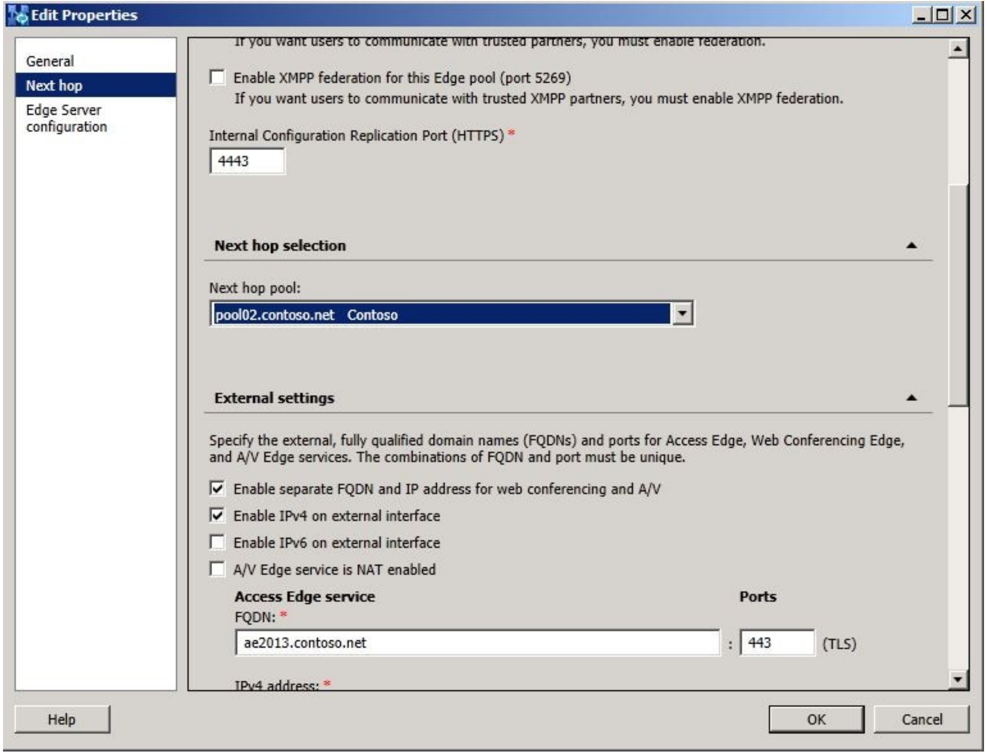
Internal server FQDN:	edge2013.contoso.net
Internal IPv4 address:	192.168.100.14
Federation (port 5061):	Enabled
XMPP federation (port 5269):	Disabled
Internal Configuration Replication Port (HTTPS)	4443

Next hop selection

⊟To update Lync Server 2013 Edge Server federation next hop

1. From Topology Builder, in the left pane, navigate to the **Lync Server 2013** node and then to the **Edge pools** node.
2. Expand the node, right-click the Edge Server listed, and then click **Edit Properties**.

3. On the **General** page, under **Next hop selection**, select from the drop-down list the Lync Server 2013 pool.



If you want users to communicate with trusted partners, you must enable federation.

☐ Enable XMPP federation for this Edge pool (port 5269)
If you want users to communicate with trusted XMPP partners, you must enable XMPP federation.

Internal Configuration Replication Port (HTTPS) *
4443

Next hop selection

Next hop pool:
pool02.contoso.net Contoso

External settings

Specify the external, fully qualified domain names (FQDNs) and ports for Access Edge, Web Conferencing Edge, and A/V Edge services. The combinations of FQDN and port must be unique.

☑ Enable separate FQDN and IP address for web conferencing and A/V
☑ Enable IPv4 on external interface
☐ Enable IPv6 on external interface
☐ A/V Edge service is NAT enabled

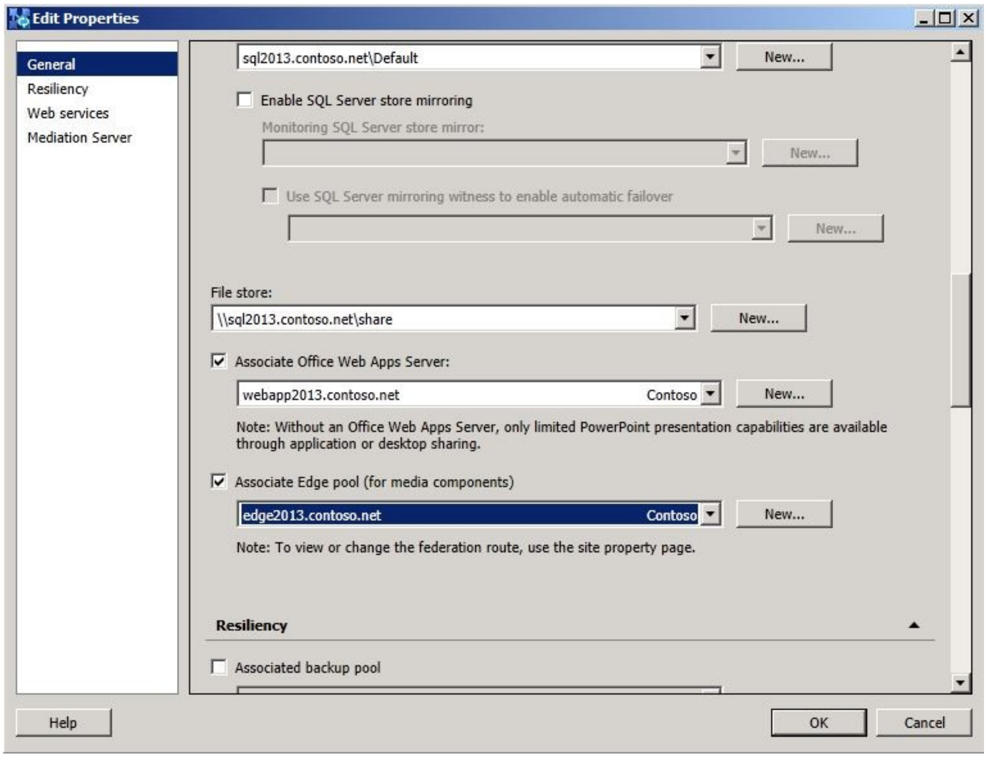
Access Edge service **Ports**
FQDN: *
ae2013.contoso.net : 443 (TLS)

IPv4 address: *

4. Click **OK** to close the Edit Properties page.
5. From **Topology Builder**, select the top node **Lync Server** .
6. From the **Action** menu, click **Publish Topology** and complete the wizard.

⊟To configure Lync Server 2013 Edge Server outbound media path

1. From Topology Builder, in the left pane, navigate to the **Lync Server 2013** node and then to the pool below **Standard Edition Front End Servers** or **Enterprise Edition Front End pools**.
2. Right-click the pool, and then click **Edit Properties**.
3. In the **Associations** section, select the **Associate Edge pool (for media components)** check box.



sql2013.contoso.net\Default

□ Enable SQL Server store mirroring

Monitoring SQL Server store mirror:

□ Use SQL Server mirroring witness to enable automatic failover

File store:
\\sql2013.contoso.net\share

☑ Associate Office Web Apps Server:
webapp2013.contoso.net Contoso

Note: Without an Office Web Apps Server, only limited PowerPoint presentation capabilities are available through application or desktop sharing.

☑ Associate Edge pool (for media components)
edge2013.contoso.net Contoso

Note: To view or change the federation route, use the site property page.

Resiliency

□ Associated backup pool

4. From the drop down box, select the Lync Server 2013 Edge Server.
5. Click **OK** to close the **Edit Properties** page.

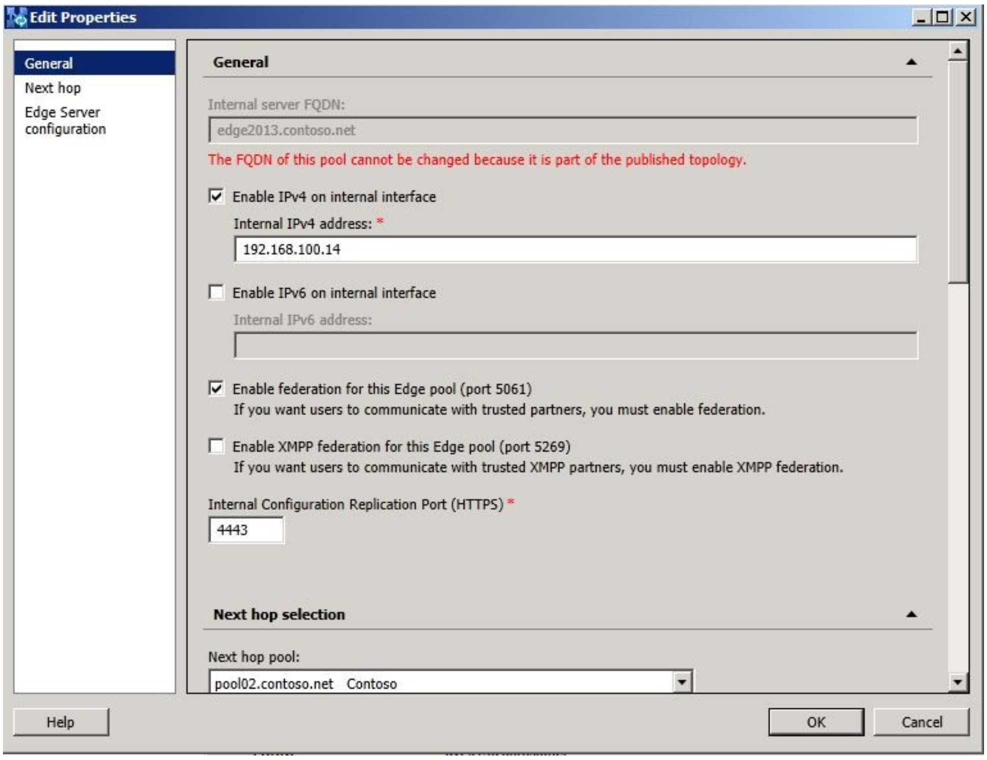
⊟To turn on Lync Server 2013 Edge Server federation

1. From Topology Builder, in the left pane, navigate to the **Lync Server 2013** node and then to the **Edge pools** node.
2. Expand the node, right-click the Edge Server listed, and then click **Edit Properties**.

Note:

Federation can only be enabled for a single Edge pool. If you have multiple Edge pools, select one to use as the federating Edge pool.

3. On the **General** page, verify the **Enable federation for this Edge pool (Port 5061)** setting is checked.



General

Internal server FQDN:

edge2013.contoso.net

The FQDN of this pool cannot be changed because it is part of the published topology.

☑ Enable IPv4 on internal interface

Internal IPv4 address: *

192.168.100.14

☐ Enable IPv6 on internal interface

Internal IPv6 address:

☑ Enable federation for this Edge pool (port 5061)

If you want users to communicate with trusted partners, you must enable federation.

☐ Enable XMPP federation for this Edge pool (port 5269)

If you want users to communicate with trusted XMPP partners, you must enable XMPP federation.

Internal Configuration Replication Port (HTTPS) *

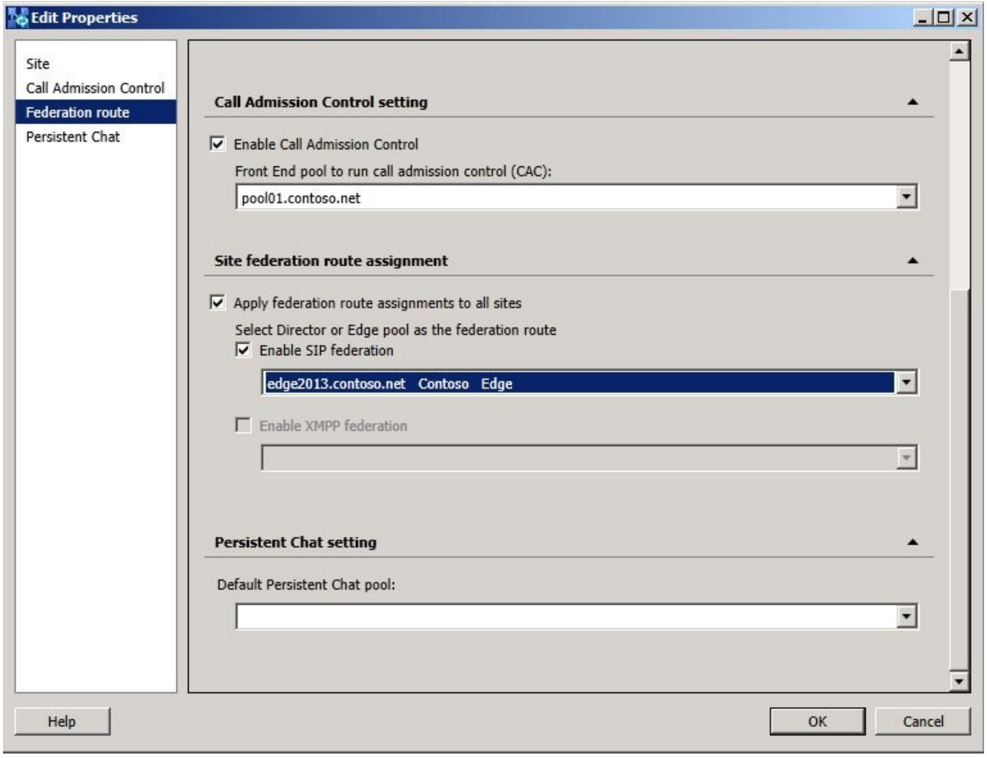
4443

Next hop selection

Next hop pool:

pool02.contoso.net Contoso

4. Click **OK** to close the Edit Properties page.
5. Next, navigate to the site node.
6. Right-click the site, and then click **Edit Properties**.
7. In the left pane, click **Federation route**.
8. Under **Site federation route assignment**, select **Enable SIP federation**, and then from the list select the Lync Server 2013 Edge Server listed.



Call Admission Control setting

☑ Enable Call Admission Control

Front End pool to run call admission control (CAC):

pool01.contoso.net

Site federation route assignment

☑ Apply federation route assignments to all sites

Select Director or Edge pool as the federation route

☑ Enable SIP federation

edge2013.contoso.net Contoso Edge

☐ Enable XMPP federation

Persistent Chat setting

Default Persistent Chat pool:

9. Click **OK** to close the **Edit Properties** page.

For multi-site deployments, complete this procedure at each site.

⊟To publish Edge Server configuration changes

1. From **Topology Builder**, select the top node **Lync Server** .
2. From the **Action** menu, select **Publish Topology** and complete the wizard.
3. Wait for Active Directory replication to occur to all pools in the deployment.

> **Note:**
>
> You may see the following message:
> **Warning: The topology contains more than one Federated Edge Server. This can occur during migration to a more recent version of the product. In that case, only one Edge Server would be actively used for federation. Verify that the external DNS SRV record points to the correct Edge Server. If you want to deploy multiple federation Edge Server to be active concurrently (that is, not a migration scenario), verify that all federated partners are using Lync Server. Verify that the external DNS SRV record lists all federation enabled Edge Servers.**
> This warning is expected and can be safely ignored.

⊟To configure Lync Server 2013 Edge Server

1. Bring all of the Lync Server 2013 Edge Servers online.
2. Update the external firewall routing rules or the hardware load balancer settings to send SIP traffic for external access (usually port 443) and federation (usually port 5061) to the Lync Server 2013 Edge Server, instead of the legacy Edge Server.

> **Note:**
>
> If you do not have a hardware load balancer, you need to update the DNS A record for federation to resolve to the new Lync Server Access Edge server. To accomplish this with minimum disruption, reduce the TLL value for the external Lync Server Access Edge FQDN so that when DNS is updated to point to the new Lync Server Access Edge, federation and remote access will be updated quickly.

3. Next, stop the **Lync Server Access Edge** from each Edge Server computer.
4. From each legacy Edge Server computer, open the **Services** applet from the **Administrative Tools**.
5. In the services list, find **Lync Server Access Edge**.
6. Right-click the services name, and then select **Stop** to stop the service.
7. Set the Startup type to **Disabled**.
8. Click **OK** to close the **Properties** window.

1.6.1.7.2 Verify Federation and Remote Access for External Users

Verify Federation and Remote Access for External Users

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 6: Move from Pilot Deployment into Production >

Topic Last Modified: *2012-09-18*

After transitioning the federation route to the Lync Server 2013 Edge Server, you should perform some functional tests to verify that federation performs as expected. Tests for external user access should include each type of external user that your organization supports, including any or all of the following.

⊟Test Connectivity of External Users and External access

- Users from at least one federated domain, an internal user on Lync Server

2013, and a user on Lync Server 2010. Test instant messaging (IM), presence, audio/video (A/V), and desktop sharing.
- Users of each public IM service provider that your organization supports (and for which provisioning has been completed) communicating with a user on Lync Server 2013 and a user on Lync Server 2010.
- Verify that anonymous users are able to join conferences.
- A user hosted on Lync Server 2010 using remote user access (logging into Lync Server 2010 from outside the intranet but without VPN) with a user on Lync Server 2013, and a user on Lync Server 2010. Test IM, presence, A/V, and desktop sharing.
- A user hosted on Lync Server 2013 using remote user access (logging into Lync Server 2013 from outside the intranet but without VPN) with a user on Lync Server 2013, and a user on Lync Server 2010. Test IM, presence, A/V, and desktop sharing.

1.6.1.7.3 Change Simple URLs after Migration

Change Simple URLs after Migration

See Also

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 6: Move from Pilot Deployment into Production >

Topic Last Modified: *2012-09-22*

Lync Server supports three simple URLs:
- **Meet** is used as the base URL for all conferences in the site or organization. With the Meet simple URL, links to join meetings are easy to comprehend, and easy to communicate and distribute.
- **Dial-in** enables access to the Dial-in Conferencing Settings webpage. The Dial-in simple URL is included in all meeting invitations so that users who want to dial in to the meeting can access the necessary phone number and PIN information.
- **Admin** enables quick access to the Lync Server Control Panel. The Admin simple URL is internal to your organization.

After migrating to Lync Server 2013, you must be aware of how the change impacts your DNS records and certificates for simple URLs. If the legacy Lync Server 2010 Director remains in use in the topology, no changes to your simple URLs are required. If the Lync Server 2010 Director is removed from the topology after migration, the simple URL DNS records must be updated to point to one of the Lync Server 2013 pools. Whenever you change a simple URL name, however, you must run Enable-CsComputer on each Director and Front End Server to register the change.

Changing Simple URLs after Migration

To update the Meet simple URL

1. In Topology Builder, right-click the top node **Lync Server**, and then click **Edit Properties**.
2. Select **Simple URLs** in the left pane, then below **Meeting URLs:** select the Meet URL and then click **Edit URL**.
3. Update the URL to the value you want, and then click **OK** to save the edited URL.

To update the Admin simple URL

1. In Topology Builder, right-click the top node **Lync Server**, and then click **Edit Properties**.
2. Select **Simple URLs** in the left pane, then below **Administrative access URL** box, enter the simple URL you want for administrative access to Lync Server

2013 Control Panel, and then click **OK**.

Tip:

We recommend using the simplest possible URL for the Admin URL. The simplest option is **https://admin.**<*domain*>.

See Also

Concepts

Planning for Simple URLs

1.6.1.7.4 Move Remaining Users to Lync Server 2013

Move Remaining Users to Lync Server 2013

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 6: Move from Pilot Deployment into Production >

Topic Last Modified: *2012-09-29*

You can move users to the new Lync Server 2013 deployment by using either Lync Server Control Panel or Lync Server Management Shell. You must meet some requirements to ensure a smooth transition to Lync Server 2013. For details about prerequisites to completing the procedures in this topic, see Configure Clients for Migration. For detailed steps about moving users, see Phase 4: Move test users to the Pilot Pool.

Important:

You cannot use the Active Directory Users and Computers snap-in or the Lync Server 2010 administrative tools to move users from your legacy environment to Lync Server 2013.

When you move a user to an Lync Server 2013 pool, the data for the user is moved to the back-end database that is associated with the new pool.

Important:

This includes the active meetings created by the legacy user. For example, if a legacy user has configured a **my meeting** conference, that conference will still be available in the new Lync Server 2013 pool after the user has been moved. The details to access that meeting will still be the same **conference URL and conference ID**. The only difference is that the conference is now hosted in the Lync Server 2013 pool, and not in the Lync Server 2010 pool.

Note:

Homing users on Lync Server 2013 does not require that you deploy upgraded clients at the same time. New functionality will be available to users only when they have upgraded to the new client software.

Post Migration Task

1. After you move users, verify the conferencing policy that is assigned to them.
2. To ensure that meetings organized by users homed on Lync Server 2013 work seamlessly with federated users who are homed on Lync Server 2010, the conferencing policy assigned to the migrated users should allow anonymous participants.
3. Conferencing policies that allow anonymous participants have **Allow participants to invite anonymous users** selected in Lync Server 2013 Control Panel and have **AllowAnonymousParticipantsInMeetings** set to **True** in the output from the **Get-CsConferencingPolicy** cmdlet in the Lync Server Management Shell.
4. For details about configuring conferencing policy by using Lync Server

Management Shell, see Set-CsConferencingPolicy in the Lync Server Management Shell documentation.

1.6.1.7.5 Configure XMPP Gateway on Lync Server 2013

Configure XMPP Gateway on Lync Server 2013

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 6: Move from Pilot Deployment into Production >

Topic Last Modified: *2012-10-19*

The final steps for migrating your XMPP Gateway are to configure certificates for the Lync Server 2013 Edge Server, deploy the Lync Server 2013 XMPP Gateway, and update the DNS records for the XMPP Gateway. These steps should be performed in parallel to minimize the down time of your XMPP Gateway. All users must be moved to your Microsoft Lync Server 2013 deployment before performing these steps.

⊟Configure XMPP Gateway Certificates on the Lync Server 2013 Edge Server

1. On the Edge Server, in the Deployment Wizard, next to **Step 3: Request, Install, or Assign Certificates**, click **Run again**.

   Tip:

   If you are deploying the Edge Server for the first time, you will see Run instead of Run Again.

2. On the **Available Certificate Tasks** page, click **Create a new certificate request**.
3. On the **Certificate Request** page, click **External Edge Certificate**.
4. On the **Delayed or Immediate Request** page, select the **Prepare the request now, but send it later** check box.
5. On the **Certificate Request File** page, type the full path and file name of the file to which the request is to be saved (for example, c:\cert_exernal_edge.cer).
6. On the **Specify Alternate Certificate Template** page, to use a template other than the default WebServer template, select the **Use alternative certificate template for the selected certification authority** check box.
7. On the **Name and Security Settings** page, do the following:
   7.a. In **Friendly name**, type a display name for the certificate.
   7.b. In **Bit length**, specify the bit length (typically, the default of 2048).
   7.c. Verify that the **Mark certificate private key as exportable** check box is selected.
8. On the **Organization Information** page, type the name for the organization and the organizational unit (for example, a division or department).
9. On the **Geographical Information** page, specify the location information.
10. On the **Subject Name/Subject Alternate Names** page, the information to be automatically populated by the wizard is displayed. If additional subject alternative names are needed, you specify them in the next two steps.
11. On the **SIP Domain Setting on Subject Alternate Names (SANs)** page, select the domain check box to add a sip.<sipdomain> entry to the subject alternative names list.
12. On the **Configure Additional Subject Alternate Names** page, specify any additional subject alternative names that are required.

    Tip:

    If the XMPP proxy is installed, by default the domain name (such as contoso.com) is populated in the SAN entries. If you require more entries, add them in this step.

13. On the **Request Summary** page, review the certificate information to be

used to generate the request.

14. After the commands finish running, you can **View Log**, or click Next to continue.
15. On the **Certificate Request File** page, you can view the generated certificate signing request (CSR) file by clicking **View** or exit the Certificate Wizard by clicking **Finish**.
16. Copy the request file and submit to your public certification authority.
17. After receiving, importing and assigning the public certificate, you must stop and restart the Edge Server services. You do this by typing in the Lync Server Management console:

```
Stop-CsWindowsService
```

```
Start-CsWindowsService
```

Configure a new Lync Server 2013 XMPP Gateway

1. Open Lync Server Control Panel.
2. In the left navigation bar, click **Federation and External Access** and then click **XMPP Federated Partners**.
3. To create a new configuration, click **New**.
4. Define the following settings:
5. **Primary domain** (Required). The primary domain is the base domain of the XMPP partner. For example, you would enter **fabrikam.com** for the XMPP partner domain name. This is a required entry.
6. **Description** The description is for notes or other identifying information for this particular configuration. This entry is optional.
7. **Additional domains** Additional domains are domains that are a part of your XMPP partner's domain that should be included as part of the allowed XMPP communication. For example, if the primary domain is **fabrikam.com**, then you would list all other domains that are under fabrikam.com that you will communicate with by way of XMPP.
8. **Partner type** The **Partner type** is a required setting. You must choose one of the following to describe and enforce what contacts can be added. You can select from:
   - **Federated** A **Federated** partner type represents a high level of trust between the Lync Server deployment and the XMPP partner. This partner type is recommended for federating with XMPP servers within the same enterprise or where there is an established business relationship. XMPP contacts in Federated partners can:

     8..a.Add Lync contacts and view their presence without express authorization from the Lync user.

     8..b.Send instant messages to Lync contacts whether or not the Lync user has added them into their contact list.

     8..c.See a Lync user's status notes.
   - **Public verified** A **Public verified** partner is a public XMPP provider that is trusted to verify the identity of its users. XMPP contacts in Public Verified networks can add Lync contacts and view their presence and send instant messages to them without express authorization from the Lync users. XMPP contacts in public verified networks never see a Lync users' status notes. This setting is not recommended.
   - **Public unverified** A **Public unverified** partner is a public XMPP provider that is not trusted to verify the identity of its users. XMPP users on Public Unverified networks cannot communicate with Lync users unless the Lync user has expressly authorized them by adding them to the contact list. XMPP users on public unverified networks never see Lync users' status notes. This setting is recommended for any federation with public XMPP providers such as Google Talk.
9. **Connection Type:** Defines the various rules and dialback settings.
   - **TLS Negotiation** Defines the TLS negotiation rules. An XMPP service can require TLS, can make TLS optional, or you define that TLS is not

supported. Choosing Optional leaves the requirement up to the XMPP service for a mandatory-to-negotiate decision. To view all possible settings and details for SASL, TLS and Dialback negotiation –including not valid and known error configurations - see Negotiation Settings for XMPP Federated Partners.

9..a.**Required** The XMPP service requires TLS negotiation.
9..b.**Optional** The XMPP service indicates that TLS is mandatory-to-negotiate.
9..c.**Not Supported** The XMPP service does not support TLS.

- **SASL negotiation** Defines the SASL negotiation rules. An XMPP service can require SASL, can make SASL optional, or you define that SASL is not supported. Choosing Optional leaves the requirement up to the partner XMPP service for a mandatory-to-negotiate decision.

  9..a.**Required** The XMPP service requires SASL negotiation.
  9..b.**Optional** The XMPP service indicates that SASL is mandatory-to-negotiate.
  9..c.**Not Supported** The XMPP service does not support SASL.

- **Support server dialback negotiation** The support server dialback negotiation process uses the domain name system (DNS) and an authoritative server to verify that the request came from a valid XMPP partner. To do this, the originating server creates a message of a specific type with a generated dialback key and looks up the receiving server in DNS. The originating server sends the key in an XML stream to the resulting DNS lookup, presumably the receiving server. On receipt of the key over the XML stream, the receiving server does not respond to the originating server, but sends the key to a known authoritative server. The authoritative server verifies that the key is either valid or not valid. If not valid, the receiving server does not respond to the originating server. If the key is valid, the receiving server informs the originating server that the identity and key is valid and the conversation can commence.

  There are two valid states for **Dialback negotiation**:

  9..a.**True** The XMPP server is configured to use Dialback negotiation if a request should be received from an originating server.
  9..b.**False** The XMPP server is not configured to use Dialback negotiation and if a request should be received from an originating server, it will be ignored.

10.Click **Commit** to save your changes to the site or user policy.

⊟Update DNS Records for Lync Server 2013 XMPP Gateway

1.To configure DNS for XMPP federation, you add the following SRV record to your external DNS:_xmpp-server._tcp.<domain name> The SRV record will resolve to the Access Edge FQDN of the Edge server, with a port value of 5269.

1.6.1.8 Phase 7: Complete Post-Migration Tasks

Phase 7: Complete Post-Migration Tasks

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010 to Lync Server 2013 >

Topic Last Modified: *2012-10-19*

The topics in this section describe tasks that you will need to perform after you have completed your migration to Lync Server 2013.

In This Section

1.6.1.8.1 Migrate Existing Meetings and Meeting Content

Migrate Existing Meetings and Meeting Content

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2013-02-22*

When a user account is moved from Lync Server 2010 to a Lync Server 2013 server, the following information is moved with that user account:

- **Meetings already scheduled by the user**. This includes moving the conferencing directories and conferencing data.
- **User's personal identification number (PIN)**. The user's current PIN continues to work until it expires or the user requests a new PIN.

The following user account information does not move to the new server.

- **Meeting content**. In order to move the content shared during a meeting, for example PowerPoint, Whiteboard, attachments or poll data, use the **-MoveConferenceData** parameter as part of the **Move-CsUser** cmdlet.

1.6.1.8.2 Migrate Dial-In Access Numbers

Migrate Dial-In Access Numbers

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-19*

Migrating dial-in access numbers from Lync Server 2010 to Lync Server 2013 requires running the **Move-CsApplicationEndpoint** cmdlet to migrate the contact objects. During the Lync Server 2010 and Lync Server 2013 coexistence period, dial-in access numbers that you created in Lync Server 2013 behave similarly to the dial-in access numbers that you create in Lync Server 2010, as described in this section.

Dial-in access numbers that you created in Lync Server 2010 but moved to Lync Server 2013 or that you created in Lync Server 2013 before, during or after migration have the following characteristics:

- Do not appear on Office Communications Server 2007 R2 meeting invitations and the dial-in access number page.

- Appear on Lync Server 2010 meeting invitations and the dial-in access number page.
- Appear on Lync Server 2013 meeting invitations and the dial-in access number page.
- Cannot be viewed or modified in the Office Communications Server 2007 R2 administrative tool.
- Can be viewed and modified in the Lync Server 2010 Control Panel and in Lync Server 2010 Management Shell.
- Can be viewed and modified in the Lync Server 2013 Control Panel and in Lync Server 2013 Management Shell.
- Can be re-sequenced within the region by using the Set-CsDialinConferencingAccessNumber cmdlet with the Priority parameter.

You must finish migrating dial-in access numbers that point to a Lync Server 2010 pool before you decommission the Lync Server 2010 pool. If you do not complete dial-in access number migration as described in the following procedure, incoming calls to the access numbers will fail.

Important:

You must perform this procedure prior to decommissioning the Lync Server 2010 pool.

Note:

We recommend that you move dial-in access numbers when network usage is low, in case there is a short period of service outage.

To identify and move dial-in access numbers

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. To move each dial-in access number to a pool hosted on Lync Server 2013, from the command line run:

```
Move-CsApplicationEndpoint -Identity <SIP URI of the access number to
```

3. Open Lync Server Control Panel.
4. In the left navigation bar, click **Conferencing**.
5. Click the **Dial-in Access Number** tab.
6. Verify that no dial-in access numbers remain for the Lync Server 2010 pool from which you are migrating.

Note:

When all dial-in access numbers point to the Lync Server 2013 pool, you can then decommission the Lync Server 2010 pool.

Verify the dial-in access number migration using Lync Server Control Panel

1. From a user account that is assigned to the **CsUserAdministrator** role or the **CsAdministrator** role, log on to any computer in your internal deployment.
2. Open Lync Server Control Panel.
3. In the left navigation bar, click **Conferencing**.
4. Click the **Dial-in Access Number** tab.
5. Verify all the dial-in access number are migrated to the pool hosted on Lync Server 2013.

Verify the dial-in access number migration using Lync Server Management Shell

1. Open Lync Server Management Shell.
2. To return all the dial-in conferencing access numbers migrated, from the command line run:

```
Get-CsDialInConferencingAccessNumber -Filter {Pool -eq "<FQDN of the p
```

3. Verify all the dial-in access numbers are migrated to the pool hosted on Lync Server 2013.

1.6.1.8.3 Migrate Call Park Application Settings

Migrate Call Park Application Settings

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-19*

The migration of the Call Park application from Lync Server 2010 to Lync Server 2013 includes provisioning the Lync Server 2013 pool with any custom music on hold files that have been uploaded in Lync Server 2010, restoring the service level settings and retargeting all Call Park orbits to the Lync Server 2013 pool. If customized music-on-hold files have been configured in the Lync Server 2010 pool, these files need to be copied to the new Lync Server 2013 pool. Additionally, it is recommended that you back up any Call Park customized music-on-hold files from Lync Server 2010 to another destination to keep a separate backup copy of any customized music-on-hold files that have been uploaded for Call Park. The customized music-on-hold files for the Call Park application are stored in the file store of the pool. To copy the audio files from a Lync Server 2010 pool file store to a Lync Server 2013 file store, use the **Xcopy** command with the following parameters:

```
Xcopy <Source: Lync Server 2010 Pool CPS File Store Path> <Destination: Lync Serv
```

```
Example usage:  Xcopy "<Lync Server 2010 File Store Path>\OcsFileStore\coX-Applic
```

When all customized audio files have been copied to the Lync Server 2013 file store, the Call Park application settings of the Lync Server 2013 pool must be configured, and the Call Park orbit ranges that are associated with the Lync Server 2010 pool must be reassigned to the Lync Server 2013 pool.

The Call Park application settings include the pickup timeout threshold, enabling or disabling music on hold, the maximum call pickup attempts and the timeout request. You must manage Call Park application settings by using the Lync Server Management Shell to run the **Set-CsCpsConfiguration** cmdlet. You cannot manage the Call Park application settings using the Lync Server Control Panel.

Reconfigure the Call Park Service Settings

1. From the Lync Server 2013 Front End Server, open the Lync Server Management Shell.
2. At the command line, type the following:

   Note:

   If your Lync Server 2013 Call Park application settings are identical to the legacy Lync Server 2010 settings, you can skip running this step. If Call Park application settings are different for the Lync Server 2013 and Lync Server 2010 environments, use the cmdlet below as a template to update those changes.

   ```
   Set-CsCpsConfiguration -Identity "<LS2013 Call Park Service ID>" -Call
   ```

To reassign all Call Park orbit ranges from Lync Server 2010 pool to the Lync Server 2013 pool, you can use either the Lync Server Control Panel or the Lync Server Management Shell.

Reassign all Call Park Orbit Ranges using Lync Server Control Panel

1. Open Lync Server Control Panel.
2. In the left pane, select **Voice Features**.
3. Select the **Call Park** tab.
4. For each Call Park orbit range assigned to a Lync Server 2010 pool, edit the **FQDN of destination server** setting and select the Lync Server 2013 pool that will process the Call Park requests.

5. Select **Commit** to save the changes.

Reassign all Call Park Orbit Ranges using Lync Server Management Shell

1. Open Lync Server Management Shell.
2. At the command line, type the following:

   ```
   Get-CsCallParkOrbit
   ```

   This cmdlet lists all of the Call Park orbit ranges in the deployment. All Call Park orbits that have the **CallParkServiceId** and **CallParkServerFqdn** parameters set as the Lync Server 2010 pool must be reassigned.

   To reassign the Lync Server 2010 Call Park orbit ranges to the Lync Server 2013 pool, at the command line, type the following:

   ```
   Set-CsCallParkOrbit -Identity "<Call Park Orbit Identity>" -CallParkSe
   ```

After reassigning all Call Park orbit ranges to the the Lync Server 2013 pool, the migration process for the Call Park application will be completed and the Lync Server 2013 pool will handle all future Call Park requests.

1.6.1.8.4 Migrate Response Groups

Migrate Response Groups

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

***Topic Last Modified:** 2012-10-19*

After your users are moved to Lync Server 2013 pools, you can migrate your response groups. Migrating response groups includes copying agent groups, queues, workflows, audio files, and moving Response Group contact objects from the legacy deployment to the Lync Server 2013 pool. After you migrate your legacy response groups, calls to the response groups are handled by the Response Group application in the Lync Server 2013 pool. Calls to response groups are no longer handled by the legacy pool.

Note:

Although you can migrate response groups before you move all users to the Lync Server 2013 pool, we recommend that you move all users first. In particular, users who are response group agents will not have full functionality of new features until they are moved to the Lync Server 2013 pool.

Before you migrate response groups, you must have deployed a Lync Server 2013 pool that includes the Response Group application. The Response Group application is installed and activated by default when you deploy Enterprise Voice. You can ensure that the Response Group application is installed by running the **Get-CsService–ApplicationServer** cmdlet.

Note:

You can create new Lync Server 2013 response groups in the Lync Server 2013 pool before you migrate your legacy response groups.

To migrate response groups from a legacy pool to the Lync Server 2013, you run the **Move-CsRgsConfiguration** cmdlet.

Important:

The Response Group migration cmdlet moves the Response Group configuration for the entire pool. You cannot select specific groups, queues, or workflows to migrate.

After you migrate the response groups, you need to use Lync Server Control Panel or Lync Server Management Shell cmdlets to verify that all agent groups, queues, and workflows moved successfully.

When you migrate response groups, the Lync Server 2010 response groups are not removed. When you manage response groups after migration by using either Lync Server Control Panel or Lync Server Management Shell, you can see both the Lync Server 2010 response groups and the Lync Server 2013 response groups. You should apply updates only to the Lync Server 2013 response groups. The Lync Server 2010 response groups are retained only for rollback purposes.

Caution:

Do not remove Lync Server 2010 response groups. If you remove a Lync Server 2010 response group, the response groups in Lync Server 2013 stop working.

Important:

We recommend that you do not remove any data from your previous deployment until you decommission the pool. In addition, we strongly recommend that you export response groups immediately after you migrate. If a Lync Server 2010 response group should get removed, you can then restore your response groups from the backup to get Lync Server 2013 response groups running again.

Lync Server 2013 introduces a new Response Group feature called **Workflow Type**. **Workflow Type** can be **Managed** or **Unmanaged**. All response groups are migrated with **Workflow Type** set to **Unmanaged** and with an empty Manager list.

When you run the **Move-CsRgsConfiguration** cmdlet, the agent groups, queues, workflows, and audio files remain in the legacy pool for rollback purposes. If you do need to roll back to the legacy pool, however, you need to run the **Move-CsApplicationEndpoint** cmdlet to move contact objects back to the legacy pool.

The following procedure for migrating Response Group configurations assumes that you have a one-to-one relationship between your legacy pools and the Lync Server 2013 pools. If you plan to consolidate or split up pools during your migration and deployment, you need to plan which legacy pool maps to which Lync Server 2013 pool.

To migrate Response Group configurations

1. Log on to the computer with an account that is a member of the RTCUniversalServerAdmins group or has equivalent administrator rights and permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

   ```
   Move-CsRgsConfiguration -Source <source pool FQDN> -Destination <desti
   ```

   For example:

   ```
   Move-CsRgsConfiguration -Source lync-old.contoso.net -Destination lync
   ```

4. After you migrate response groups and agents to the Lync Server 2013 pool, the URL that agents use to sign in and sign out is a Lync Server 2013 URL and is available from the **Tools** menu. Remind agents to update any references, such as bookmarks, to the new URL.

To verify Response Group migration by using Lync Server Control Panel

1. Log on to the computer with an account that is a member of RTCUniversalReadOnlyAdmins group or is minimally a member of the CsViewOnlyAdministrator role.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation pane, click **Response Groups**.

4. On the **Workflow** tab, verify that all the workflows in your Lync Server 2010 environment are included in the list.
5. Click the **Queue** tab, and verify that all the queues in your Lync Server 2010 environment are included in the list.
6. Click the **Group** tab, and verify that all the agent groups in your Lync Server 2010 environment are included in the list.

To verify Response Group migration by using Lync Server Management Shell

1. Log on to the computer with an account that is a member of RTCUniversalReadOnlyAdmins group or is minimally a member of the CsViewOnlyAdministrator role.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

   For details about the following cmdlets, run:

   ```
   Get-Help <cmdlet name> -Detailed
   ```
3. Run:

   ```
   Get-CsRgsAgentGroup
   ```
4. Verify that all the agent groups in your Lync Server 2010 environment are included in the list.
5. Run:

   ```
   Get-CsRgsQueue
   ```
6. Verify that all the queues in your Lync Server 2010 environment are included in the list.
7. Run:

   ```
   Get-CsRgsWorkflow
   ```
8. Verify that all the workflows in your Lync Server 2010 environment are included in the list.

1.6.1.8.5 Migrate Address Book

Migrate Address Book

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-09*

In general, the Lync Server 2010 Address Book is migrated along with the rest of your topology. However, you might need to perform some post-migration steps if you customized the following in your Lync Server 2010 environment:

- Set the **PartitionbyOU** WMI property to group Address Book entries by organizational unit (OU).
- Customized the Address Book normalization rules.
- Changed the default value for the **UseNormalizationRules** parameter to False.

Grouped Address Book Entries

If you set the **PartitionbyOU** WMI property to True to create address books for each OU, you need to set the **msRTCSIP-GroupingId** Active Directory attribute on users and contacts if you want to continue grouping address book entries. You might want to group address book entries to limit the scope of Address Book searches. To use the **msRTCSIP-GroupingId** attribute, write a script to populate the attribute, assigning the same value for all of the users that you want to group together. For example, assign a single value for all the users in an OU.

Address Book Normalization Rules

If you customized Address Book normalization rules in your Lync Server 2010 environment, you must migrate the customized rules to your pilot pool. If you did not customize Address Book normalization rules, you have nothing to migrate for Address Book service. The default normalization rules for Lync Server 2013 are the same as the default rules for Lync Server 2010. Follow the procedure later in this section to migrate customized normalization rules.

> **Note:**
>
> If your organization uses remote call control and you customized Address Book normalization rules, you must perform the procedure in this topic before you can use remote call control. The procedure requires membership in the RTCUniversalServerAdmins group or equivalent rights.

UseNormalizationRules Set to False

If you set the value for **UseNormalizationRules** to False so that users can use phone numbers as they are defined in Active Directory Domain Services (AD DS) without having Lync Server 2013 apply normalization rules, you need to set the **UseNormalizationRules** and **IgnoreGenericRules** parameters to True. Follow the procedure later in this section to set these parameters to True.

To migrate Address Book customized normalization rules

1. Find the Company_Phone_Number_Normalization_Rules.txt file in the root of the Address Book shared folder, and copy it to the root of the Address Book shared folder in your Lync Server 2013 pilot pool.

   > **Note:**
   >
   > The sample Address Book normalization rules have been installed in your ABS Web component file directory. The path is **$installedDriveLetter:\Program Files\Microsoft Lync Server 2013\Web Components\Address Book Files\Files\ Sample_Company_Phone_Number_Normalization_Rules.txt,**. This file can be copied and renamed as **Company_Phone_Number_Normalization_Rules.txt** to the address book shared folder’s root directory. For example, the address book shared in **$serverX**, the path will be similar to: **\\$serverX \LyncFileShare\2-WebServices-1\ABFiles**.

2. Use a text editor, such as Notepad, to open the Company_Phone_Number_Normalization_Rules.txt file.
3. Certain types of entries will not work correctly in Lync Server 2013. Look through the file for the types of entries described in this step, edit them as necessary, and save the changes to the Address Book shared folder in your pilot pool.

   Strings that include required whitespace or punctuation cause normalization rules to fail because these characters are stripped out of the string that is input to the normalization rules. If you have strings that include required whitespace or punctuation, you need to modify the strings. For example, the following string would cause the normalization rule to fail:

   ```
   \s*\(\s*\d\d\d\s*\)\s*\-\s*\d\d\d\s*\-\s*\d\d\d\d
   ```

   The following string would not cause the normalization rule to fail:

   ```
   \s*\(?\s*\d\d\d\s*\)?\s*\-?\s*\d\d\d\s*\-?\s*\d\d\d\d
   ```

To set UseNormalizationRules and IgnoreGenericRules to true

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management**

Shell.

2. Do one of the following:
   - If your deployment includes only Lync Server 2013, run the following cmdlet at the global level to change the values for **UseNormalizationRules** and **IgnoreGenericRules** to True:

     ```
     Set-CsAddressBookConfiguration -identity <XdsIdentity> -UseN
     ```

   - If your deployment includes a combination of Lync Server 2013 and Lync Server 2010 or Office Communications Server 2007 R2, run the following cmdlet and assign it to each Lync Server 2013 pool in the topology:

     ```
     New-CsAddressBookConfiguration -identity <XdsIdentity> -UseN
     ```

3. Wait for Central Management store replication to occur on all pools.
4. Modify the phone normalization rules file, "Company_Phone_Number_Normalization_Rules.txt", for your deployment to clear the content. The file is on the file share of each Lync Server 2013 pool. If the file is not present, then create an empty file named "Company_Phone_Number_Normalization_Rules.txt".
5. Wait several minutes for all Front End pools to read the new files.
6. Run the following cmdlet on each Lync Server 2013 pool in your deployment:

   ```

   Update-CsAddressBook
   ```

1.6.1.8.6 Configure the Meeting Join Page

Configure the Meeting Join Page

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-12-14*

When a user clicks a meeting link in a meeting request, the meeting join page detects whether a Lync 2013 client is already installed on the user’s computer. If a client is already installed, that client opens and joins the meeting. If a client is not installed, by default the 2013 version of Lync Web App opens.

You can modify the behavior of the meeting join page if you want to allow users to join meetings with Office Communicator 2007 R2 or Lync 2010 Attendant. These configuration options have been removed from the Lync Server 2013 Control Panel, but you configure them by using the CsWebServiceConfiguration cmdlet.

Meeting Join Page CsWebServiceConfiguration Parameters

CsWebServiceConfiguration Parameter	Description
ShowJoinUsingLegacyClientLink	If set to True, users joining a meeting by using a client application other than Lync will be given the opportunity to join the meeting by using Office Communicator 2007 R2. The default value is False.
ShowAlternateJoinOptionsExpanded	When set to True then alternate options for joining an online conference (such as Office Communicator 2007 R2) will automatically be expanded and shown to users. When set to False (the default value) these options will be available, but the user will have to display the list of options for themselves.

To configure the meeting join page by using Lync Server 2013 Management Shell

1. Start the Lync Server 2013 Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the following cmdlet:

   ```
   Get-CsWebServiceConfiguration
   ```

   This cmdlet returns the web service configuration settings.
3. Run the following command, with the parameters set to True or False, depending on your preference (for details about the parameters for this cmdlet, see the Lync Server 2013 Management Shell documentation):

   ```
   Set-CsWebServiceConfiguration -Identity global -ShowJoinUsingLegacyCli
   ```

1.6.1.8.7 Remove Legacy Archiving and Monitoring Servers

Remove Legacy Archiving and Monitoring Servers

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-19*

If your legacy deployment contained an Archiving Server or a Monitoring Server, after migrating to Lync Server 2013, those servers can be removed from the legacy environment provided all users have been removed from any remaining legacy pools. You can remove the Archiving Server or Monitoring Server in any sequence. The key requirement is that all users have been removed from any remaining legacy pools.

You can move users from Lync Server 2010 to Lync Server 2013 by following the procedures outlined in Phase 4: Move test users to the Pilot Pool.

After you have confirmed that all users have been removed from any remaining pools, follow the procedure in "Uninstalling Microsoft Lync Server 2010 and Removing Server Roles," which can be downloaded at http://go.microsoft.com/fwlink/p/?linkId=246227.

1.6.1.8.8 Configure Trusted Application Servers

Configure Trusted Application Servers

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-11*

In a mixed environment, if you create a new trusted application server, you must set the next hop pool to be a Lync Server 2013 pool. In a mixed environment, both the legacy Lync Server 2010 pool and the Lync Server 2013 pool appear in the drop down list. Selecting the legacy pool is not supported.

Select Lync Server 2013 as next hop when creating a Trusted application server

1. Open Topology Builder.
2. In the left pane, right click **Trusted application servers** and click **New Trusted Application Pool**.
3. Enter the **Pool FQDN** of the trusted application pool and select whether it will be a single-server or multiple-server.
4. Click **Next**.
5. On the **Select the next hop** page, from the list, select the Lync Server 2013 Front End pool.
6. Click **Finish**.
7. Select the top node **Lync Server** and from the **Action** menu, select **Publish**.
   Verify the **Trusted Application Pool** has been created successfully and is associated with the correct Front End pool.

1.6.1.8.9 Deploy Lync Server 2013 Clients

Deploy Lync Server 2013 Clients

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-09-08*

For details, see Deploying Clients and Devices in the Deployment documentation.

1.6.1.8.10 Connect a Survivable Branch Appliance

Connect a Survivable Branch Appliance

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-19*

Every Survivable Branch Appliance (SBA) is associated with a Front End pool which serves as a backup registrar for the SBA. When the Front End pool is migrated to Lync Server 2013, the SBA must be disassociated from the Lync Server 2010 Front End pool while the pool is upgraded, Once the pool has been migrated to Lync Server 2013, the SBA can be re-associated with the upgraded Front End pool. This involves deleting the SBA from the legacy Lync Server 2010 topology in Topology Builder and then adding the SBA to the Lync Server 2013 topology. Users homed on the legacy Lync Server 2010 SBA must first be moved to another Front End pool before removing the SBA from the topology. Once the SBA is added to the Lync Server 2013 topology, those users can then be moved back to the SBA. These steps are summarized below:

1. Move branch users homed on the legacy SBA Lync Server 2010 to another Front End pool.
2. Remove SBA from the legacy Lync Server 2010 topology to disconnect the existing Front End pool as a backup registrar.
3. Add SBA to the Lync Server 2013 topology and configure this new Front End pool as the backup registrar.
4. Move the branch users to the new Lync Server 2013 SBA.

Add Lync Server 2010 SBA Branch Site to Your Topology

1. Open **Topology Builder**.
2. In the left pane right-click **Branch sites**, and then click **New Branch Site**.
3. In the **Define New Branch Site** dialog box, click **Name**, and then type the name of the branch site.
4. (Optional) Click **Description**, and then type a meaningful description for the branch site.
5. Click **Next**.

6.(Optional) In the next **Define New Branch Site** dialog box, do any of the following:
6.a.Click **City**, and then type the name of the city in which the branch site is located.
6.b.Click **State/Region**, and then type the name of the state or region in which the branch site is located.
6.c.Click **Country Code**, and then type the two-digit calling code for the country/region in which the branch site is located.
7.Click **Next**, and then do one of the following:
7.a.If you are using a Lync 2010 Survivable Branch Appliance or Server at this site, be sure to uncheck the **Open the New Survivable Wizard when this wizard closes** option. Click **Finish**.
8.To associate the legacy Lync Server 2010 SBA to the Lync Server 2013 Front End pool:
8.a.Expand the branch site that has been created.
8.b.Right click on **Lync Server 2010** and then click **New**.
8.c.Click **Survivable Branch Appliance…**
9.Follow the directions in the wizard that opens. For information about wizard items, see Define a Survivable Branch Appliance or Server.

> **Note:**
> A Lync Server 2010 Survivable Branch Appliance can only be associated with a Lync Server 2010 Monitoring Store.

10.If you are not using a Survivable Branch Appliance or Server at this site, clear the **Open the New Survivable Wizard when this wizard closes** check box, and then click **Finish**.
11.Repeat the previous steps for each branch site you want to add to the topology.

1.6.1.8.11 Configure SCOM Monitoring

Configure SCOM Monitoring

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-04*

After migrating to Microsoft Lync Server 2013, you must complete a few tasks to configure Lync Server 2013 to work with System Center Operations Manager.

- Apply Lync Server 2010 updates to a server elected to manage the central discovery logic.
- Update the central discovery candidate server registry key.
- Configure your primary System Center Operations Manager management server to override the candidate central discovery node.

Instructions for carrying out each of these tasks are provided below.

Apply Lync Server 2010 updates to a server elected to manage the central discovery logic.
1.Elect a server that has the System Center Operations Manager agent files installed and is configured as a candidate discovery node.
2.Apply Lync Server 2010 updates to this server. See the topic Apply Lync Server 2010 Updates.
Update the central discovery candidate server registry key.
1.On the server elected to manage the central discovery logic, open a Windows PowerShell command window.
2.At the command line, type the following:

```
New-Item -Path "HKLM:\Software\Microsoft\Real-Time Communications\Heal
```

```
New-Item -Path "HKLM:\Software\Microsoft\Real-Time Communications\Heal
```

Note:
Whenever you edit the registry, you may experience an error that the command failed if the registry key already exists. If you experience this, you can safely ignore the error.

Configure your primary System Center Operations Manager management server to override the candidate central discovery watcher node.

1. On a computer where the System Center Operations Manager console has been installed, expand **Management Pack Objects** and then select **Object Discoveries**.
2. Click **Change Scope...**
3. From the **Scope Management Pack Objects** page, select **LS Discovery Candidate**.
4. Override the **LS Discovery Candidate Effective Value** to the name of the candidate server elected in the earlier procedure.

Lastly, to finalize your changes, restart the health service on the System Center Operations Manager Root Management Server.

1.6.1.8.12 Migrate Common Area Phones

Migrate Common Area Phones

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-09-29*

Common Area Phones are IP phones that most often reside in a shared workspace or common area, like a lobby, kitchen, or factory floor. Common Area Phones do not need to be connected to a computer to provide Lync Server UC functionality. After migrating an Lync Server 2010 deployment to Lync Server 2013, you must also migrate the contact objects associated with the legacy Common Area Phone. Using Lync Server Management Shell you will first retrieve all contact objects associated with the Lync Server 2010 Common Area Phones, and then move those objects to the Lync Server 2013 pool.

Migrate Common Area Phones

1. From the Lync Server 2013 Front End server, open Lync Server Management Shell.
2. From the command line, type the following:

```
Get-CsCommonAreaPhone -Filter {RegistrarPool -eq "pool01.contoso.net"}
```

3. To verify all contact objects have been moved to the Lync Server 2013 pool, from the Lync Server Management Shell type the following:

```
Get-CsCommonAreaPhone -Filter {RegistrarPool -eq "pool02.contoso.net"}
```

   Verify all contact objects are now associated with the Lync Server 2013 pool.

1.6.1.8.13 Migrate Analog Devices

Migrate Analog Devices

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 7: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-16*

Lync Server provides support for analog devices. Specifically, the supported analog devices are analog audio phones and analog fax machines. You can configure the qualified gateways to support the use of analog devices in your Lync Server environment.

After you migrate from Lync Server 2010 to Lync Server 2013, you must also migrate the contact objects associated with the analog devices. Use Lync Server Management Shell to first retrieve all contact objects associated with the Lync Server 2010 analog devices, and then move those objects to the Lync Server 2013 pool.

To migrate analog devices

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. At the command line, type:
   ```
   Get-CsAnalogDevice -Filter {RegistrarPool -eq "pool01.contoso.net"} |
   ```
3. Verify that all contact objects have been moved to the Lync Server 2013 pool. At the command line, type:
   ```
   Get-CsAnalogDevice -Filter {RegistrarPool -eq "pool02.contoso.net"}
   ```
4. Verify that all the contact objects are now associated with the Lync Server 2013 pool.

1.6.1.9 Phase 8: Decommission Legacy Pools

Phase 8: Decommission Legacy Pools

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010 to Lync Server 2013 >

Topic Last Modified: *2012-10-19*

The following topic provides guidance in updating DNS entries, moving the Content Management Server, decommissioning pools, and deactivating and removing servers and pools from a legacy deployment of Lync Server 2010. Not all of the procedures listed in this section are required. Read the documentation and determine which decommissioning procedure to use.

For exhaustive coverage of removing Lync Server 2010 servers and server roles, and a step-by-step guide to decommissioning a Lync Server 2010 deployment, see "Uninstalling Microsoft Lync Server 2010 and Removing Server Roles," which can be downloaded at http://go.microsoft.com/fwlink/p/?linkId=246227.

Important:

For information on migrating and upgrading Microsoft Unified Communications Managed API (UCMA) applications, prior to decommissioning your legacy environment, see http://go.microsoft.com/fwlink/p/?LinkId=269555

- Update DNS SRV Records
- Move the Lync Server 2010 Configuration Management Server to Lync Server 2013
- Remove the Archiving Server Association
- Remove the Monitoring Server Association
- Remove the Enterprise Edition Front End Server or Standard Edition Front End Server
- Remove SQL Server Instances and Databases on the Back End Server

1.6.1.9.1 Update DNS SRV Records

Update DNS SRV Records

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools >

Topic Last Modified: *2012-09-29*

To successfully complete this procedure, you should be logged on to the server or domain as a member of the Domain Admins group or a member of the DnsAdmins group.

This topic describes how to update the Domain Name System (DNS) records after migrating to Lync Server 2013. After all users have been moved to Lync Server 2013, but before the legacy Lync Server 2010 pool or Director is decommissioned, you must update the DNS SRV records in your internal DNS for every SIP domain. This procedure assumes that your internal DNS has zones for your SIP user domains.

To configure a DNS SRV record

1. On the DNS server, click **Start**, click **Administrative Tools**, and then click **DNS**.
2. In the console tree for your SIP domain, expand **Forward Lookup Zones**, expand the SIP domain in which Lync Server 2013 is installed, and navigate to the **_tcp** setting.
3. In the right pane, right click **_sipinternaltls** and select **Properties**.
4. In **Host offering this service**, update the host FQDN to point to the Lync Server 2013 pool.
5. Click **OK**.

To verify that the FQDN of the Front End pool or Standard Edition server can be resolved

1. Log on to a client computer in the domain.
2. Click **Start**, and then click **Run**.
3. In the **Open** box, type **cmd**, and then click **OK**.
4. At the command prompt, type **nslookup** *<FQDN of the Front End pool>* or *<FQDN of the Standard Edition server>*, and then press ENTER.
5. Verify that you receive a reply that resolves to the appropriate IP address for the FQDN.

1.6.1.9.2 Move the Lync Server 2010 Configuration Management Server to Lync Server 2013

Move the Lync Server 2010 Configuration Management Server to Lync Server 2013

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools >

Topic Last Modified: *2012-10-05*

After migrating from Lync Server 2010 to Lync Server 2013, you need to move the Lync Server 2010 Central Management Server to the Lync Server 2013 Front End Server or pool, before you can remove the legacy Lync Server 2010 server.

The Central Management Server is a single master/multiple replica system, where the read/write copy of the database is held by the Front End Server that contains the Central Management Server. Each computer in the topology, including the Front End Server that contains the Central Management Server, has a read-only copy of the Central Management store data in the SQL Server database (named RTCLOCAL by default) installed on the computer during setup and deployment. The local database receives replica updates by way of the Lync Server Replica Replicator Agent that runs as a service on all computers. The name of the actual database on the Central Management Server and the local replica is XDS, which is made up of the xds.mdf and xds.ldf files. The master database location is referenced by a service control point (SCP) in Active Directory Domain Services (AD DS). All tools that use the Central Management Server to manage and configure Lync Server use the SCP to locate the Central Management store.

After you have successfully moved the Central Management Server, you should remove the Central Management Server databases from the original Front End Server. For information on removing the Central Management Server databases, see Remove the SQL Server Database for a Front End Pool.

You use the Windows PowerShell cmdlet **Move-CsManagementServer** in the Lync Server Management Shell to move the database from the Lync Server 2010 SQL Server database to the Lync Server 2013 SQL Server database, and then update the SCP to point to the Lync Server 2013 Central Management Server location.

Preparing Lync Server 2013 Front End Servers before moving the Central Management Server

Use the procedures in this section to prepare the Lync Server 2013 Front End Servers before you move the Lync Server 2010 Central Management Server.

⊟To prepare an Enterprise Edition Front End pool

1. On the Lync Server 2013 Enterprise Edition Front End pool where you want to relocate the Central Management Server: Log on to the computer where the Lync Server Management Shell is installed as a member of the **RTCUniversalServerAdmins** group. You must also have SQL Server database sysadmin user rights and permissions on the database where you want to install the Central Management store.
2. Open the Lync Server Management Shell.
3. To create the new Central Management store in the Lync Server 2013 SQL Server database, in the Lync Server Management Shell, type:

   ```
   Install-CsDatabase -CentralManagementDatabase -SQLServerFQDN <FQDN of
   ```

4. Confirm that the status of the **Lync Server Front-End** service is **Started**.

⊟To prepare a Standard Edition Front End Server

1. On the Lync Server 2013 Standard Edition Front End Server where you want to relocate the Central Management Server: Log on to the computer where the Lync Server Management Shell is installed as a member of the **RTCUniversalServerAdmins** group.
2. Open the Lync Server Deployment Wizard.
3. In the Lync Server Deployment Wizard, click **Prepare first Standard Edition server**.
4. On the **Executing Commands** page, SQL Server Express is installed as the Central Management Server. Necessary firewall rules are created. When the installation of the database and prerequisite software is completed, click **Finish**.

   Note:

   The initial installation may take some time with no visible updates to the command output summary screen. This is due to the installation of the SQL Server Express. If you need to monitor the installation of the database, use Task Manager to monitor the setup.

5. To create the new Central Management store on the Lync Server 2013 Standard Edition Front End Server, in the Lync Server Management Shell, type:

   ```
   Install-CsDatabase -CentralManagementDatabase -SQLServerFQDN <FQDN of
   ```

6. Confirm that the status of the **Lync Server Front-End** service is **Started**.

⊟To move the Lync Server 2010 Central Management Server to Lync Server 2013

1. On the Lync Server 2013 server that will be the Central Management Server: Log on to the computer where the Lync Server Management Shell is installed as a member of the **RTCUniversalServerAdmins** group. You must also have the SQL Server database administrator user rights and permissions.
2. Open Lync Server Management Shell.
3. In the Lync Server Management Shell, type:

   ```
   Enable-CsTopology
   ```

   > **Warning:**
   >
   > If `Enable-CsTopology` is not successful, resolve the problem preventing the command from completing before continuing. If **Enable-CsTopology** is not successful, the move will fail and it may leave your topology in a state where there is no Central Management store.

4. On the Lync Server 2013 Front End Server or Front End pool, in the Lync Server Management Shell, type:

   ```
   Move-CsManagementServer
   ```

5. Lync Server Management Shell displays the servers, file stores, database stores, and the service connection points of the Current State and the Proposed State. Read the information carefully and confirm that this is the intended source and destination. Type **Y** to continue, or **N** to stop the move.
6. Review any warnings or errors generated by the **Move-CsManagementServer** command and resolve them.
7. On the Lync Server 2013 server, open the Lync Server Deployment Wizard.
8. In Lync Server Deployment Wizard, click **Install or Update Lync Server System**, click **Step 2: Setup or Remove Lync Server Components**, click **Next**, review the summary, and then click **Finish**.
9. On the Lync Server 2010 server, open the Lync Server Deployment Wizard.
10. In Lync Server Deployment Wizard, click **Install or Update Lync Server System**, click **Step 2: Setup or Remove Lync Server Components**, click **Next**, review the summary, and then click **Finish**.
11. To confirm that replication with the new Central Management store is occurring, in the Lync Server Management Shell, type:

    ```
    Get-CsManagementStoreReplicationStatus
    ```

    > **Note:**
    >
    > The replication may take some time to update all current replicas.

To remove Lync Server 2010 Central Management store files after a move

1. On the Lync Server 2010 server: Log on to the computer where the Lync Server Management Shell is installed as a member of the **RTCUniversalServerAdmins** group. You must also have the SQL Server database administrator user rights and permissions.
2. Open Lync Server Management Shell

   > **Warning:**
   >
   > Do not proceed with the removal of the previous database files until replication is complete and is stable. If you remove the files prior to completing replication, you will disrupt the replication process and leave the newly moved Central Management Server in an unknown state. Use the cmdlet **Get-CsManagementStoreReplicationStatus** to confirm the replication status.

3. To remove the Central Management store database files from the Lync Server 2010 Central Management Server, type:

   ```
   Uninstall-CsDatabase -CentralManagementDatabase -SqlServerFqdn <FQDN c
   ```

   For example:

   ```
   Uninstall-CsDatabase -CentralManagementDatabase -SqlServerFqdn sql.con
   ```

Where the *<FQDN of SQL Server>* is either the Lync Server 2010 Back End Server in an Enterprise Edition deployment or the FQDN of the Standard Edition server.

1.6.1.9.3 Remove the Archiving Server Association

Remove the Archiving Server Association

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools >

Topic Last Modified: *2012-10-04*

To remove an Archiving Server, you need to change or clear the dependency on the associated Front End pool, Front End Server, Survivable Branch Appliance and Survivable Branch Server. You edit the properties of the Front End pool, Front End Server, Survivable Branch Appliance and Survivable Branch Server to remove the dependency. After you clear the dependency and you delete the server in Topology Builder, you are notified that the associated database store object in Topology Builder will also be deleted.

⊟To remove the Archiving Server association

1. Open the Lync Server 2013 Front End Server, open Topology Builder.
2. Navigate to the Lync Server 2010 node.
3. In Topology Builder, expand **Enterprise Edition Front End pools**, **Standard Edition Front End Servers**, or **Branch sites**, based on where the Archiving Server is defined.
4. If you have Survivable Branch Server associated, expand **Branch sites**, expand the branch site name, and then expand **Survivable Branch Appliances**.

   > **Note:**
   >
   > **Survivable Branch Appliances** in the user interface applies to both Survivable Branch Server and Survivable Branch Appliance.

5. Right-click the pool, server, or device that is associated with the Archiving Server, and then click **Edit Properties**.
6. In **Edit Properties**, under **General**, under **Associations**, clear the **Associate Archiving Server** check box, and then click **OK**.
7. Repeat the previous step for any other pool, server or device associated with the Archiving Server that you want to remove.
8. Right-click the Archiving Server, and then click **Delete**.
9. On **Delete Dependent Stores**, click **OK**.
10. Publish the topology, check replication status, and then run the Lync Server Deployment Wizard as needed.

1.6.1.9.4 Remove the Monitoring Server Association

Remove the Monitoring Server Association

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools >

Topic Last Modified: *2012-10-04*

To remove the Monitoring Server, you need to change or clear the dependency on the associated Front End pool, Front End Server, Survivable Branch Appliance and Survivable Branch Server. You edit the properties of the Front End pool, Front End Server, Survivable Branch Appliance and Survivable Branch Server to remove the dependency. After you clear the dependency and delete the server in Topology Builder, you are notified that the associated database store object in Topology Builder will also be deleted.

⊟To remove the Monitoring Server association

1. Open the Lync Server 2013 Front End Server, open Topology Builder.
2. Navigate to the Lync Server 2010 node.
3. In Topology Builder, expand **Enterprise Edition Front End pools**, **Standard Edition Front End Servers**, or **Branch sites**, based on where the Monitoring Server is defined.
4. If you have Survivable Branch Server associated, expand **Branch sites**, expand the branch site name, and then expand **Survivable Branch Appliances**.

   Note:

   Survivable Branch Appliances in the user interface applies to both Survivable Branch Server and Survivable Branch Appliance.
5. Right-click the pool, server, or device that is associated with the Monitoring Server, and then click **Edit Properties**.
6. In **Edit Properties**, under **General**, under **Associations**, clear the **Associate Monitoring Server** check box, and then click **OK**.
7. Repeat the previous step for any other pool, server or device associated with the Monitoring Server.
8. Right-click the Monitoring Server, and then click **Delete**.
9. On **Delete Dependent Stores**, click **OK**.
10. Publish the topology, check replication status, and run the Lync Server Deployment Wizard as needed.

1.6.1.9.5 Remove the Enterprise Edition Front End Server or Standard Edition Front End Server

Remove the Enterprise Edition Front End Server or Standard Edition Front End Server

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools >

***Topic Last Modified:** 2012-10-10*

The procedures outlined in this topic are designed to guide you through the process of removing a Microsoft Lync Server 2010 Enterprise Edition Front End pool or a Standard Edition Front End Server. After migrating to Lync Server 2013, this is one of the first steps to decommissioning your legacy Lync Server 2010 environment.

- Reset Call Admission Control
- Prevent Sessions for Services
- Stop Lync Server 2010 Services
- Remove a Front End Server from a Pool
- Remove Front End Pool or Standard Edition Server

1.6.1.9.5.1 Reset Call Admission Control

Reset Call Admission Control

Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools > Remove the Enterprise Edition Front End Server or Standard Edition Front End Server >

***Topic Last Modified:** 2012-10-11*

If a Lync Server 2010 Front End pool is hosting call admission control (CAC), you must move CAC hosting to a Lync Server 2013 pool before you can remove the Lync Server 2010 Front End pool.

⊟To reset CAC

1. Open Topology Builder.
2. Right-click the site node, and then click **Edit Properties**.
3. Under **Call Admission Control setting**, make sure **Enable Call Admission Control** is selected.
4. Under **Front End pool to run call admission control (CAC)**, select the Lync Server 2013 pool that is to host CAC, and then click **OK**.
5. Publish the topology.

1.6.1.9.5.2 Prevent Sessions for Services

Prevent Sessions for Services

Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools > Remove the Enterprise Edition Front End Server or Standard Edition Front End Server >

Topic Last Modified: *2012-10-04*

You can use Microsoft Lync Server 2010 Control Panel to prevent new sessions for all the Lync Server 2010 services running on a specific computer or to prevent new sessions for a specific Lync Server 2010 service.

⊟To prevent new sessions for all Lync Server services on a computer

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open Lync Server Control Panel.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the services for which you want to prevent new sessions, and then click it.
5. Click **Action**.
6. Click **Prevent new sessions for all services**.

⊟To prevent new sessions for a specific service

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open Lync Server Control Panel.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the service you want to start or stop, and then click it.
5. Click **Properties**.
6. Sort the list of services, if necessary, and click the service for which you want to prevent new sessions.
7. Click **Action**.
8. Click **Prevent new sessions for service**.
9. Click **Close**.

1.6.1.9.5.3 Stop Lync Server 2010 Services

Stop Lync Server 2010 Services

Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools > Remove the Enterprise Edition Front End Server or Standard Edition Front End Server >

Topic Last Modified: *2012-10-04*

You can use Lync Server Control Panel to start or stop all the Lync Server 2010 services running on a specific computer or to start or stop a specific Lync Server 2010 service.

⊟To start or stop all Lync Server services on a computer

1. Open Lync Server Control Panel.
2. In the left navigation bar, click **Topology** and then click **Status**.
3. On the **Status** page, sort or search through the list as needed to find the computer that is running the services you want to start or stop, and then click it.
4. Click **Action**.
5. Click **Start All services** or **Stop All services**.

⊟To start or stop a specific service

1. Open Lync Server Control Panel.
2. In the left navigation bar, click **Topology** and then click **Status**.
3. On the **Status** page, sort or search through the list as needed to find the computer that is running the service you want to start or stop, and then click it.
4. Click **Properties**.
5. Sort the list of services, if necessary, and click the service you want to start or stop.
6. Click **Action**.
7. Click **Start service** or **Stop service**.
8. Click **Close**.

1.6.1.9.5.4 Remove a Front End Server from a Pool

Remove a Front End Server from a Pool

Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools > Remove the Enterprise Edition Front End Server or Standard Edition Front End Server >

Topic Last Modified: *2012-10-04*

The Microsoft Lync Server 2010 Enterprise Edition Front End Server cannot exist as a stand-alone computer. It must be defined as a Front End pool, even if there is only a single computer in the pool.

This topic guides you through the process of removing an individual Front End Server from an existing Front End pool. If the Front End Server is the last server in the pool or if you are removing the pool completely, see Remove Front End Pool or Standard Edition Server. There is no need to remove the individual Front End Servers before you remove the Front End pool. When you remove the pool, you remove each Front End Server.

⊟To remove a Front End Server from a pool

1. Open the Lync Server 2013 Front End Server, open Topology Builder.
2. Navigate to the Lync Server 2010 node.

3. Expand **Enterprise Edition Front End pools**, expand the Front End pool with the Front End Server that you want to remove, right-click the Front End Server that you want to remove, and then click **Delete**.

1.6.1.9.5.5 Remove Front End Pool or Standard Edition Server

Remove Front End Pool or Standard Edition Server

Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools > Remove the Enterprise Edition Front End Server or Standard Edition Front End Server >

Topic Last Modified: *2012-10-04*

This topic guides you through the process of removing a Front End pool or a Standard Edition Front End Server. When you remove a Front End pool, you remove each Front End Server that belongs to the pool as a part of the pool removal process. When you remove a Standard Edition Front End Server, you must remove the SQL Store definition from Topology Builder.

⊟To remove a Front End Server pool

1. Open Topology Builder.
2. Navigate to the Lync Server 2010 node.
3. Expand **Enterprise Edition Front End pools**, expand the Front End pool, right-click the Front End pool that you want to remove, and then click **Delete**.
4. Publish the topology, check replication status, and then run the Lync Server Deployment Wizard as needed.

⊟To remove a Standard Edition Front End server

1. Open Topology Builder.
2. Navigate to the Lync Server 2010 node.
3. Expand **Standard Edition Front End servers**, right-click the Front End Server that you want to remove, and then click **Delete**.
4. Expand **SQL stores**, right-click the SQL Server database that is associated with the Standard Edition Front End Server, and then click **Delete**.

Important:
You must remove the definition of the collocated SQL Server databases from the Standard Edition Front End Server.

5. Publish the topology, check replication status, and then run the Lync Server Deployment Wizard as needed.

1.6.1.9.6 Remove SQL Server Instances and Databases on the Back End Server

Remove SQL Server Instances and Databases on the Back End Server

Migration > Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools >

Topic Last Modified: *2012-10-19*

You remove the Microsoft SQL Server databases and instances after you remove the servers running Lync Server 2010 that are dependent on them, or after you reconfigure the servers running Lync Server 2010 to use another database. You need to perform the procedure in this topic when you retire the current SQL Server or reconfigure the current server running Lync Server 2010 in such a way that it renders the databases obsolete or unavailable.

To remove the databases or instances for the Archiving Server or Monitoring Server, you must first remove the server role. Similarly, to remove the instances or databases for Front End pool, you must first remove or reconfigure the dependent server role. These procedures make no distinction between collocated databases or separate instances for servers. The procedures are unaffected by the collocation of databases.

- Remove the SQL Server Database for a Front End Pool
- Remove the SQL Server Database for a Monitoring Server
- Remove the SQL Server Database for an Archiving Server

1.6.1.9.6.1 Remove the SQL Server Database for a Front End Pool

Remove the SQL Server Database for a Front End Pool

Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools > Remove SQL Server Instances and Databases on the Back End Server >

Topic Last Modified: *2012-10-04*

After you remove a Microsoft Lync Server 2010 Front End pool or reconfigure the pool to use a different database, you can remove the SQL Server databases that hosted the pool data. Use the following procedures to remove the definitions from Topology Builder, and then remove the database and log files from the database server.

To remove the SQL Server database using Topology Builder

1. From the Lync Server 2013 Front End Server, open Topology Builder and download the existing topology.
2. In Topology Builder, navigate to **Shared Components** and then **SQL Server Stores**, right-click the SQL Server instance associated with the removed or reconfigured Front End pool, and then click **Delete**.
3. Publish the topology, and then check the replication status.

To remove user and application databases from the SQL Server

1. To remove the databases on the SQL Server, you must be a member of the SQL Server sysadmins group for the SQL Server where you are removing the database files.
2. Open Lync Server Management Shell
3. To remove the database for the pool user store, type:

   ```
   Uninstall-CsDataBase -DatabaseType User -SqlServerFqdn <FQDN> [-SqlIns
   ```

   Where *<FQDN>* is the fully qualified domain name (FQDN) of the database server, and *<instance>* is the named database instance (that is, if one was defined).
4. To remove the database for the pool application store, type:

   ```
   Uninstall-CsDataBase -DatabaseType Application -SqlServerFqdn <FQDN> [
   ```

   Where *<FQDN>* is the FQDN of the database server, and *<instance>* is the named database instance (that is, if one was defined).
5. When the **Uninstall-CsDataBase** cmdlet prompts you to confirm actions, read the information, and then press **Y** (or press Enter) to proceed, or press **N** and then Enter if you want to stop the cmdlet (that is, in case there errors).

1.6.1.9.6.2 Remove the SQL Server Database for a Monitoring Server

Remove the SQL Server Database for a Monitoring Server

Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools > Remove SQL Server Instances and Databases on the Back End Server >

Topic Last Modified: *2012-10-04*

After you remove a Microsoft Lync Server 2010 Monitoring Server, you can remove the SQL Server databases that hosted the server data. Use the following procedures to remove the definitions from Topology Builder, and then remove the database and log files from the database server.

To remove the SQL Server database using Topology Builder

1. On the Lync Server 2013 Front End Server, open Topology Builder.
2. In Topology Builder, navigate to **Shared Components** and then **SQL Server Stores**, right-click the SQL Server instance associated with the removed or reconfigured Monitoring Server, and then click **Delete**.
3. Publish the topology, and then check replication status.

To remove the database files from the SQL Server

1. To remove the databases on the SQL Server-based server, you must be a member of the SQL Server sysadmins group for the SQL Server server where you are removing the database files.
2. Open the Lync Server Management Shell.
3. At the command line, type the following:

   ```
   Uninstall-CsDataBase -DatabaseType Monitoring -SqlServerFqdn <FQDN> [-
   ```

   Where *<FQDN>* is the fully qualified domain name (FQDN) of the database server, and *<instance>* is the optional named database instance.
4. When the **Uninstall-CsDataBase** cmdlet prompts you to confirm actions, read the information, and then press **Y** (or press Enter) to proceed, or press **N** and then Enter if you want to stop the cmdlet (that is, in case there errors).

1.6.1.9.6.3 Remove the SQL Server Database for an Archiving Server

Remove the SQL Server Database for an Archiving Server

Migration from Lync Server 2010 to Lync Server 2013 > Phase 8: Decommission Legacy Pools > Remove SQL Server Instances and Databases on the Back End Server >

Topic Last Modified: *2012-10-04*

After you remove a Microsoft Lync Server 2010 Archiving Server, you can remove the SQL Server databases that hosted the pool data. Use the following procedures to remove the definitions from Topology Builder, and then remove the database and log files from the database server.

To remove the SQL Server database using Topology Builder

1. On the Lync Server 2013 Front End Server, open Topology Builder.
2. In Topology Builder, navigate to **Shared Components** and then **SQL Server Stores**, right-click the SQL Server instance associated with the removed or reconfigured Archiving Server, and then click **Delete**.

3. Publish the topology, and then check replication status.

To remove the database files from the SQL Server

1. To remove the databases on the SQL Server, you must be a member of the SQL Server sysadmins group for the SQL Server where you are removing the database files.
2. Open the Lync Server Management Shell.
3. At the command line, type the following:

   ```
   Uninstall-CsDataBase -DatabaseType Archiving -SqlServerFqdn <FQDN> [-S
   ```

   Where *<FQDN>* is the fully qualified domain name (FQDN) of the database server, and *<instance>* is the named database instance (that is, if one was defined).
4. When the **Uninstall-CsDataBase** cmdlet prompts you to confirm actions, read the information, and then press **Y** (or press Enter) to proceed, or press **N** and then Enter if you want to stop the cmdlet (that is, in case there errors).

1.6.2 Migration from Office Communications Server 2007 R2 to Lync Server 2013

Migration from Office Communications Server 2007 R2 to Lync Server 2013

Microsoft Lync Server 2013 > Migration >

Topic Last Modified: *2012-10-19*

The topics in this section guide you through the process of migrating from Office Communications Server 2007 R2 to Lync Server 2013

Important:

This document describes the steps generally required to accomplish each phase of migration. It does not address every possible legacy deployment topology or every possible migration scenario. Therefore, you may not need to perform every step described, or you may need to perform additional steps, depending on your deployment. This document also provides examples of verification steps. These verification steps are provided to help you understand what you need to look for to ensure that each phase completes successfully as you progress through your migration. Tailor these verification steps to your specific migration process.

This guide provides information specific to upgrading your existing deployment. It does not explain how to change your existing topology. This guide does not cover the implementation of new features. When a detailed procedure is documented elsewhere, this guide directs you to the appropriate document or document section.

This document defines terms as specified in the following list.

migration

Moving your production deployment from a previous version of Office Communications Server 2007 R2 to Lync Server 2013.

upgrade

Installing a newer version of software on a server or client computer.

coexistence

The temporary environment that exists during migration when some functionality has been migrated to Lync Server 2013 and other functionality still remains on a prior version of Office Communications Server 2007 R2.

interoperability

The ability of your deployment to operate successfully during the period of coexistence.

In This Section

- Before You Begin the Migration
- Migration Phases
- Phase 1: Plan Your Migration from Office Communications Server 2007 R2
- Phase 2: Prepare for Migration
- Phase 3: Deploy Lync Server 2013 Pilot Pool
- Phase 4: Merge Topologies
- Phase 5: Configure the Pilot Pool
- Phase 6: Move users to the Pilot Pool
- Phase 7: Add Lync Server 2013 Edge Server to Pilot Pool
- Phase 8: Move from Pilot Deployment into Production
- Phase 9: Complete Post-Migration Tasks
- Phase 10: Decommission Legacy Site

1.6.2.1 Before You Begin the Migration

Before You Begin the Migration

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-08-29*

Before you begin, we recommend that you read this document and the following guides to familiarize yourself with deploying the corresponding Lync Server 2013 roles:

- Deploying Lync Server 2013
- Deploying External User Access
- Deploying Clients and Devices
- Migration Process
- Migration Phases

1.6.2.1.1 Migration Process

Migration Process

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Before You Begin the Migration >

Topic Last Modified: *2012-09-24*

The recommended and supported migration procedure for Lync Server 2013 is the side-by-side migration procedure. This topic describes why you should use side-by-side migration and also includes information about coexistence.

Side-by-Side Migration

In nearly every migration, you should use the side-by-side migration path. In a side-by-side migration, you deploy a new server with Lync Server 2013 alongside a corresponding server that is running Office Communications Server 2007 R2, and then you transfer operations to the new server. If it becomes necessary to roll back to Office Communications Server 2007 R2, you have only to shift operations back to the original servers. Be aware that in this situation any new meetings scheduled with upgraded clients will not work, and the clients would also need to be downgraded.

Coexistence Testing

After you have deployed Lync Server 2013 in parallel with Office Communications Server 2007 R2, the topology represents a coexistence testing state of Lync Server 2013 and Office Communications Server 2007 R2. While in this state, it is important to test and ensure services are started, each site can be administered, and clients can communicate with current and legacy users. Prior to the migration of all users, it is very important that you understand the state of each deployment and ensure that each deployment is functional and working properly. Typically, the coexistence testing phase exists throughout the pilot testing of Lync Server 2013. Legacy users are moved to Lync Server 2013 for a period of time to ensure that application compatibility and features and functions are working properly. After pilot testing, users and applications are moved to the production version of Lync Server 2013, and the legacy pools and applications of Office Communications Server 2007 R2 are retired.

1.6.2.1.2 Migration Phases

Migration Phases

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Before You Begin the Migration >

Topic Last Modified: *2012-08-29*

The following phases describe the process of a pool migration from Office Communications Server 2007 R2 to Lync Server 2013.

- Phase 1: Plan Your Migration from Office Communications Server 2007 R2
- Phase 2: Prepare for Migration
- Phase 3: Deploy Lync Server 2013 Pilot Pool
- Phase 4: Merge Topologies
- Phase 5: Configure the Pilot Pool
- Phase 6: Move users to the Pilot Pool
- Phase 7: Add Lync Server 2013 Edge Server to Pilot Pool
- Phase 8: Move from Pilot Deployment into Production
- Phase 9: Complete Post-Migration Tasks
- Phase 10: Decommission Legacy Site

1.6.2.2 Phase 1: Plan Your Migration from Office Communications Server 2007 R2

Phase 1: Plan Your Migration from Office Communications Server 2007 R2

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-09-29*

This section covers planning topics for migrating from Office Communications Server 2007 R2 to Lync Server 2013.

In This Section

- User Migration

- Migrating Archiving and Monitoring Servers
- Administering Servers after Migration
- Migrating Multiple Sites and Pools
- Migrating XMPP Federation

1.6.2.2.1 User Migration

User Migration

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 1: Plan Your Migration from Office Communications Server 2007 R2 >

Topic Last Modified: *2012-10-19*

A generally accepted best practice for migrations is to create several test users and use them to conduct systems tests. After you have successfully moved and tested those accounts, you should identify a group of pilot production users and move their accounts and conduct validation tests on them. When you get satisfactory results, you can move the rest of your users to the new deployment.

1.6.2.2.2 Migrating Archiving and Monitoring Servers

Migrating Archiving and Monitoring Servers

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 1: Plan Your Migration from Office Communications Server 2007 R2 >

Topic Last Modified: *2012-10-02*

If you deployed Archiving Server and Monitoring Server in your Office Communications Server 2007 R2, you can deploy these servers in your Lync Server 2013 environment after you migrate your Front End pools. If archiving and monitoring functionality are critical to your organization, however, you should add archiving and monitoring to your pilot pool before you migrate so that the functionality is available during the migration process.

If you want archiving and monitoring functionality during the migration and coexistence phase, keep the following considerations in mind:

- Archiving data and monitoring data are not moved to the Lync Server 2013 deployment. The data you back up prior to decommissioning the legacy environment will be your history of activity in the Office Communications Server 2007 R2.
- The Office Communications Server 2007 R2 version of Archiving Server and Monitoring Server can be associated only with a Office Communications Server 2007 R2 Front End pool. In Lync Server 2013, Archiving and Monitoring are no longer server roles, but services integrated into the Lync Server 2013 Front End pool.
- During the time that your legacy and Lync Server 2013 deployments coexist, the Office Communications Server 2007 R2 version of Archiving Server and Monitoring Server gather data for users homed on Office Communications Server 2007 R2 pools. The Lync Server 2013 version of Archiving Server and Monitoring Server gather data for users homed on Lync Server 2013 pools.

> **Note:**
> During the phase of migration when you are still using your legacy Edge server with the new Lync Server 2013 pilot pool, the Office Communications Server 2007 R2 version of Archiving Server continues to gather data for users

homed on Office Communications Server 2007 R2 pools and the Lync Server 2013 version of Archiving Server gathers data for users homed on Lync Server 2013 pools.

- If you use a third-party archiving and monitoring solution in conjunction with Archiving Server and Monitoring Server, talk to your vendor about when and how you need to integrate the third-party solution with Lync Server 2013.

1.6.2.2.3 Administering Servers after Migration

Administering Servers after Migration

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 1: Plan Your Migration from Office Communications Server 2007 R2 >

Topic Last Modified: *2012-09-29*

In general, you must use the administrative tool that corresponds to the server version that you want to manage. You cannot install the Lync Server 2013 and Office Communications Server 2007 R2 administrative tools on the same computer. Also, the Lync Server 2013 Control Panel is not installed automatically on each server. To install the Lync Server 2013 Control Panel, follow the procedure inside the topic Install Lync Server Administrative Tools in the Deployment documentation.

1.6.2.2.4 Migrating Multiple Sites and Pools

Migrating Multiple Sites and Pools

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 1: Plan Your Migration from Office Communications Server 2007 R2 >

Topic Last Modified: *2012-08-26*

Lync Server 2013 supports multi-site and multi-pool deployments. The process of migrating multiple pools from Office Communications Server 2007 R2 to Lync Server 2013 requires the following considerations:

1. After deploying a Lync Server 2013 pilot pool, you need to define a subset of pilot users that will be moved to the Lync Server 2013 pool, and a methodology for validating the functionality of the users.
2. After deploying an Edge Server in the pilot pool, you need to validate that external users can communicate with the Lync Server 2013 pool.
3. After transitioning the federated routes from Office Communications Server 2007 R2 Edge Servers to the pilot Lync Server 2013 Edge Servers, you need to validate that federated users can communicate with the Lync Server 2013 pool.
4. After moving all the users and non-user contact objects, you need to validate that the Office Communications Server 2007 R2 pool is empty.
5. After verifying that the Office Communications Server 2007 R2 pool is empty, you can then deactivate the pool.
   For details about how to deactivate the legacy Office Communications Server 2007 R2 pool and servers, see Phase 10: Decommission Legacy Site.

1.6.2.2.5 Migrating XMPP Federation

Migrating XMPP Federation

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 1: Plan Your Migration from Office Communications Server 2007 R2 >

Topic Last Modified: *2012-10-16*

Previous versions of Office Communications Server provided an extensible messaging and presence protocol (XMPP) gateway that could be deployed as a separate server role to allow federating with XMPP deployments. In Lync Server 2013, the XMPP functionality can be deployed as a feature. XMPP functionality is installed in two parts: as an XMPP proxy that runs on the Lync Server 2013 Edge Server, and the XMPP Gateway that runs on the Lync Server 2013 Front End Server.

From a migration perspective, a Office Communications Server 2007 R2 user account can be moved to a Lync Server 2013 pool and continue to use the Office Communications Server 2007 R2 XMPP gateway. This is possible only when the XMPP federated partner is not configured in Lync Server 2013.

In summary, if Office Communications Server has been deployed with the Office Communications Server 2007 R2 XMPP Gateway and XMPP federation has been enabled for legacy Office Communications Server 2007 R2 users, to migrate the XMPP federation to Lync Server 2013:

1. Deploy a Lync Server 2013 pool.
2. Deploy a Lync Server 2013 Edge server.
3. Move all users to the Lync Server 2013 pool.
4. Create XMPP access policies and certificates for the Edge Server.
5. Enable XMPP federation in Lync Server 2013.
6. Update the DNS entries to point to the Lync Server 2013 XMPP Gateway.

1.6.2.3 Phase 2: Prepare for Migration

Phase 2: Prepare for Migration

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-08-24*

Before you begin to migrate to Lync Server 2013 from Office Communications Server 2007 R2, follow the steps described in this section.

In This Section

- Apply Office Communications Server 2007 R2 Updates
- Configure DNS Records for Pilot Pool Deployment
- Run Best Practices Analyzer
- Back Up Systems and Data
- Configure Clients for Migration
- Verify Office Communications Server 2007 R2 Environment

1.6.2.3.1 Apply Office Communications Server 2007 R2 Updates

Apply Office Communications Server 2007 R2 Updates

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase

2: Prepare for Migration >

Topic Last Modified: *2012-10-19*

Before you migrate to Lync Server 2013, updates must be applied to your Office Communications Server 2007 R2 environment. For the most up-to-date information about Office Communications Server 2007 R2, see **Updates for Communications Server 2007 R2** at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=968802.

To install updates for Office Communications Server 2007 R2, we recommend you follow the **Method 1 Cumulative Server Update Installer** procedure described in Microsoft Knowledge Base article 968802, "Updates for Communications Server 2007 R2," at http://go.microsoft.com/fwlink/p/?linkid=3052&kbid=968802.

1.6.2.3.2 Configure DNS Records for Pilot Pool Deployment

Configure DNS Records for Pilot Pool Deployment

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-09-24*

Prior to deploying the Lync Server 2013 pilot pool, you must update the DNS Host A entries for the pilot pool. To successfully complete this procedure, you should be logged on to the server or domain at minimum as a member of the Domain Admins group or a member of the DnsAdmins group.

To configure DNS Host A records

1. On the Domain Name System (DNS) server, click **Start**, click **Administrative Tools**, and then click **DNS**.
2. In the console tree for your domain, expand **Forward Lookup Zones**, and then right-click the domain in which Lync Server 2013 will be installed.
3. Click **New Host (A or AAAA)**.
4. Click **Name**, type the host name for the pool (the domain name is assumed from the zone that the record is defined in and does not need to be entered as part of the A record).
5. Click **IP Address**, type the IP address for the Front End pool.
6. Click **Add Host**, and then click **OK**.
7. When you are finished, click **Done**.

1.6.2.3.3 Run Best Practices Analyzer

Run Best Practices Analyzer

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-10-11*

The Office Communications Server 2007 R2 Best Practices Analyzer tool gathers configuration information from an Office Communications Server 2007 R2 deployment and determines whether the configuration is set according to Microsoft best practices. You can install the tool on a client computer that runs Microsoft .NET Framework 2.0, or directly on the server that runs Office Communications Server 2007 R2. We recommend that you install and run this tool on a client computer. The Office Communications Server 2007 R2 Administrative Tools should also be installed locally on the client computer so that the Best Practices Analyzer can collect a full set of data.

You can download the Office Communications Server 2007 R2 Best Practices Analyzer from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?LinkId=268702.

1.6.2.3.4 Back Up Systems and Data

Back Up Systems and Data

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-10-19*

Before you begin the migration to Lync Server 2013, we strongly recommend that you perform a full system backup and document your existing system, including an inventory of user accounts that are homed on each pool, so that you can roll back to Office Communications Server 2007 R2 if it becomes necessary. Multiple tools and programs are available for backing up and restoring data, settings, and systems. For details and procedures, see "Office Communications Server 2007 R2 Backup and Restoration Guide" at http://go.microsoft.com/fwlink/p/?linkid=168162.

1.6.2.3.5 Configure Clients for Migration

Configure Clients for Migration

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-10-02*

This topic contains the recommended client deployment steps you should take prior to migrating to Lync Server 2013. These configuration changes should be made on Office Communications Server 2007 R2. It is very important that you perform these steps prior to migrating. For details, see Planning for Clients and Devices in Lync Server 2013.

⊟To configure clients prior to migration

1. Deploy the most recent server, client, and device updates (hotfixes) for Office Communications Server 2007 R2 as listed in Apply Office Communications Server 2007 R2 Updates.
2. On Office Communications Server 2007 R2, use Client Version Filtering to allow only Office Communications Server 2007 R2 clients with the most current updates installed to sign in.
3. On Office Communications Server 2007 R2, use Client Version Filtering to block Lync Server 2013 clients from signing in. Follow the steps described in **Configuring Client Version Filtering** at http://go.microsoft.com/fwlink/p/?linkId=202488 to add the version filters listed in the following table. For each version filter, assign the action **Block**.

Client	User agent header	Version
Lync 2013	OC	15.*.*.*
Lync Web App	CWA	5.*.*.*
Lync Phone Edition	OCPhone	4.*.*.*

Verify Office Communications Server 2007 R2 Environment

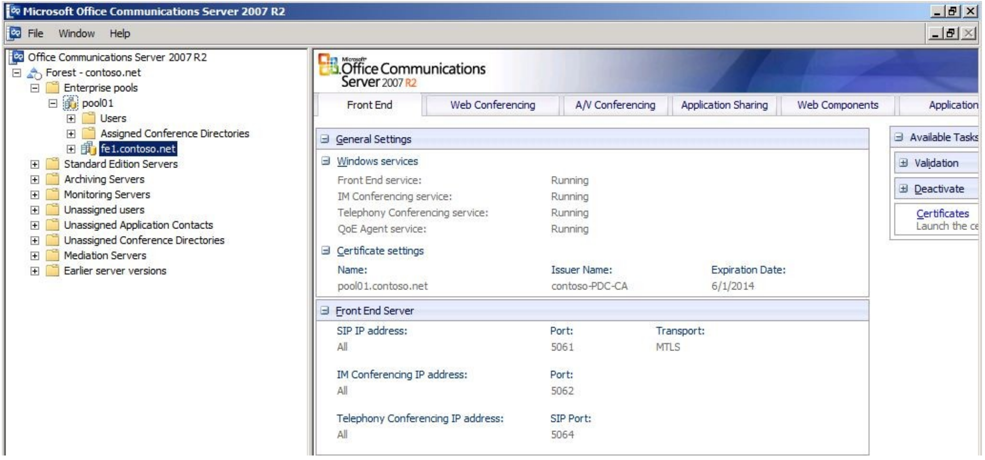
Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 2: Prepare for Migration >

Topic Last Modified: *2012-10-16*

Prior to deploying Lync Server 2013 in a coexistence state with Office Communications Server 2007 R2, you need to verify the Office Communications Server 2007 R2 services are configured and started.

Verify the Pool is started using the Office Communications Server 2007 R2 Administrative Tool

1. Open the Office Communications Server 2007 R2 administrative tool.
2. Expand the **Forest** node, expand the **Standard Edition Servers** or **Enterprise pools** node, and then expand the pool or server name.
3. Ensure that the services are running on the Standard Edition server or Enterprise pool.



General Settings

Windows services

Front End service: Running
IM Conferencing service: Running
Telephony Conferencing service: Running
QoE Agent service: Running

Certificate settings

Name:	Issuer Name:	Expiration Date:
pool01.contoso.net	contoso-PDC-CA	6/1/2014

Front End Server

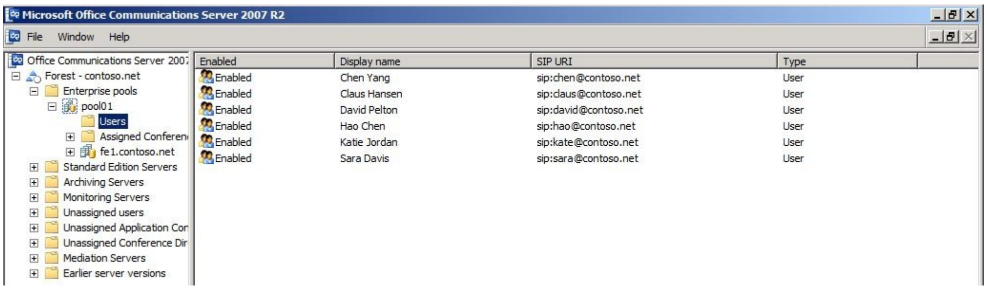
SIP IP address:	Port:	Transport:
All	5061	MTLS

IM Conferencing IP address: All — Port: 5062

Telephony Conferencing IP address: All — SIP Port: 5064

Review Users configured for Office Communications Server 2007 R2

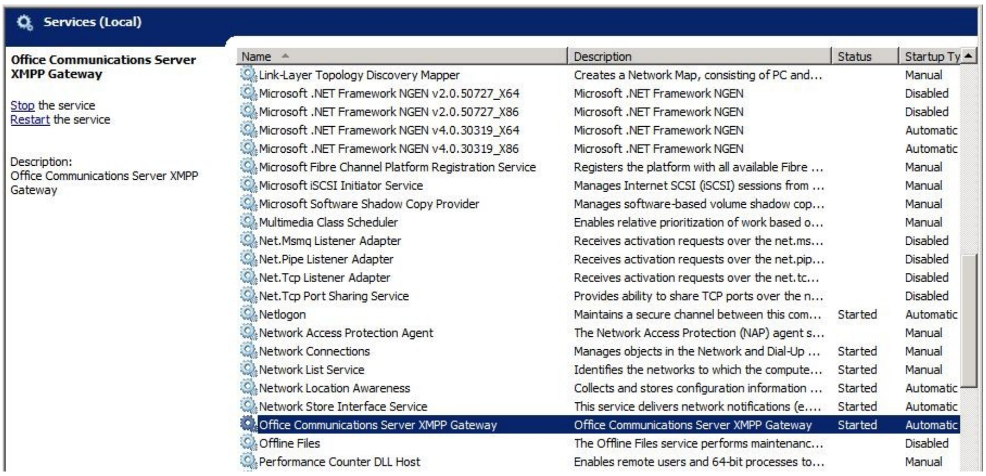
1. Open the Office Communications Server 2007 R2 administrative tool.
2. Expand the **Forest** node, expand the **Standard Edition Servers** or **Enterprise pools** node, and then expand the pool or server name.
3. Click **Users**.
4. Verify the list of Office Communications Server 2007 R2 users.



Enabled	Display name	SIP URI	Type
Enabled	Chen Yang	sip:chen@contoso.net	User
Enabled	Claus Hansen	sip:claus@contoso.net	User
Enabled	David Pelton	sip:david@contoso.net	User
Enabled	Hao Chen	sip:hao@contoso.net	User
Enabled	Katie Jordan	sip:kate@contoso.net	User
Enabled	Sara Davis	sip:sara@contoso.net	User

Verify legacy XMPP Federated Partner Configuration

1. From the legacy XMPP server, navigate to the Administrative Tools\Services applet.
2. Verify that the Office Communications Server XMPP Gateway service is started.



Services (Local)

Office Communications Server XMPP Gateway

Stop the service
Restart the service

Description:
Office Communications Server XMPP Gateway

Name	Description	Status	Startup Ty
Link-Layer Topology Discovery Mapper	Creates a Network Map, consisting of PC and...		Manual
Microsoft .NET Framework NGEN v2.0.50727_X64	Microsoft .NET Framework NGEN		Disabled
Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft .NET Framework NGEN		Disabled
Microsoft .NET Framework NGEN v4.0.30319_X64	Microsoft .NET Framework NGEN		Automatic
Microsoft .NET Framework NGEN v4.0.30319_X86	Microsoft .NET Framework NGEN		Automatic
Microsoft Fibre Channel Platform Registration Service	Registers the platform with all available Fibre ...		Manual
Microsoft iSCSI Initiator Service	Manages Internet SCSI (iSCSI) sessions from ...		Manual
Microsoft Software Shadow Copy Provider	Manages software-based volume shadow cop...		Manual
Multimedia Class Scheduler	Enables relative prioritization of work based o...		Manual
Net.Msmq Listener Adapter	Receives activation requests over the net.ms...		Disabled
Net.Pipe Listener Adapter	Receives activation requests over the net.pip...		Disabled
Net.Tcp Listener Adapter	Receives activation requests over the net.tc...		Disabled
Net.Tcp Port Sharing Service	Provides ability to share TCP ports over the n...		Disabled
Netlogon	Maintains a secure channel between this com...	Started	Automatic
Network Access Protection Agent	The Network Access Protection (NAP) agent s...		Manual
Network Connections	Manages objects in the Network and Dial-Up ...	Started	Manual
Network List Service	Identifies the networks to which the compute...	Started	Manual
Network Location Awareness	Collects and stores configuration information ...	Started	Automatic
Network Store Interface Service	This service delivers network notifications (e....	Started	Automatic
Office Communications Server XMPP Gateway	Office Communications Server XMPP Gateway	Started	Automatic
Offline Files	The Offline Files service performs maintenanc...		Disabled
Performance Counter DLL Host	Enables remote users and 64-bit processes to...		Manual

1.6.2.4 Phase 3: Deploy Lync Server 2013 Pilot Pool

Phase 3: Deploy Lync Server 2013 Pilot Pool

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-08-28*

This section describes the steps required to deploy a pilot deployment of Lync Server 2013, and a few key validation steps to ensure the two pools are coexisting.

In This Section

- Prepare Active Directory for Lync Server 2013
- Install Lync Server Administration Tools
- Deploy Lync Server 2013 Pilot Pool
- Verify Pilot Pool Coexistence with Legacy Pool

1.6.2.4.1 Prepare Active Directory for Lync Server 2013

Prepare Active Directory for Lync Server 2013

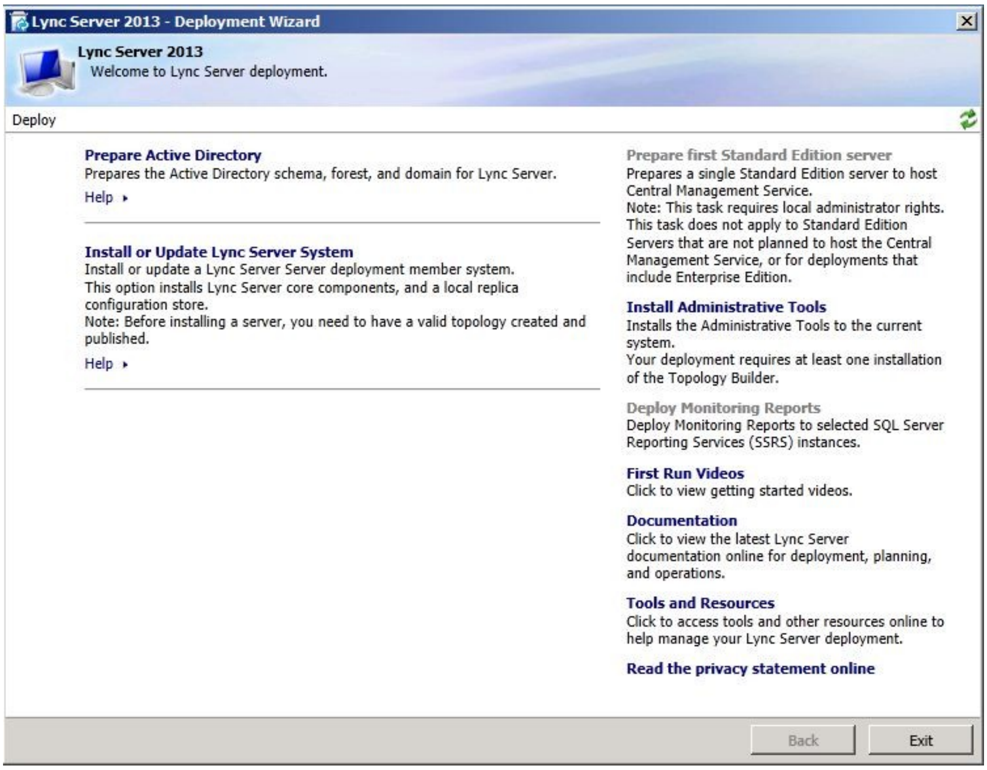
Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

Topic Last Modified: *2012-10-01*

Prior to deploying Lync Server 2013 in a coexistence state with Office Communications Server 2007 R2, you must perform some additional Active Directory tasks to configure the schema, forest, and domain for Lync Server 2013. The schema extensions add the Active Directory classes and attributes that are required by Lync Server. For additional information, see the topic Preparing Active Directory Domain Services for Lync Server 2013.

Prepare Active Directory for Lync Server 2013

1. On the Lync Server 2013 Front End Server, run Lync Server 2013 Setup.
2. Select **Prepare Active Directory**



Lync Server 2013 - Deployment Wizard

Lync Server 2013
Welcome to Lync Server deployment.

Deploy

Prepare Active Directory
Prepares the Active Directory schema, forest, and domain for Lync Server.
Help ▸

Install or Update Lync Server System
Install or update a Lync Server Server deployment member system.
This option installs Lync Server core components, and a local replica configuration store.
Note: Before installing a server, you need to have a valid topology created and published.
Help ▸

Prepare first Standard Edition server
Prepares a single Standard Edition server to host Central Management Service.
Note: This task requires local administrator rights.
This task does not apply to Standard Edition Servers that are not planned to host the Central Management Service, or for deployments that include Enterprise Edition.

Install Administrative Tools
Installs the Administrative Tools to the current system.
Your deployment requires at least one installation of the Topology Builder.

Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

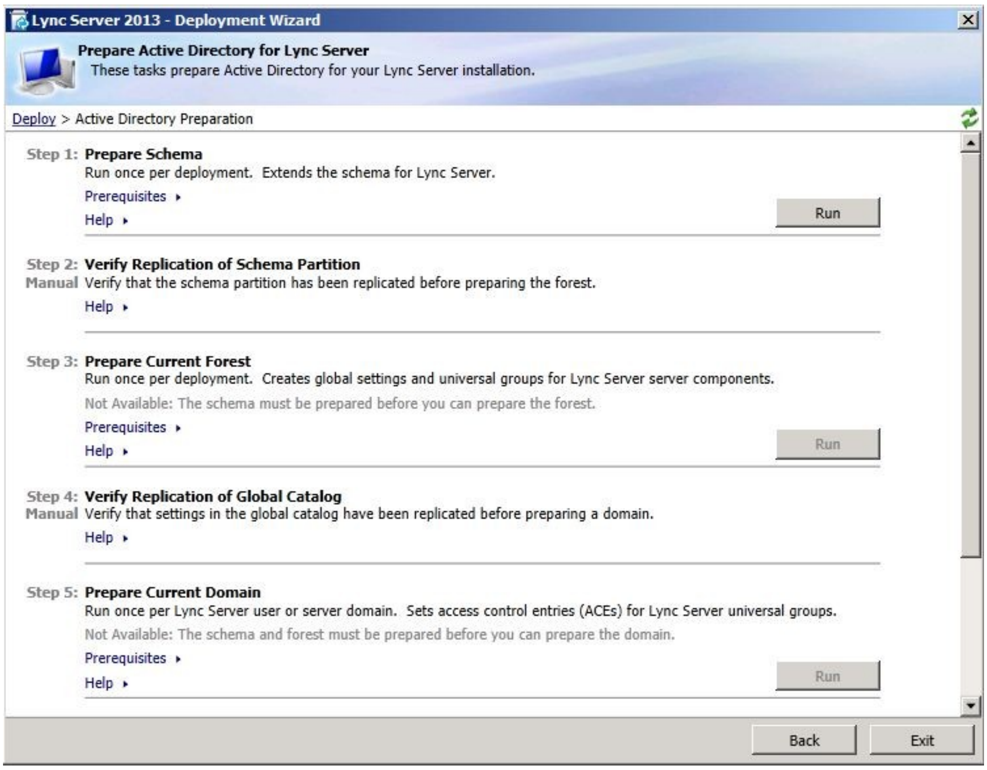
First Run Videos
Click to view getting started videos.

Documentation
Click to view the latest Lync Server documentation online for deployment, planning, and operations.

Tools and Resources
Click to access tools and other resources online to help manage your Lync Server deployment.

Read the privacy statement online

3. Complete steps 1 through 5.



Lync Server 2013 - Deployment Wizard

Prepare Active Directory for Lync Server
These tasks prepare Active Directory for your Lync Server installation.

Deploy > Active Directory Preparation

Step 1: **Prepare Schema**
Run once per deployment. Extends the schema for Lync Server.
Prerequisites ▸
Help ▸

Step 2: **Verify Replication of Schema Partition**
Manual Verify that the schema partition has been replicated before preparing the forest.
Help ▸

Step 3: **Prepare Current Forest**
Run once per deployment. Creates global settings and universal groups for Lync Server server components.
Not Available: The schema must be prepared before you can prepare the forest.
Prerequisites ▸
Help ▸

Step 4: **Verify Replication of Global Catalog**
Manual Verify that settings in the global catalog have been replicated before preparing a domain.
Help ▸

Step 5: **Prepare Current Domain**
Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups.
Not Available: The schema and forest must be prepared before you can prepare the domain.
Prerequisites ▸
Help ▸

1.6.2.4.2 Install Lync Server Administration Tools

Install Lync Server Administration Tools

See Also

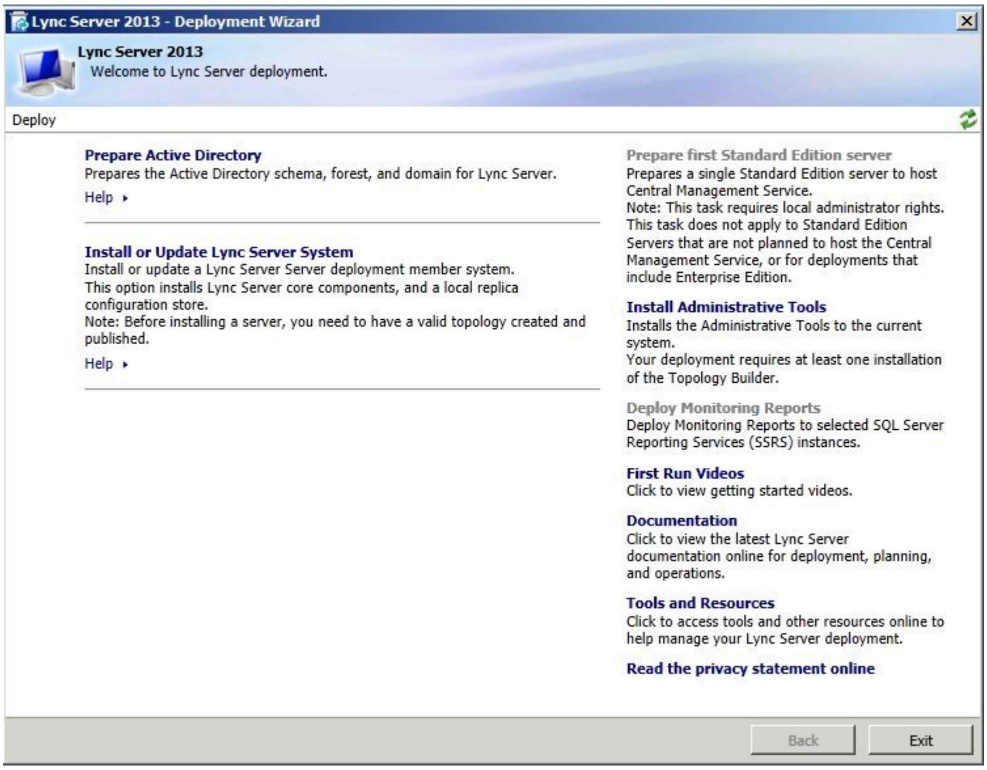
Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

Topic Last Modified: *2012-10-02*

This topic describes how to install the administrative tools you need to use to deploy and manage Lync Server 2013. You can also install the administrative tools on other computers, such as dedicated administrative consoles.

⊟To install the Lync Server 2013 administrative tools

1. On the Lync Server 2013 Front End Server, run Lync Server 2013 Setup.
2. From the Lync Server 2013 Deployment Wizard page, select **Install Administrative Tools**



Lync Server 2013 - Deployment Wizard

Lync Server 2013

Welcome to Lync Server deployment.

Deploy

Prepare Active Directory
Prepares the Active Directory schema, forest, and domain for Lync Server.
Help ▸

Install or Update Lync Server System
Install or update a Lync Server Server deployment member system.
This option installs Lync Server core components, and a local replica configuration store.
Note: Before installing a server, you need to have a valid topology created and published.
Help ▸

Prepare first Standard Edition server
Prepares a single Standard Edition server to host Central Management Service.
Note: This task requires local administrator rights.
This task does not apply to Standard Edition Servers that are not planned to host the Central Management Service, or for deployments that include Enterprise Edition.

Install Administrative Tools
Installs the Administrative Tools to the current system.
Your deployment requires at least one installation of the Topology Builder.

Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

First Run Videos
Click to view getting started videos.

Documentation
Click to view the latest Lync Server documentation online for deployment, planning, and operations.

Tools and Resources
Click to access tools and other resources online to help manage your Lync Server deployment.

Read the privacy statement online

Concepts

Lync Server Administrative Tools

1.6.2.4.3 Deploy Lync Server 2013 Pilot Pool

Deploy Lync Server 2013 Pilot Pool

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

Topic Last Modified: *2012-10-16*

One of the first steps required for migration to Lync Server 2013 is to deploy a pilot pool. The pilot pool is where you test coexistence of Lync Server 2013 with your Office Communications Server 2007 R2 deployment. Coexistence is a temporary state that lasts until you have moved all users and pools to Lync Server 2013.

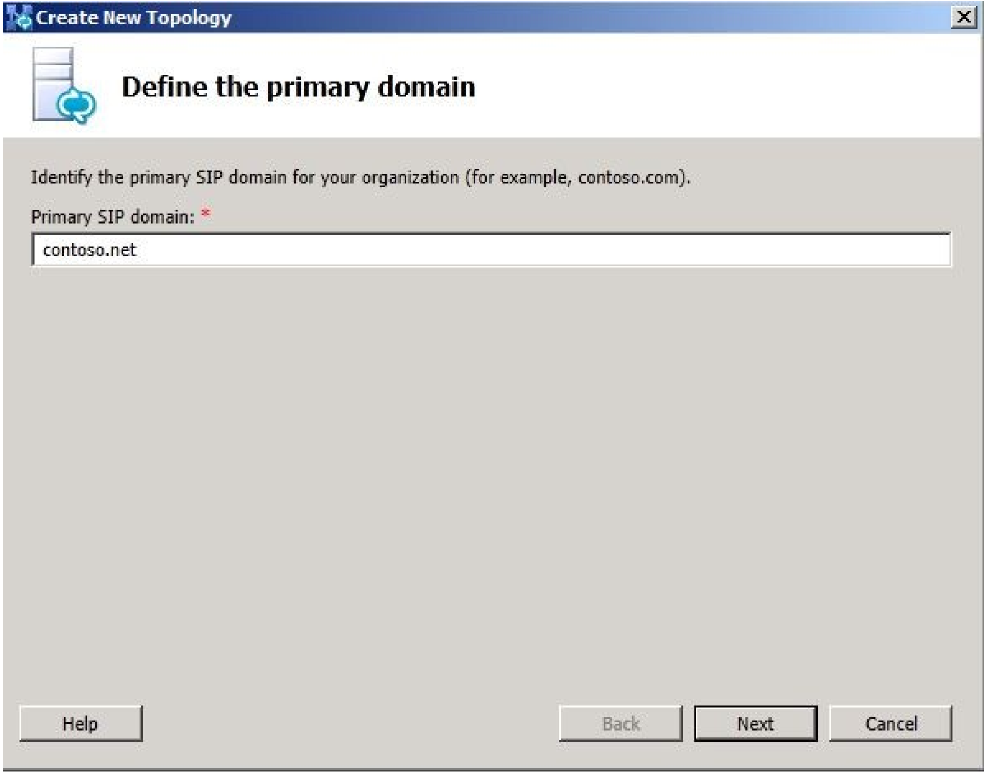
When you deploy a pilot pool, you use the Define New Front End Pool wizard. You should deploy the same features and workloads in your Lync Server 2013 pilot pool that you have in your Office Communications Server 2007 R2 pool. If you deployed Archiving Server, Monitoring Server, or System Center Operations Manager for archiving or monitoring your Office Communications Server 2007 R2 environment, and you want to continue archiving or monitoring throughout the migration, you need to also deploy these features in your pilot environment. The version you deployed to archive or monitor your Office Communications Server 2007 R2 environment will not capture data in your Lync Server 2013 environment.

Note:

The following procedure discusses features and settings you should consider as part of your overall pilot pool deployment process. This section only highlights key points you should consider as part of your pilot pool deployment. For detailed steps, refer to the Deploying Lync Server 2013 deployment guide.

To deploy a Lync Server 2013 pilot pool

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Open Topology Builder and choose to create a new topology.
3. Enter the primary SIP domain.

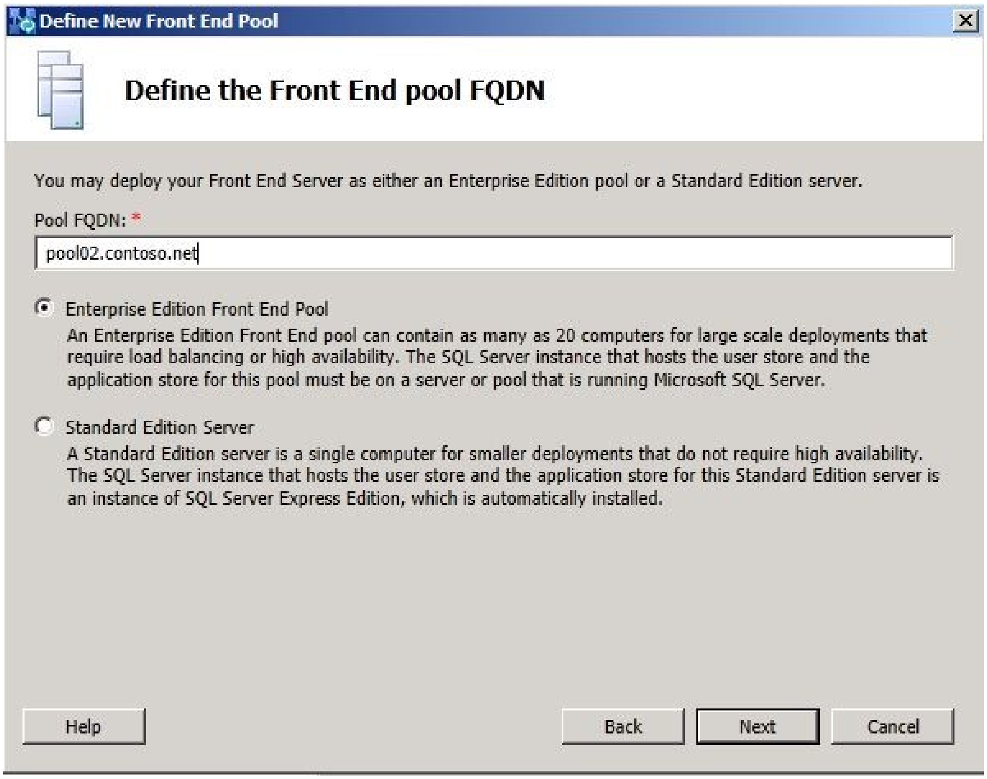


Identify the primary SIP domain for your organization (for example, contoso.com).

Primary SIP domain: * contoso.net

4. Continue completing the wizard until you reach the **Define the New Front End pool** wizard. Click Next.
5. Enter the pool FQDN. When you define your pilot pool, you can choose to deploy an Enterprise Edition Front End pool or a Standard Edition server. Lync Server 2013 does not require that your pilot pool features match what was deployed in your legacy pool.

Warning:
The pool or server fully qualified domain name (FQDN) that you define for the pilot pool must be unique. It cannot match the name of the currently deployed Office Communications Server 2007 R2 pool, or any other servers currently deployed.



Define the Front End pool FQDN

You may deploy your Front End Server as either an Enterprise Edition pool or a Standard Edition server.

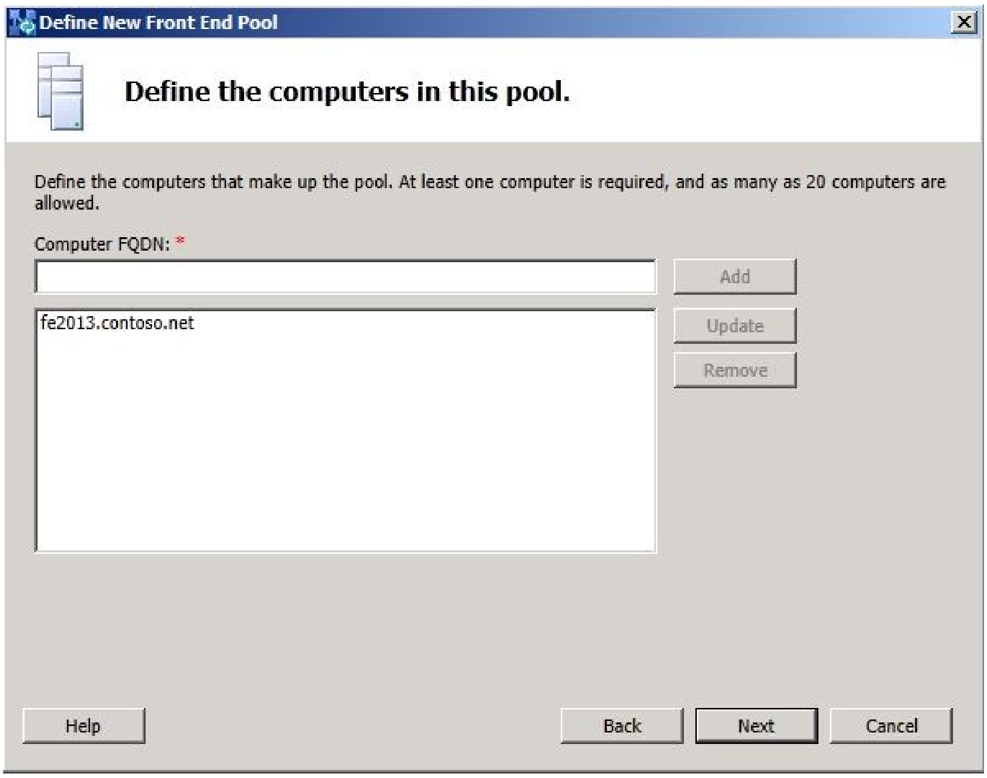
Pool FQDN: *

pool02.contoso.net

● Enterprise Edition Front End Pool
An Enterprise Edition Front End pool can contain as many as 20 computers for large scale deployments that require load balancing or high availability. The SQL Server instance that hosts the user store and the application store for this pool must be on a server or pool that is running Microsoft SQL Server.

○ Standard Edition Server
A Standard Edition server is a single computer for smaller deployments that do not require high availability. The SQL Server instance that hosts the user store and the application store for this Standard Edition server is an instance of SQL Server Express Edition, which is automatically installed.

6. Define the computer that will be added to the pool.



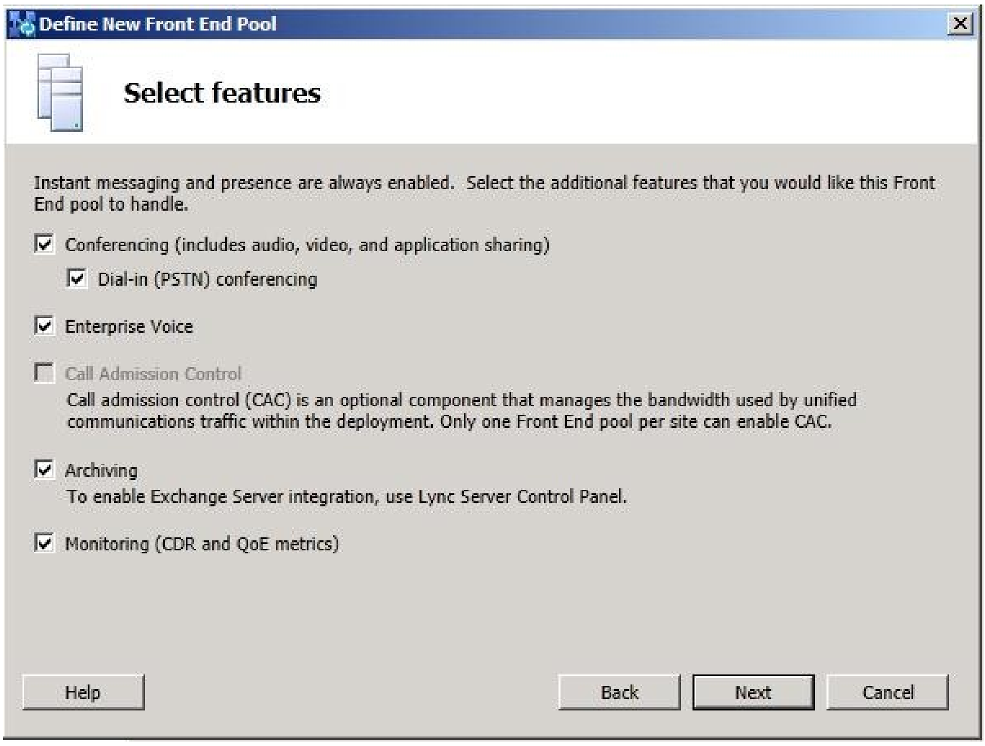
Define the computers in this pool.

Define the computers that make up the pool. At least one computer is required, and as many as 20 computers are allowed.

Computer FQDN: *

fe2013.contoso.net

7. On the **Select features** page, select the check boxes for the features that you want on this Front End pool. For example, if you are deploying only instant messaging (IM) and presence features, you would select the Conferencing check box to allow multiparty IM, but would not select the Dial-in (PSTN) conferencing, Enterprise Voice, or Call Admission Control check boxes, because they represent voice, video, and collaborative conferencing features. For additional information on selecting features, see Define and Configure a Front End Pool or Standard Edition Server in the Deployment documentation.



Define New Front End Pool

Select features

Instant messaging and presence are always enabled. Select the additional features that you would like this Front End pool to handle.

☑ Conferencing (includes audio, video, and application sharing)

☑ Dial-in (PSTN) conferencing

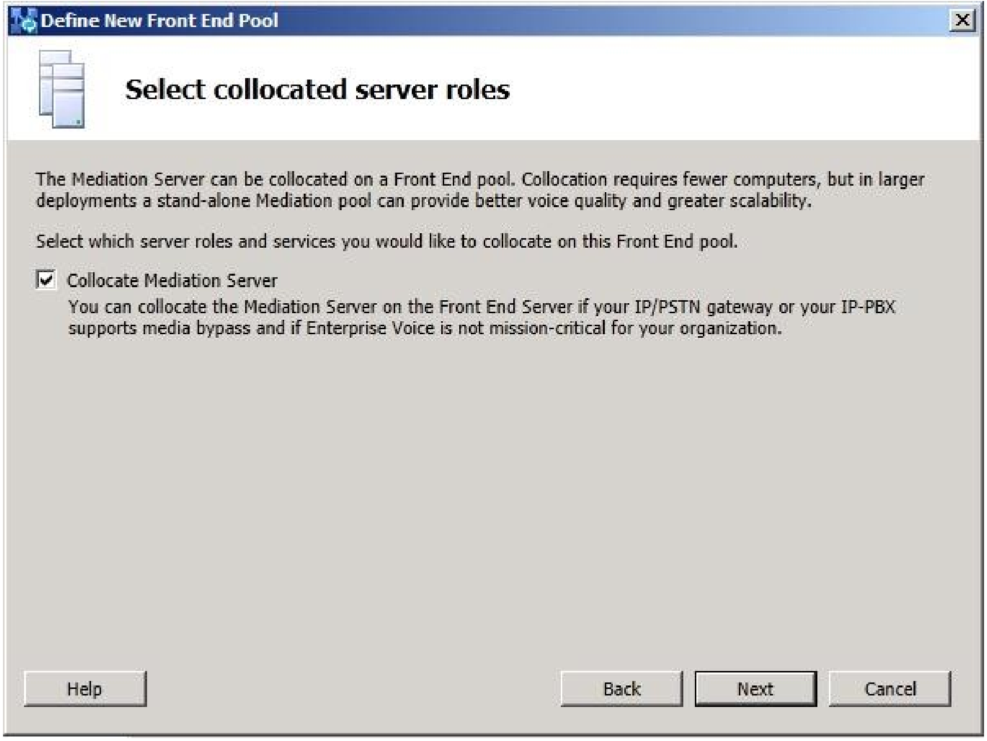
☑ Enterprise Voice

□ Call Admission Control
Call admission control (CAC) is an optional component that manages the bandwidth used by unified communications traffic within the deployment. Only one Front End pool per site can enable CAC.

☑ Archiving
To enable Exchange Server integration, use Lync Server Control Panel.

☑ Monitoring (CDR and QoE metrics)

8. On the **Select collocated server roles** page, we recommend you collocate the Mediation Server in Lync Server 2013. When merging a legacy topology with Lync Server 2013, we require that you first collocate the Office Communications Server 2007 R2 Mediation Server. After merging the topologies and configuring the Lync Server 2013 Mediation Server, you can decide to keep the collocated Mediation Server or change it to a stand-alone server in your Lync Server 2013 deployment.



Define New Front End Pool

Select collocated server roles

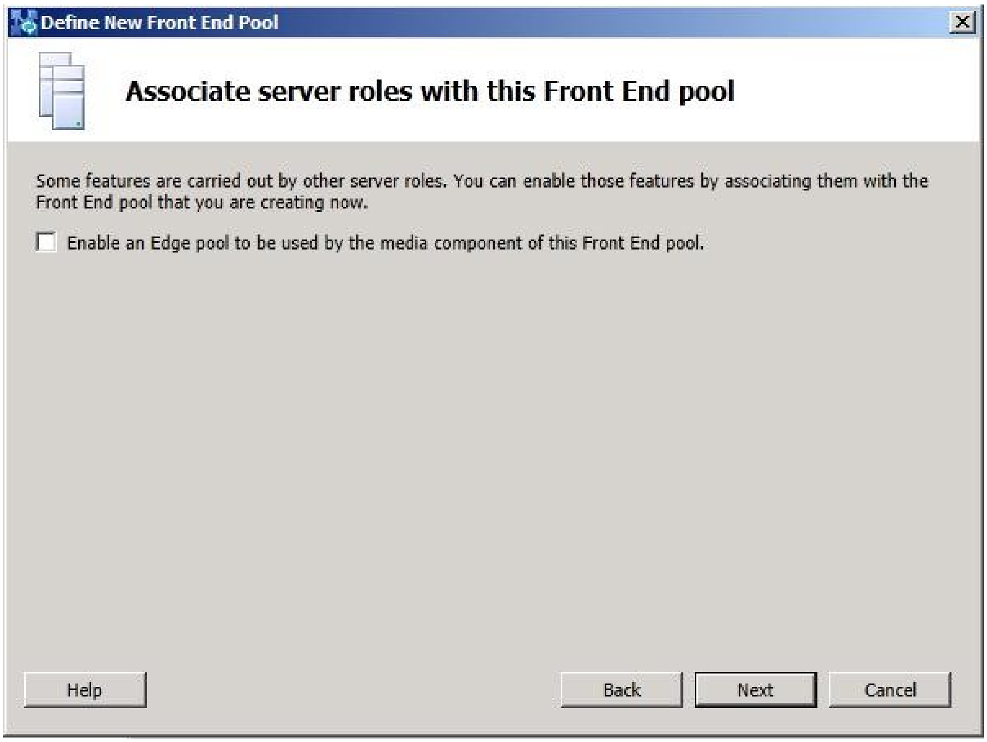
The Mediation Server can be collocated on a Front End pool. Collocation requires fewer computers, but in larger deployments a stand-alone Mediation pool can provide better voice quality and greater scalability.

Select which server roles and services you would like to collocate on this Front End pool.

☑ Collocate Mediation Server
You can collocate the Mediation Server on the Front End Server if your IP/PSTN gateway or your IP-PBX supports media bypass and if Enterprise Voice is not mission-critical for your organization.

9. On the **Associate server roles with this Front End pool** page, during pilot

pool deployment, do not choose the **Enable an Edge pool to be used by the media component of this Front End pool** option. This is a feature you will enable and bring online in a later phase of migration. Keep this setting cleared for now.



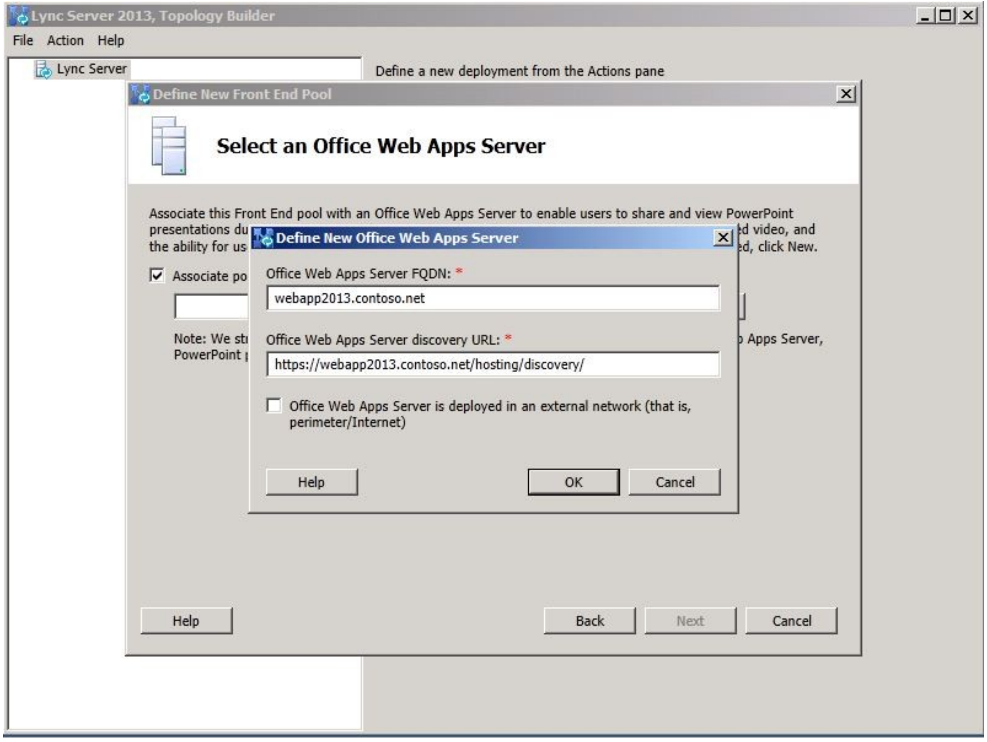
Define New Front End Pool

Associate server roles with this Front End pool

Some features are carried out by other server roles. You can enable those features by associating them with the Front End pool that you are creating now.

☐ Enable an Edge pool to be used by the media component of this Front End pool.

10.On the **Select an Office Web Apps Server** page, click **New**, and specify the FQDN of the application server.



Lync Server 2013, Topology Builder

Define a new deployment from the Actions pane

Define New Front End Pool

Select an Office Web Apps Server

Associate this Front End pool with an Office Web Apps Server to enable users to share and view PowerPoint presentations du … d video, and the ability for us … d, click New.

☑ Associate po

Note: We st … Apps Server, PowerPoint

Define New Office Web Apps Server

Office Web Apps Server FQDN: *

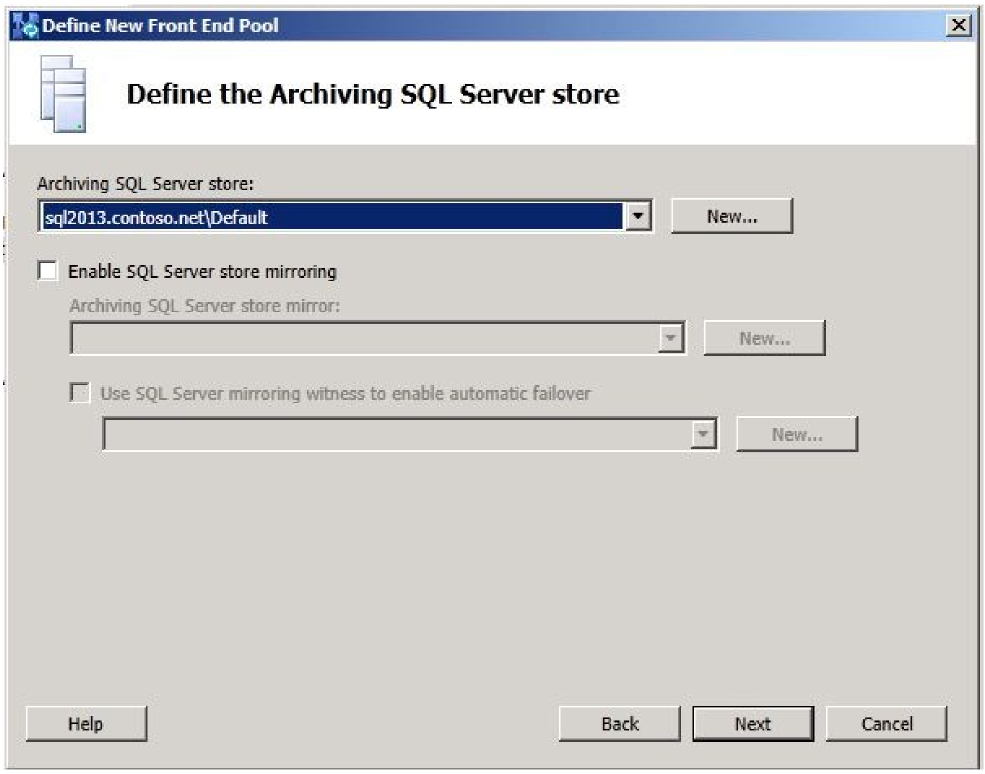
webapp2013.contoso.net

Office Web Apps Server discovery URL: *

https://webapp2013.contoso.net/hosting/discovery/

☐ Office Web Apps Server is deployed in an external network (that is, perimeter/Internet).

11.On the **Define the Archiving SQL Server store** page, select the SQL Server instance created earlier for Lync Server 2013.



Define New Front End Pool

Define the Archiving SQL Server store

Archiving SQL Server store: sql2013.contoso.net\Default

□ Enable SQL Server store mirroring

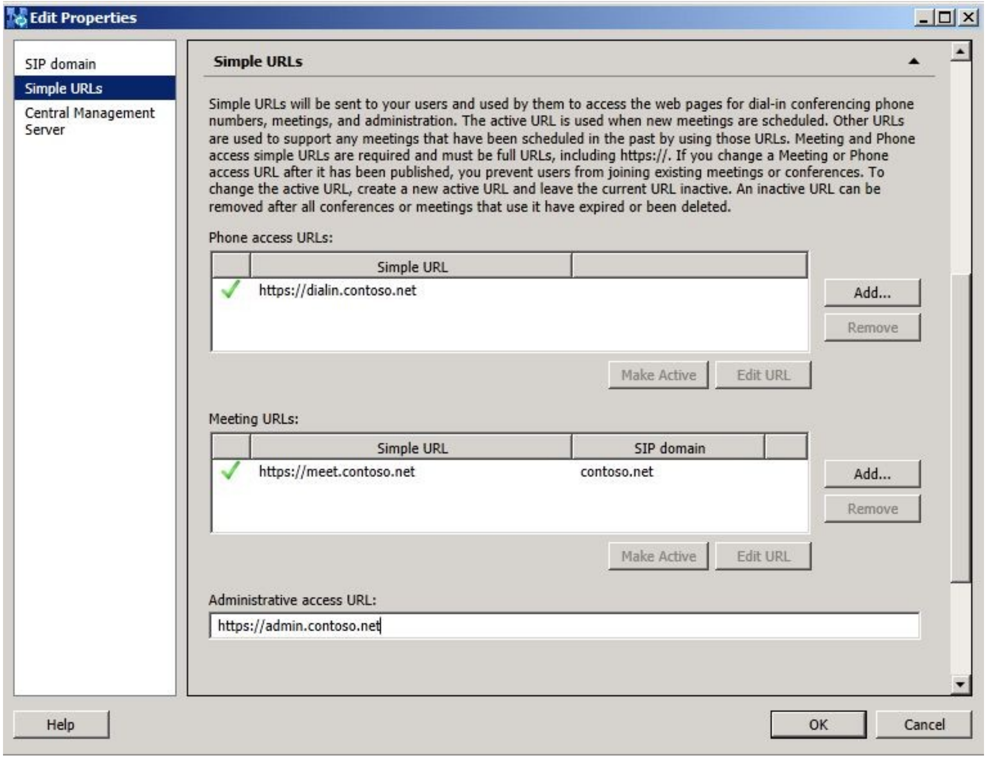
Archiving SQL Server store mirror:

□ Use SQL Server mirroring witness to enable automatic failover

12.On the **Define the Monitoring SQL Server store** page, select the SQL Server instance created earlier for Lync Server 2013. Click **Finish**.

13.From the top node of Topology Builder, right click **Lync Server** and click **Edit Properties.** Click **Simple URLs**.

14.Update the **Administrative access URL**.



Edit Properties

Simple URLs

Simple URLs will be sent to your users and used by them to access the web pages for dial-in conferencing phone numbers, meetings, and administration. The active URL is used when new meetings are scheduled. Other URLs are used to support any meetings that have been scheduled in the past by using those URLs. Meeting and Phone access simple URLs are required and must be full URLs, including https://. If you change a Meeting or Phone access URL after it has been published, you prevent users from joining existing meetings or conferences. To change the active URL, create a new active URL and leave the current URL inactive. An inactive URL can be removed after all conferences or meetings that use it have expired or been deleted.

Phone access URLs:

	Simple URL	
✓	https://dialin.contoso.net	

Meeting URLs:

	Simple URL	SIP domain
✓	https://meet.contoso.net	contoso.net

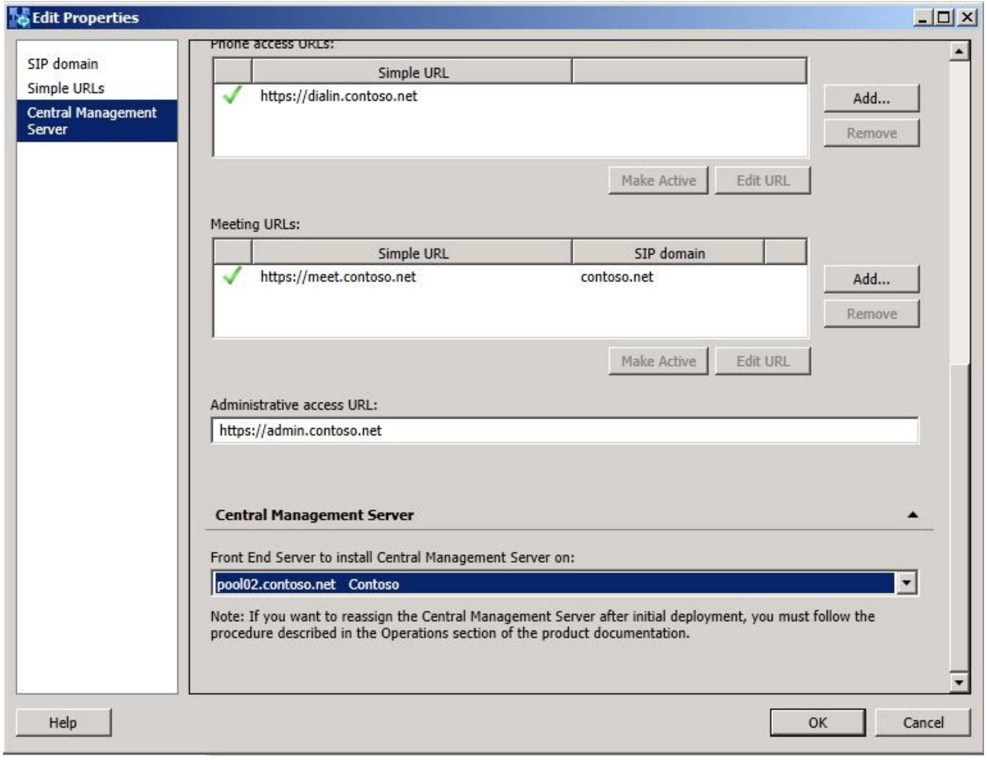
Administrative access URL: https://admin.contoso.net

For additional information on Simple URLs, see the topic Edit or Configure

Simple URLs in the Deployment documentation.

15.From the **Edit Properties**, click **Central Management Server**.

16.From the drop-down list, select the Lync Server 2013 pool.



Phone access URLs:

	Simple URL	
✓	https://dialin.contoso.net	

Meeting URLs:

	Simple URL	SIP domain
✓	https://meet.contoso.net	contoso.net

Administrative access URL:
https://admin.contoso.net

Central Management Server

Front End Server to install Central Management Server on:
pool02.contoso.net Contoso

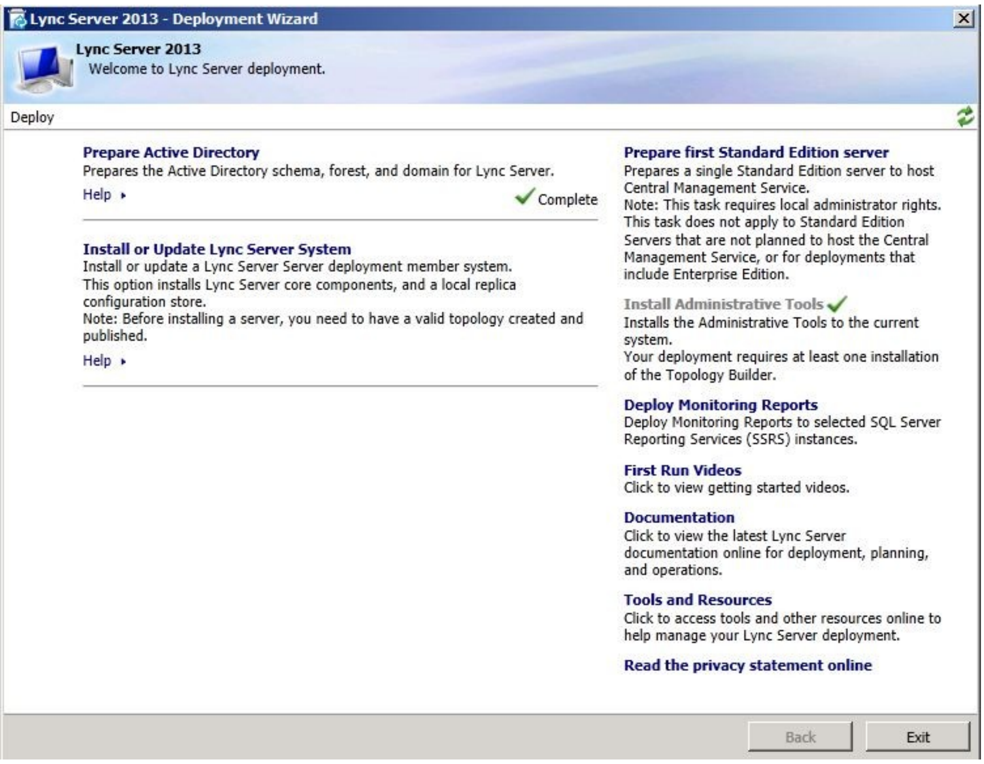
Note: If you want to reassign the Central Management Server after initial deployment, you must follow the procedure described in the Operations section of the product documentation.

17.Click OK to close **the Edit Properties** page.

18.From the **Action** menu, select **Publish Topology**.

19.When the publish process has completed, click **Finish**.

20.Returning to the Lync Server 2013 Deployment Wizard, click **Install or Update Lync Server System**.



Lync Server 2013 - Deployment Wizard

Lync Server 2013

Welcome to Lync Server deployment.

Deploy

Prepare Active Directory
Prepares the Active Directory schema, forest, and domain for Lync Server.
Help ▸ ✓ Complete

Install or Update Lync Server System
Install or update a Lync Server Server deployment member system.
This option installs Lync Server core components, and a local replica configuration store.
Note: Before installing a server, you need to have a valid topology created and published.
Help ▸

Prepare first Standard Edition server
Prepares a single Standard Edition server to host Central Management Service.
Note: This task requires local administrator rights.
This task does not apply to Standard Edition Servers that are not planned to host the Central Management Service, or for deployments that include Enterprise Edition.

Install Administrative Tools ✓
Installs the Administrative Tools to the current system.
Your deployment requires at least one installation of the Topology Builder.

Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

First Run Videos
Click to view getting started videos.

Documentation
Click to view the latest Lync Server documentation online for deployment, planning, and operations.

Tools and Resources
Click to access tools and other resources online to help manage your Lync Server deployment.

Read the privacy statement online

To install a local copy of the configuration store and start the required services, see Setting Up Front End Servers and Front End Pools in the Deployment documentation.

1.6.2.4.4 Verify Pilot Pool Coexistence with Legacy Pool

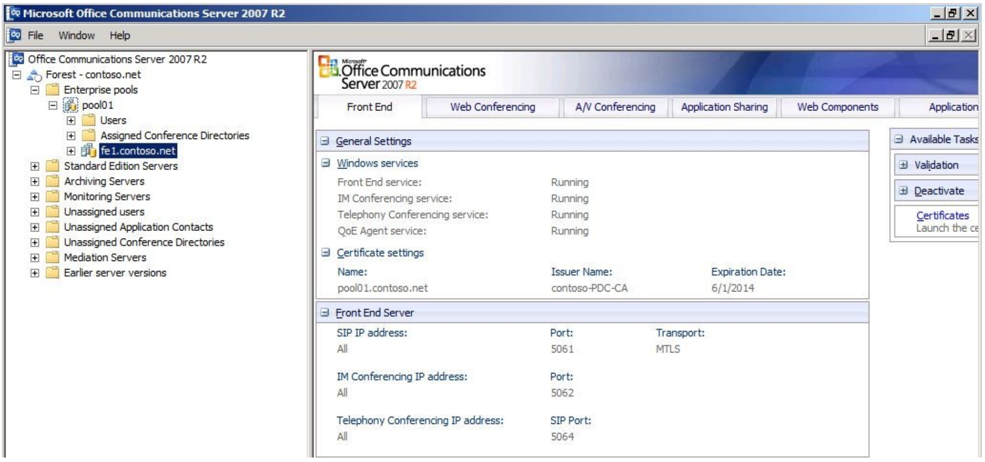
Verify Pilot Pool Coexistence with Legacy Pool

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 3: Deploy Lync Server 2013 Pilot Pool >

Topic Last Modified: *2012-09-28*

Verify the Pool in Office Communications Server 2007 R2 Administrative Tool

1. Open the Office Communications Server 2007 R2 administrative tool.
2. Expand the **Forest** node, expand the **Standard Edition Servers** or **Enterprise pools** node, and then expand the pool or server name.
3. Ensure that the Office Communications Server 2007 R2 services are running on the pool.



General Settings

Windows services

Front End service: Running
IM Conferencing service: Running
Telephony Conferencing service: Running
QoE Agent service: Running

Certificate settings

Name:	Issuer Name:	Expiration Date:
pool01.contoso.net	contoso-PDC-CA	6/1/2014

Front End Server

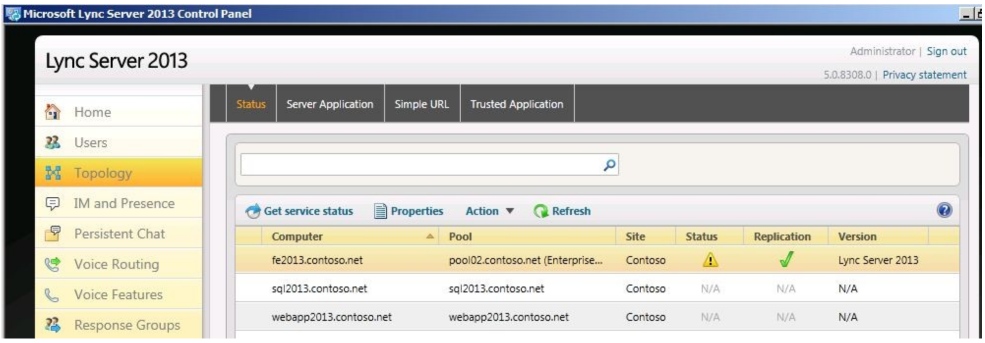
SIP IP address:	Port:	Transport:
All	5061	MTLS

IM Conferencing IP address: All
Port: 5062

Telephony Conferencing IP address: All
SIP Port: 5064

Verify the Pilot Pool in Lync Server 2013 Control Panel

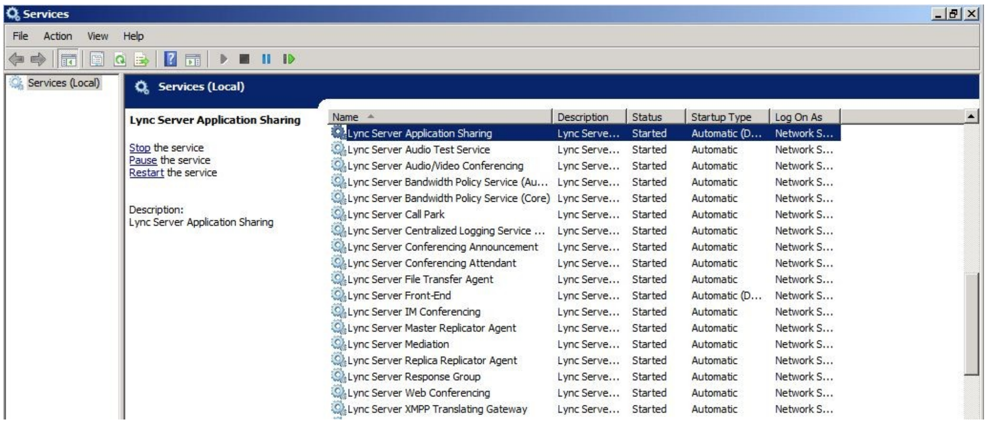
1. From a user account that is a member of the CsAdministrator role, log on to the Lync Server 2013 Front End server.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. Click **Topology**.
4. Verify that the servers you deployed are present in your pilot pool.



Computer	Pool	Site	Status	Replication	Version
fe2013.contoso.net	pool02.contoso.net (Enterprise...	Contoso	⚠	✓	Lync Server 2013
sql2013.contoso.net	sql2013.contoso.net	Contoso	N/A	N/A	N/A
webapp2013.contoso.net	webapp2013.contoso.net	Contoso	N/A	N/A	N/A

Verify Lync Server 2013 services have started

1. On the Lync Server 2013 Front End Server, open the **Services** applet from the **Administrative Tools** group.
2. Verify that the services listed match the list in the following figure.



Lync Server Application Sharing

Stop the service
Pause the service
Restart the service

Description:
Lync Server Application Sharing

Name	Description	Status	Startup Type	Log On As
Lync Server Application Sharing	Lync Serve...	Started	Automatic (D...	Network S...
Lync Server Audio Test Service	Lync Serve...	Started	Automatic	Network S...
Lync Server Audio/Video Conferencing	Lync Serve...	Started	Automatic	Network S...
Lync Server Bandwidth Policy Service (Au...	Lync Serve...	Started	Automatic	Network S...
Lync Server Bandwidth Policy Service (Core)	Lync Serve...	Started	Automatic	Network S...
Lync Server Call Park	Lync Serve...	Started	Automatic	Network S...
Lync Server Centralized Logging Service ...	Lync Serve...	Started	Automatic	Network S...
Lync Server Conferencing Announcement	Lync Serve...	Started	Automatic	Network S...
Lync Server Conferencing Attendant	Lync Serve...	Started	Automatic	Network S...
Lync Server File Transfer Agent	Lync Serve...	Started	Automatic	Network S...
Lync Server Front-End	Lync Serve...	Started	Automatic (D...	Network S...
Lync Server IM Conferencing	Lync Serve...	Started	Automatic	Network S...
Lync Server Master Replicator Agent	Lync Serve...	Started	Automatic	Network S...
Lync Server Mediation	Lync Serve...	Started	Automatic	Network S...
Lync Server Replica Replicator Agent	Lync Serve...	Started	Automatic	Network S...
Lync Server Response Group	Lync Serve...	Started	Automatic	Network S...
Lync Server Web Conferencing	Lync Serve...	Started	Automatic	Network S...
Lync Server XMPP Translating Gateway	Lync Serve...	Started	Automatic	Network S...

1.6.2.5 Phase 4: Merge Topologies

Phase 4: Merge Topologies

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-03-29*

The following topics outline the steps needed to merge your Microsoft Office Communications Server 2007 R2 pools to Microsoft Lync Server 2013 pools. First, you use the Topology Builder Merge wizard to merge topology information. This tool collects information about your Office Communications Server 2007 R2 environment, including Edge Server information, and publishes that information to a database shared with Lync Server 2013. After you publish the merged topology, Topology Builder is used to view the Office Communications Server 2007 R2 topology information and information about the newly deployed Lync Server 2013 topology. Finally, you use Lync Server Management Shell cmdlets to import policies and configuration settings.

In This Section

- Install WMI Backward Compatibility Package
- Merge Using Topology Builder Merge Wizard
- Import Policies and Settings
- Verify Topology Information

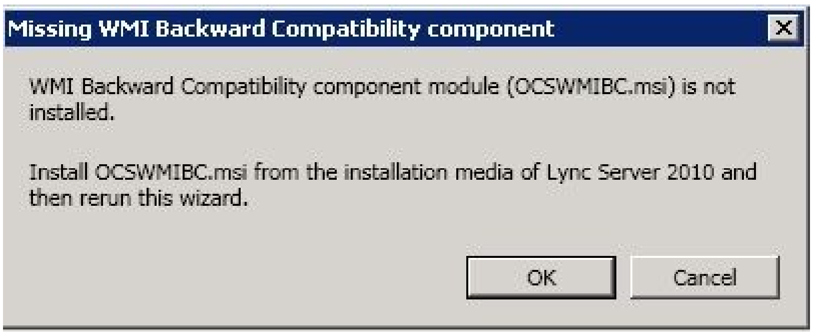
1.6.2.5.1 Install WMI Backward Compatibility Package

Install WMI Backward Compatibility Package

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 4: Merge Topologies >

Topic Last Modified: *2012-10-02*

If you attempt to run the Topology Builder Merge wizard without installing the WMI Backward Compatibility package, you will see the following error:

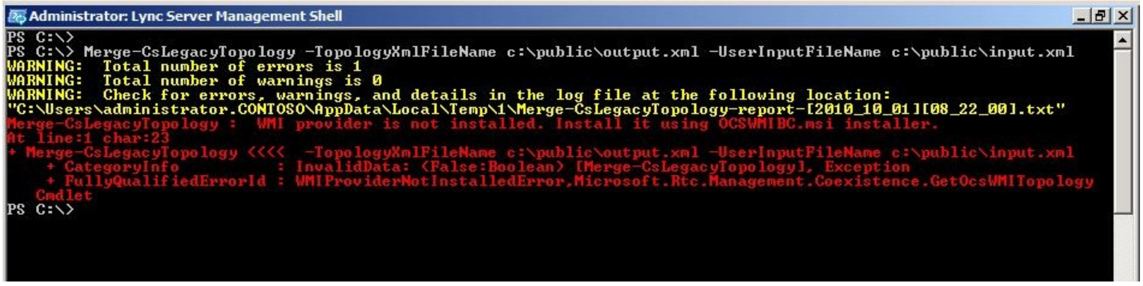


Missing WMI Backward Compatibility component

WMI Backward Compatibility component module (OCSWMIBC.msi) is not installed.

Install OCSWMIBC.msi from the installation media of Lync Server 2010 and then rerun this wizard.

If you attempt to run the **Merge-CsLegacytopology** cmdlet without installing the WMI Backward Compatibility package, you will see the following error:



```
PS C:\>
PS C:\> Merge-CsLegacyTopology -TopologyXmlFileName c:\public\output.xml -UserInputFileName c:\public\input.xml
WARNING:  Total number of errors is 1
WARNING:  Total number of warnings is 0
WARNING:  Check for errors, warnings, and details in the log file at the following location:
"C:\Users\administrator.CONTOSO\AppData\Local\Temp\1\Merge-CsLegacyTopology-report-[2010_10_01][08_22_00].txt"
Merge-CsLegacyTopology :  WMI provider is not installed. Install it using OCSWMIBC.msi installer.
At line:1 char:23
+ Merge-CsLegacyTopology <<<<  -TopologyXmlFileName c:\public\output.xml -UserInputFileName c:\public\input.xml
    + CategoryInfo          : InvalidData: (False:Boolean) [Merge-CsLegacyTopology], Exception
    + FullyQualifiedErrorId : WMIProviderNotInstalledError,Microsoft.Rtc.Management.Coexistence.GetOcsWMITopology
   Cmdlet
PS C:\>
```

To install the WMI Backward Compatibility Package

1. From your installation media, navigate to \SETUP\AMD64\SETUP \OCSWMIBC.MSI.
2. Install OCSWMIBC.MSI.

Important:

OCSWMIBC.msi must be installed on the computer where the Topology Builder Merge wizard is run. However, we recommend installing OCSWMIBC.msi on all Front End servers in your topology.

Important:

OCSWMIBC.msi can be installed on any computer in the domain that has the Lync Server 2013 Core Components and the Lync Server 2013 Management Shell installed, and has access to the Office Communications Server 2007 R2 topology (WMI provider to Active Directory Domain Services (AD DS) and SQL Server).

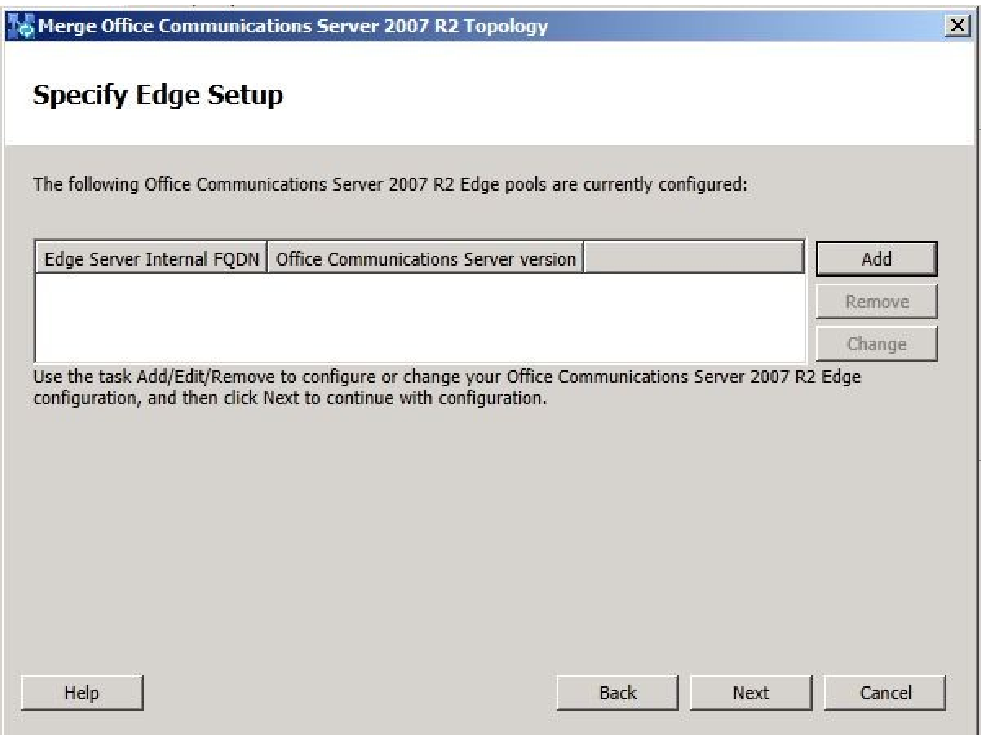
1.6.2.5.2 Merge Using Topology Builder Merge Wizard

Merge Using Topology Builder Merge Wizard

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 4: Merge Topologies >

Topic Last Modified: *2012-10-02*

1. Download the existing deployment using Topology Builder.
2. From the **Action** menu, select **Merge Office Communications Server 2007 R2**.
3. Click **Next**.
4. In **Specify Edge Setup**, click **Add**.



Specify Edge Setup

The following Office Communications Server 2007 R2 Edge pools are currently configured:

Edge Server Internal FQDN	Office Communications Server version	

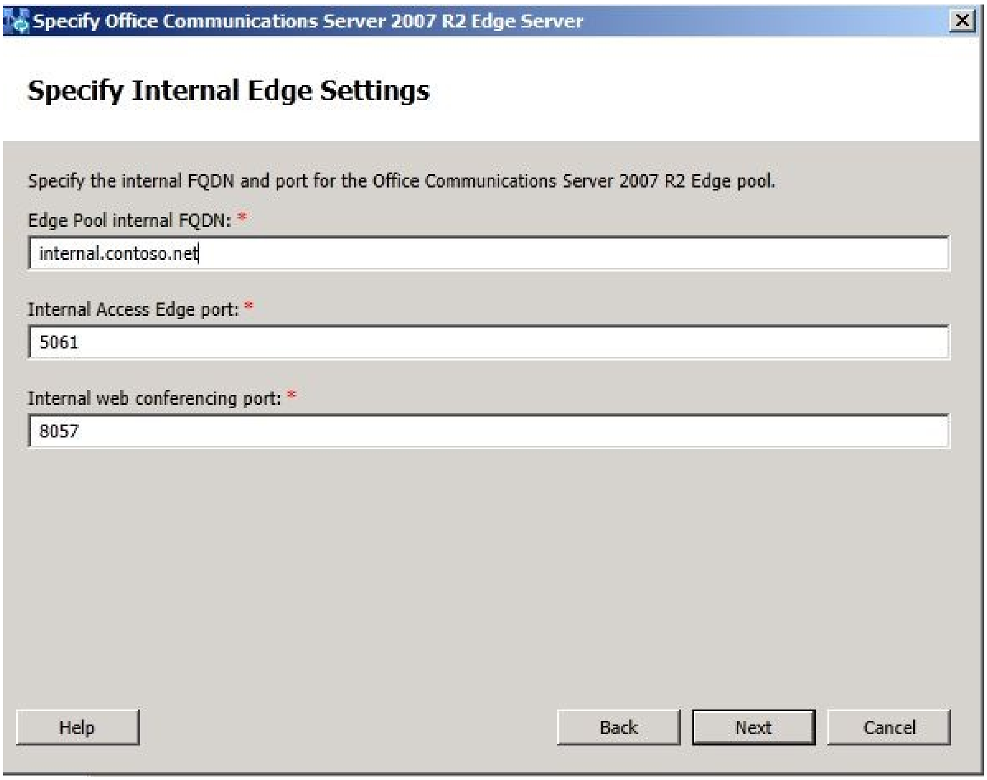
Use the task Add/Edit/Remove to configure or change your Office Communications Server 2007 R2 Edge configuration, and then click Next to continue with configuration.

5. In **Specify Edge Type**, enter the type of Edge Server configuration, and then click **Next**. This example uses the **Single Edge Server** option.

Important:

Expanded Edge deployment is not a supported configuration. An **Expanded Edge Server** must first be converted to a **Single Edge Server** or a **Load-balanced consolidated Edge** Server.

6. In **Specify Internal Edge Settings** , enter the relevant information for your Edge pool's internal FQDN and ports as needed, and then click **Next**.



Specify Internal Edge Settings

Specify the internal FQDN and port for the Office Communications Server 2007 R2 Edge pool.

Edge Pool internal FQDN: * internal.contoso.net

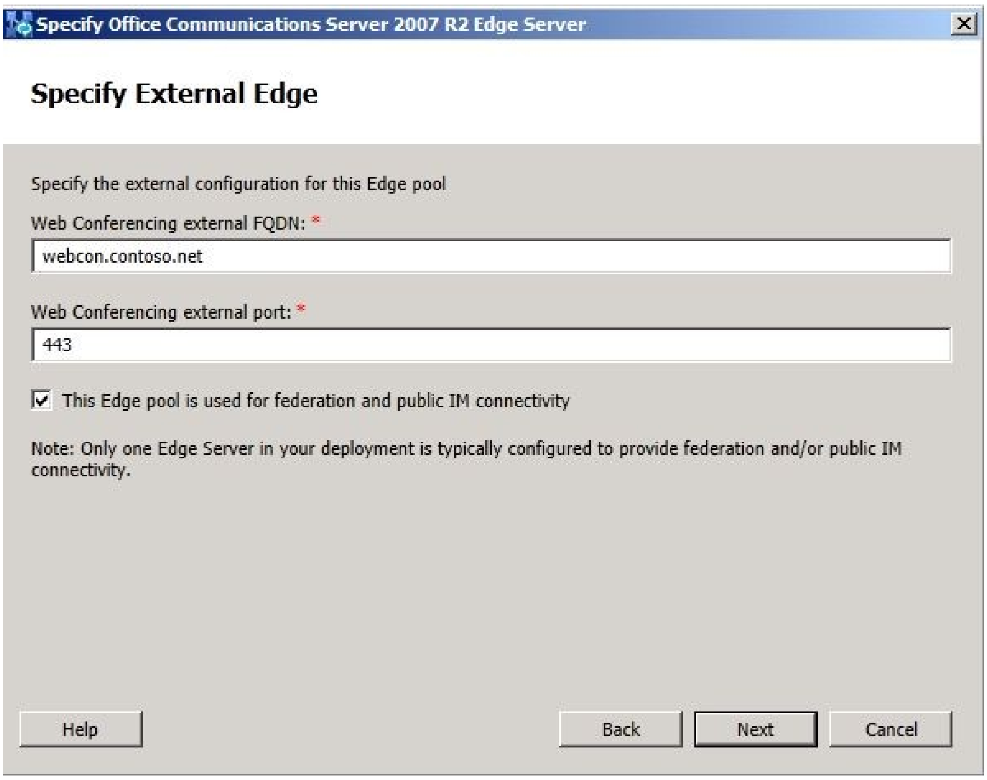
Internal Access Edge port: * 5061

Internal web conferencing port: * 8057

7. In **Specify External Edge**, enter the web conferencing FQDN information for your Edge Server.

> **Important:**
> Before you click **Next**, do the next step in this procedure. It is very important that you do not miss this step.

8. Check the **This Edge pool is used for federation and public IM connectivity** check box if you plan to use the legacy Office Communications Server 2007 R2 Edge Server for federation. If you have multiple Edge Servers deployed, only one of them will be enabled for federation. If you do not check this box and you decide later that you want to enable federation, you must run the Topology Builder Merge wizard and publish your topology again.



Specify Office Communications Server 2007 R2 Edge Server

Specify External Edge

Specify the external configuration for this Edge pool

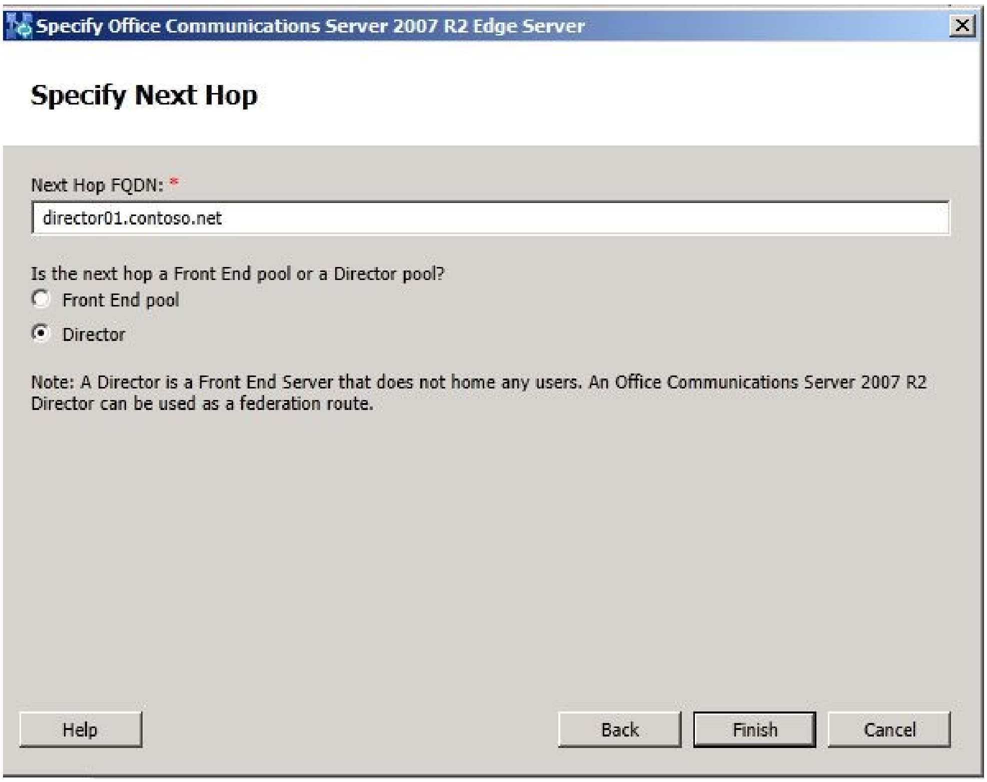
Web Conferencing external FQDN: *
webcon.contoso.net

Web Conferencing external port: *
443

☑ This Edge pool is used for federation and public IM connectivity

Note: Only one Edge Server in your deployment is typically configured to provide federation and/or public IM connectivity.

9. In **Specify Next Hop**, enter the fully qualified domain name (FQDN) of the next hop location in your environment. Click **Finish**.



Specify Office Communications Server 2007 R2 Edge Server

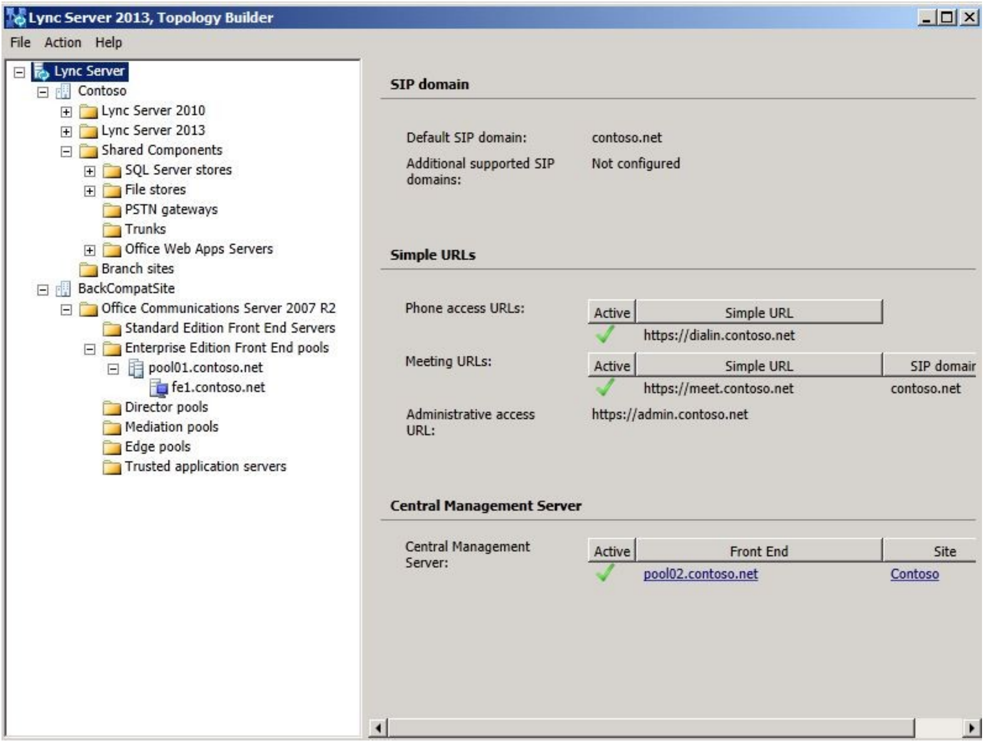
Specify Next Hop

Next Hop FQDN: *
director01.contoso.net

Is the next hop a Front End pool or a Director pool?
○ Front End pool
● Director

Note: A Director is a Front End Server that does not home any users. An Office Communications Server 2007 R2 Director can be used as a federation route.

10. In **Specify Edge Setup**, if all your Office Communications Server 2007 R2 Edge Servers have been added, click **Next**. If you have more Office Communications Server 2007 R2 Edge Servers to add, repeat this procedure starting at step 4.
11. In **Specify Internal SIP port** , select the default setting (that is, if you did not modify the default SIP port). Change as appropriate if you are not using a default port of 5061, and then click **Next**.
12. In **Summary**, click **Next** to begin merging the topologies.
13. The wizard page verifies that the merging of the topologies was successful.
14. In the **Status** column, verify that the value is **Success**, and then click **Finish**.
15. In the left pane of Topology Builder, you should now see the **BackCompatSite**, which indicates that your Office Communications Server 2007 R2 environment has been merged with Lync Server 2013.



SIP domain

Default SIP domain: contoso.net

Additional supported SIP domains: Not configured

Simple URLs

Phone access URLs:

Active	Simple URL
✓	https://dialin.contoso.net

Meeting URLs:

Active	Simple URL	SIP domair
✓	https://meet.contoso.net	contoso.net

Administrative access URL: https://admin.contoso.net

Central Management Server

Central Management Server:

Active	Front End	Site
✓	pool02.contoso.net	Contoso

16. From the **Action** menu, click **Publish Topology**, and then click **Next**.
17. When the **Publishing wizard** completes, click **Finish**.

> **Note:**
> It’s important that you complete the next topic, Import Policies and Settings, to ensure that the legacy policy settings are imported into Lync Server 2013.

1.6.2.5.3 Import Policies and Settings

Import Policies and Settings

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 4: Merge Topologies >

Topic Last Modified: *2012-09-28*

After you merge your Office Communications Server 2007 R2 topology information with your Lync Server 2013 pilot pool, you need to run a Lync Server 2013 Management Shell cmdlet to migrate your Office Communications Server 2007 R2 policies and configuration settings to your Lync Server 2013 pilot pool.

The **Import-CsLegacyConfiguration** cmdlet imports policies, voice routes, dial plans, Communicator Web Access URLs, and dial-in access numbers to Lync Server 2013.

To migrate policies and settings

1. On the Lync Server 2013 Front End server, start the Lync Server Management Shell.
2. At the command line, type the following:

   ```
   Import-CsLegacyConfiguration
   ```

   After the policies are imported, use the procedure that follows to see the imported policies in the Lync Server Control Panel .

To view imported policies

1. Open Lync Server 2013 Control Panel.
2. Click **Voice Routing** and view the imported policies.
3. Click **Conferencing** and view the imported policies.
4. Click **Federation and External Access** and view the imported policies.
5. Click **Monitoring and Archiving** and view the imported policies.

1.6.2.5.4 Verify Topology Information

Verify Topology Information

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 4: Merge Topologies >

Topic Last Modified: *2012-09-26*

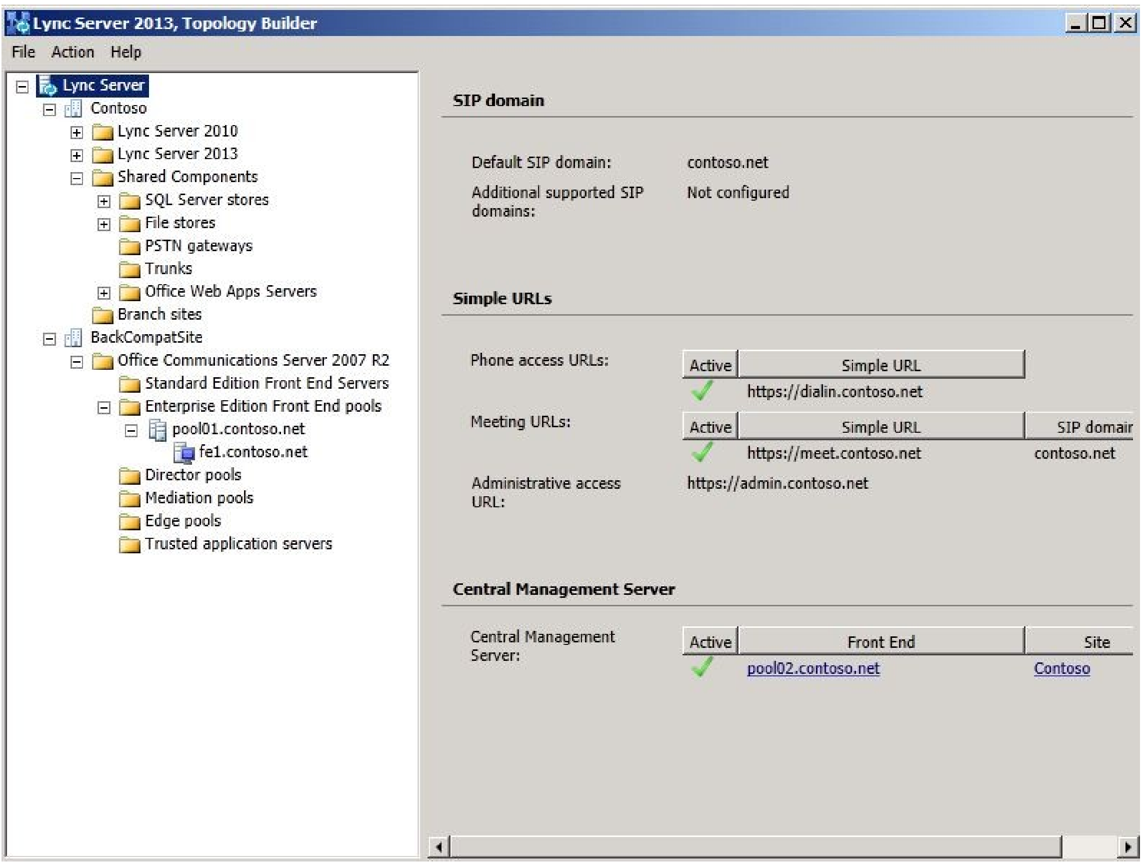
The first step in verifying the merge completed successfully is to view the Office Communications Server 2007 R2 topology information that you merged with Lync Server 2013. In Topology Builder, the **BackCompatSite** node displays the fully qualified domain name (FQDN) of each Office Communications Server 2007 R2 pool and server that you merged.

To view BackCompatSite in Topology Builder

1. In your Office Communications Server 2007 R2 environment, open the Office Communications Server 2007 R2 administrative tool and note the FQDNs of the legacy pools and servers.
2. In your Lync Server 2013 environment, open Topology Builder and then expand the **BackCompatSite** node.
3. Verify that the FQDNs for the pools and servers that you merge are displayed.

Note:

You do not see any information in **BackCompatSite** for server roles that are collocated on a Front End Server or Standard Edition server. Only server roles that are required for interoperability between Office Communications Server 2007 R2 and Lync Server 2013 are shown.



SIP domain

Default SIP domain: contoso.net

Additional supported SIP domains: Not configured

Simple URLs

Phone access URLs:

Active	Simple URL
✓	https://dialin.contoso.net

Meeting URLs:

Active	Simple URL	SIP domair
✓	https://meet.contoso.net	contoso.net

Administrative access URL: https://admin.contoso.net

Central Management Server

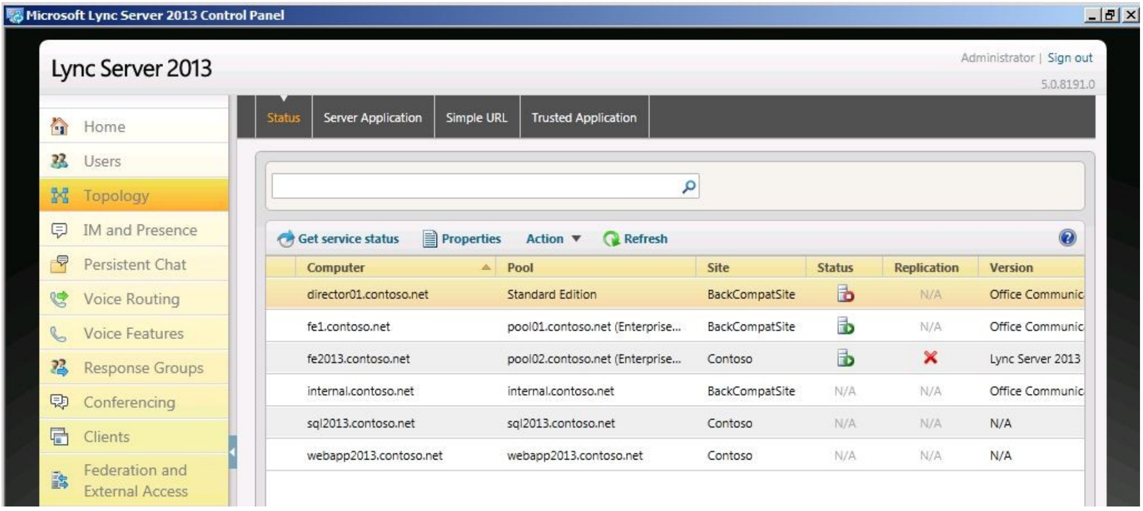
Central Management Server:

Active	Front End	Site
✓	pool02.contoso.net	Contoso

You can also use Lync Server 2013 Control Panel to view your merged topology. In Lync Server 2013 Control Panel, you can see each server FQDN, pool FQDN, and site name for your merged topology. Merged servers have a **Site** name of **BackCompatSite**.

To view the merged topology in Lync Server 2013 Control Panel

1. Open Lync Server 2013 Control Panel.
2. Click **Topology**.
3. On the **Status** tab, verify that servers and pools you merged appear by looking for **BackCompatSite** in the **Site** column.



Computer	Pool	Site	Status	Replication	Version
director01.contoso.net	Standard Edition	BackCompatSite		N/A	Office Communic
fe1.contoso.net	pool01.contoso.net (Enterprise...	BackCompatSite		N/A	Office Communic
fe2013.contoso.net	pool02.contoso.net (Enterprise...	Contoso		✗	Lync Server 2013
internal.contoso.net	internal.contoso.net	BackCompatSite	N/A	N/A	Office Communic
sql2013.contoso.net	sql2013.contoso.net	Contoso	N/A	N/A	N/A
webapp2013.contoso.net	webapp2013.contoso.net	Contoso	N/A	N/A	N/A

To see more detail about a merged pool, use the **Get-CsPool** cmdlet. In addition to the information that is available in Topology Builder and Lync Server 2013 Control Panel, this cmdlet displays the services that run on the Lync Server 2013 pool.

> **Note:**
> When you publish the topology after running the Merge wizard in Topology Builder, conference directories are merged to Lync Server 2013. Conference directories can be verified by running the **Get-CsConferenceDirectory** cmdlet.

To view services on a merged pool

1. Open the Lync Server 2013 Management Shell.
2. At the command line, type the following:

```
Get-CsPool [-Identity <FQDN of the pool>]
```

For example:

```
Get-CsPool -Identity pool02.contoso.net
```

To verify conference directories merged

1. Open the Lync Server 2013 Management Shell.
2. At the command line, type the following:

```
Get-CsConferenceDirectory
```

3. Verify that all the conference directories for the pool or server you are merging are now in Lync Server 2013.

1.6.2.6 Phase 5: Configure the Pilot Pool

Phase 5: Configure the Pilot Pool

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-10-19*

Now that the pilot pool has been created and legacy deployment information has been merged with Lync Server 2013, this section identifies a few configurations that must be made to the pilot pool.

In This Section

1.6.2.6.1 Connect Pilot Pool to Legacy Edge Servers

Connect Pilot Pool to Legacy Edge Servers

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 5: Configure the Pilot Pool >

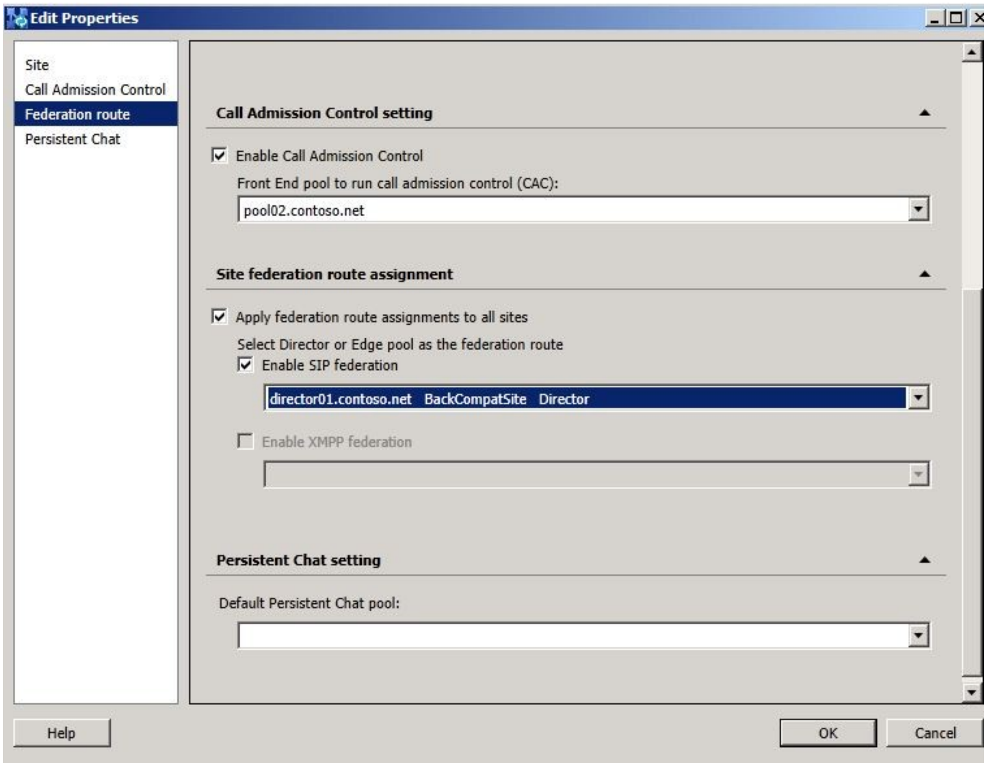
Topic Last Modified: *2012-10-02*

After deploying Lync Server 2013, a federation route for this site is not configured. In order to use the federated route that is being used by Office Communications Server 2007 R2, Lync Server 2013 must be configured to use this route.

To enable the Lync Server 2013 site to use the Director and Edge Server of the BackCompatSite, use Topology Builder to associate the legacy Edge pool.

To associate the legacy Edge pool by using Topology Builder

1. Open the pilot pool topology in Topology Builder.
2. Select your Lync Server 2013 site.
3. On the **Action** menu, click **Edit Properties**.
4. Under **Site federation route assignment**, select **Enable SIP federation**, and then select the Office Communications Server 2007 R2 Director, or the Office Communications Server 2007 R2 Edge Server if no Director is listed.



Call Admission Control setting

☑ Enable Call Admission Control

Front End pool to run call admission control (CAC): pool02.contoso.net

Site federation route assignment

☑ Apply federation route assignments to all sites

Select Director or Edge pool as the federation route

☑ Enable SIP federation

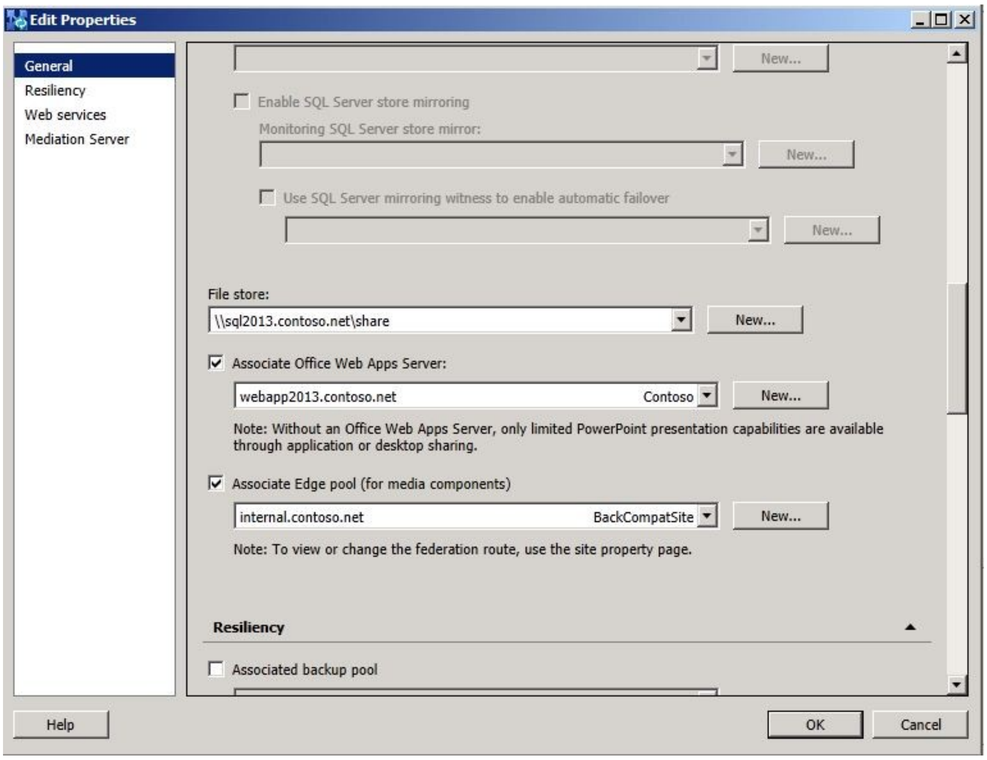
director01.contoso.net BackCompatSite Director

☐ Enable XMPP federation

Persistent Chat setting

Default Persistent Chat pool:

5. Click **OK** to close the **Edit Properties** page.
6. In Topology Builder, under the Lync Server 2013 node, navigate to the **Standard Edition server** or **Enterprise Edition Front End pools**, right-click the pool, and then click **Edit Properties**.
7. Under **Associations**, select the check box next to **Associate Edge pool (for media components)**.
8. From the list, select the Edge Server interface for the BackCompatSite.



☐ Enable SQL Server store mirroring

Monitoring SQL Server store mirror:

☐ Use SQL Server mirroring witness to enable automatic failover

File store:
\\sql2013.contoso.net\share

☑ Associate Office Web Apps Server:
webapp2013.contoso.net Contoso

Note: Without an Office Web Apps Server, only limited PowerPoint presentation capabilities are available through application or desktop sharing.

☑ Associate Edge pool (for media components)
internal.contoso.net BackCompatSite

Note: To view or change the federation route, use the site property page.

Resiliency

☐ Associated backup pool

9. Click **OK** to close the **Edit Properties** page.
10. In **Topology Builder**, select the top-most node, **Lync Server**.
11. From the **Action** menu, click **Publish Topology**, and then click **Next**.
12. When the **Publishing wizard** completes, click **Finish**.

1.6.2.6.2 Authorize Connection to Office Communications Server 2007 R2 Edge Server

Authorize Connection to Office Communications Server 2007 R2 Edge Server

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 5: Configure the Pilot Pool >

Topic Last Modified: *2012-09-28*

For each Lync Server 2013 Front End Server or Standard Edition server in your pilot pool, you must update the list of internal servers that are authorized to connect to the Office Communications Server 2007 R2 Edge Server. Without these updates, external audio/visual (A/V) conferencing for users joining by using the legacy Edge Server will not work.

To Authorize Connection to Office Communications Server 2007 R2 Edge Server

1. From the Office Communications Server 2007 R2 Edge Server, from the **Administrative Tools** group, open the **Computer Management** snap-in.
2. In the console tree, expand **Services and Applications**.
3. Right-click **Office Communications Server 2007 R2**, and then click

Properties.

4. Click the **Internal** tab.
5. Under **Add Server**, click **Add**.
6. In the **Add Office Communications Server** dialog box, enter the appropriate information:

   - Specify the fully qualified domain name (FQDN) of each Lync Server 2013 Front End Server or Standard Edition server, and Lync Server 2013 pool.

   - Specify the FQDN of the Lync Server 2013 Director if you configured a static route on the pool that specifies the next hop computer by its FQDN.

7. After you have added an entry for each Lync Server 2013, Front End Server, Standard Edition server, pool, and Director, click **Apply** and then click **OK** to close the Properties page.

1.6.2.6.3 Verify Configuration Settings

Verify Configuration Settings

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 5: Configure the Pilot Pool >

Topic Last Modified: *2012-09-28*

After you merge the topology and run the **Import-CsLegacyConfiguration** cmdlet, verify that your Office Communications Server 2007 R2 policies and settings were imported to Lync Server 2013. The following table lists the policies and settings that you should verify.

Policies and Settings to Verify after Migration

If you use this workload:	Verify these policies and settings:
Instant messaging (IM) and conferencing	Presence policy Conferencing policy
Dial-in conferencing	Dial-in access numbers Dial plans
Enterprise Voice	Voice policy Voice routes Dial plans PSTN usage settings
Communicator Web Access	Simple URLs
External users	External access policies
Archiving	Archiving policy

To verify policies and settings

1. In your Office Communications Server 2007 R2 environment, make note of the names of dial plans (formerly known as location profiles), dial-in access numbers (Conferencing Attendant access phone numbers and regions), voice routes, and the policies listed in the preceding table, in addition to the URLs used for Communicator Web Access.
2. On the Lync Server 2013 Front End server, open Lync Server Control Panel.
3. To verify imported conferencing policies, in the left pane, click **Conferencing**, click **Conferencing Policy**, and then verify that all the conferencing policies in your Office Communications Server 2007 R2 environment are included in the list.

   > **Note:**
   > The **Meeting** policy from previous versions of Office Communications Server is now known as the conferencing policy in Lync Server 2013. Additionally, the **Anonymous Particpants** setting from previous versions of Office Communications Server is now a setting in the Lync Server 2013 conferencing policy.

   > **Note:**
   > In Office Communications Server 2007 R2, if the conferencing policy is not set to **use per user**, only global policy settings are imported. No other conference policies are imported in this situation.

   > **Note:**
   > If **Anonymous Participants** is set to **Enforce per user** in your Office Communications Server 2007 R2 conferencing policy, two conferencing policies are created during migration: one with **AllowAnonymousParticipantsInMeetings** set to **True** and one with **AllowAnonymousParticipantsInMeetings** set to **False**.

4. To verify imported dial plans, click **Voice Routing**, click **Dial Plan**, and then verify that all the dial plans in your Office Communicator 2007 R2 environment are included in the list.

   > **Note:**
   > In Lync Server 2013, **location profiles** are now referred to as **dial-plans**.

5. To verify imported voice policies, click **Voice Routing**, click **Voice Policy**, and then verify that all the voice policies in your Office Communicator 2007 R2 environment are included in the list.

   > **Note:**
   > If voice policy is not set to **use per user** in your Office Communications Server 2007 R2 environment, only global policy settings are imported. No other voice policies are imported in this situation.

6. To verify imported voice routes, click **Voice Routing**, click **Route**, and then verify that all the voice routes in your Office Communicator 2007 R2 environment are included in the list.
7. To verify imported PSTN usage settings, click **Voice Routing**, click **PSTN Usage**, and then verify that the PSTN Usage settings from your Office Communicator 2007 R2 environment are included in the list.
8. To verify imported external access policies, click **Federation and External Access**, click **External Access Policy**, and then verify that all the external access policies in your Office Communicator 2007 R2 environment are included in the list.
9. To verify archiving policies, click **Monitoring and Archiving**, click **Archiving Policy**, and then verify that all the archiving policies in your Office Communications Server 2007 R2 environment are included in the list.
10. Open the Lync Server Management Shell.

11. To verify presence policies, at the command line, type the following:

    ```
    Get-CsPresencePolicy
    ```

    By looking at the name in the **Identity** parameter, verify that all the presence policies in your Office Communications Server 2007 R2 environment were imported.

To verify policies and settings by using cmdlets

1. Open the Lync Server Management Shell.
2. Run the cmdlets in the following table to verify policies and settings.

   The syntax of these cmdlets is like the following example:

   ```
   Get-CsConferencingPolicy
   ```

   For details about these cmdlets, run:

   ```
   Get-Help <cmdlet name> -Detailed
   ```

For this policy or setting:	Use this cmdlet:
Presence policy	**Get-CsPresencePolicy**
Conferencing policy	**Get-CsConferencingPolicy**
Dial-in access numbers	**Get-CsDialInConferencingAccessNumber**
Dial plans	**Get-CsDialPlan**
Voice policy	**Get-CsVoicePolicy**
Voice routes	**Get-CsVoiceRoute**
PSTN Usage	**Get-CsPstnUsage**
URLs	**Get-CsSimpleUrlConfiguration**
External access policies	**Get-CsExternalAccessPolicy**
Archiving policy	**Get-CsArchivingPolicy**

1.6.2.6.4 Configure XMPP Gateway Access Policies and Certificates

Configure XMPP Gateway Access Policies and Certificates

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 5: Configure the Pilot Pool >

***Topic Last Modified:** 2012-10-15*

XMPP federation defines an external deployment based on the eXtensible Messaging and Presence Protocol (XMPP). An XMPP configuration allows Lync users access to XMPP domain users by:

- IM and Presence – person to person only
- Creation of XMPP federated contacts in the Lync client

When you configure policies for support of extensible messaging and presence protocol

(XMPP) federated partners, the policies apply to users of XMPP federated domains, but not to users of session initiation protocol (SIP) instant messaging (IM) service providers (for example, Windows Live), or SIP federated domains. You configure an XMPP Federated Partner for each XMPP federated domain that you want to allow your users to add contacts and communicate with. Once the policies are in place, you need to configure the XMPP Gateway certificates.

Note:

To begin the XMPP Gateway migration, you need to deploy the Lync Server 2013 XMPP Gateway, and configure access policies to enable users for Lync Server 2013 XMPP Gateway. All users must be moved to the Lync Server 2013 deployment before you perform these steps. For details, see Configure XMPP Gateway on Lync Server 2013.

⊟Configure an External Access Policy to Enable Users for Lync Server 2013 XMPP Gateway

1. Open Lync Server Control Panel.
2. In the left navigation bar, click **Federation and External Access**, and then click **External Access Policy**.
3. Click **New** and then click **User policy**.
4. Enter a name for the external access user policy.
5. Provide a description for external access user policy.
6. Select **Enable communications with federated users**.
7. Select **Enable communications with XMPP federated users**.
8. Click **Commit** to save your changes to the site or user policy.

1.6.2.7 Phase 6: Move users to the Pilot Pool

Phase 6: Move users to the Pilot Pool

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-10-16*

You can move a single user or groups of users to the new Lync Server 2013 deployment using the following two methods: Lync Server Control Panel and Lync Server Management Shell. The topics in this section describe tasks you must complete during pilot deployment, as well as prior to moving your deployment of Lync Server 2013 from a pilot deployment to a production-level deployment.

In This Section

- Verify User Replication Has Completed
- Move a Single User to the Pilot Pool
- Move Multiple Users to the Pilot Pool

1.6.2.7.1 Verify User Replication Has Completed

Verify User Replication Has Completed

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 6: Move users to the Pilot Pool >

Topic Last Modified: *2012-09-28*

When running the **Move-CsLegacyUser** cmdlet, you may experience a failure due to user information between Active Directory Domain Services (AD DS) and the Lync Server 2013 databases being out of sync because the initial replication is incomplete. The time it takes for the successful completion of the Lync Server 2013 User Replicator service's initial synchronization depends on the number of domain controllers that are hosted in the Active Directory forest that hosts the Lync Server 2013 pool. The Lync Server 2013 User Replicator service initial synchronization process occurs when the Lync Server 2013 Front End Server is started for the first time. After that, the synchronization is then based on the User Replicator interval. Complete the following steps to verify user replication has completed before running the **Move-CsLegacyUser** cmdlet.

To verify that user replication has completed

1. From the Lync Server 2013 Front End server, click the **Start** menu, and then click **Run**.
2. Enter **eventvwr.exe** and then click **OK**.
3. In Event Viewer, click **Applications and Services logs** to expand it, and then select Lync Server.
4. In the **Actions** pane click **Filter Current Log**.
5. From the **Event sources** list, click **LS User Replicator**.
6. In **<All Event IDs>** enter **30024** and then click **OK**.
7. In the filtered events list, on the **General** tab, look for an entry that states user replication has completed successfully.

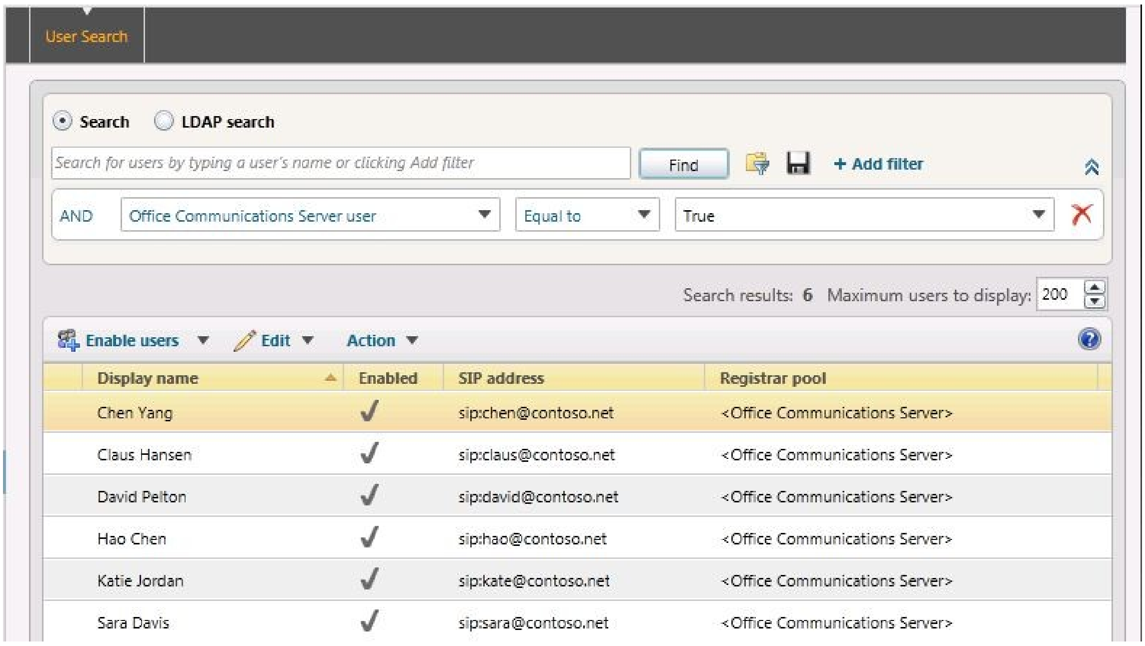
1.6.2.7.2 Move a Single User to the Pilot Pool

Move a Single User to the Pilot Pool

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 6: Move users to the Pilot Pool >

Topic Last Modified: *2012-09-28*

You can move a user from your Office Communications Server 2007 R2 pool to your Lync Server 2013 pilot pool using Lync Server 2013 Control Panel or Lync Server 2013 Management Shell. In the example below, in the Registrar pool column, **<Office Communications Server>** is the Office Communications Server 2007 R2 pool, and all six of these users are connected to this pool. Use the following procedures to move a user to your Lync Server 2013 pool using Lync Server 2013 Control Panel and Lync Server Management Shell.


User Search
● Search ○ LDAP search
Search for users by typing a user's name or clicking Add filter
Find
+ Add filter

AND | Office Communications Server user | Equal to | True

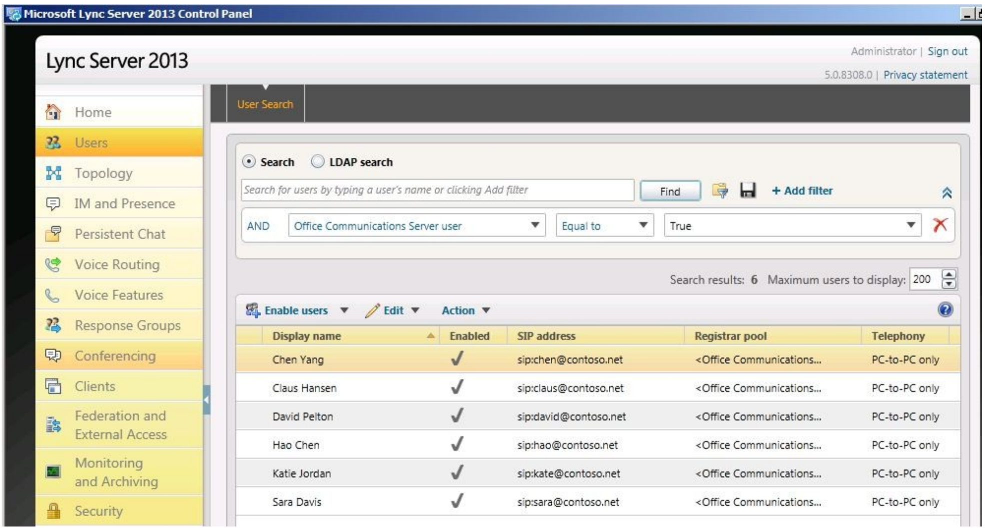
Search results: 6 Maximum users to display: 200

Enable users ▼ Edit ▼ Action ▼

Display name	Enabled	SIP address	Registrar pool
Chen Yang	✓	sip:chen@contoso.net	<Office Communications Server>
Claus Hansen	✓	sip:claus@contoso.net	<Office Communications Server>
David Pelton	✓	sip:david@contoso.net	<Office Communications Server>
Hao Chen	✓	sip:hao@contoso.net	<Office Communications Server>
Katie Jordan	✓	sip:kate@contoso.net	<Office Communications Server>
Sara Davis	✓	sip:sara@contoso.net	<Office Communications Server>

To move a user by using the Lync Server 2013 Control Panel

1. Log on to the Front End Server with an account that is a member of the RTCUniversalServerAdmins group or a member of the CsAdministrator or CsUserAdministrator administrative role.
2. Open Lync Server Control Panel.
3. Click **Users**.
4. From the **User Search** tab, click the **Search** button.
5. Next, click **Add Filter**.
6. Create a filter where **Office Communications Server user** is equal to **True**.
7. Click **Find** to search for legacy Office Communications Server 2007 R2 users.



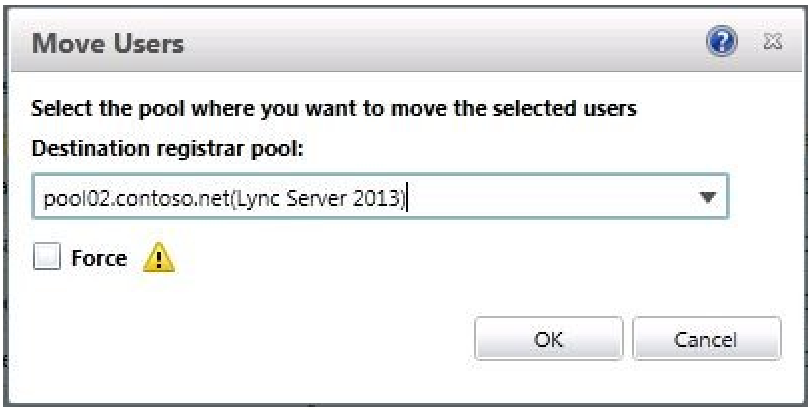
AND | Office Communications Server user | Equal to | True

Search results: 6 Maximum users to display: 200

Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	<Office Communications...	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	<Office Communications...	PC-to-PC only
David Pelton	✓	sip:david@contoso.net	<Office Communications...	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	<Office Communications...	PC-to-PC only
Katie Jordan	✓	sip:kate@contoso.net	<Office Communications...	PC-to-PC only
Sara Davis	✓	sip:sara@contoso.net	<Office Communications...	PC-to-PC only

8. Select a user that you want to move to the Lync Server 2013 pool. In this example, we will move user Sara Davis.

9. On the **Action** menu, select **Move selected users to pool**.
10. From the drop-down list, select the Lync Server 2013 pool.
11. Click **Action** and then click **Move selected users to pool**. Click **OK**.



Move Users

Select the pool where you want to move the selected users

Destination registrar pool: pool02.contoso.net(Lync Server 2013)

12. Verify that the **Registrar pool** column for the user now contains the Lync Server 2013 pool, which indicates that the user has been successfully moved

To move a user by using the Lync Server 2013 Management Shell

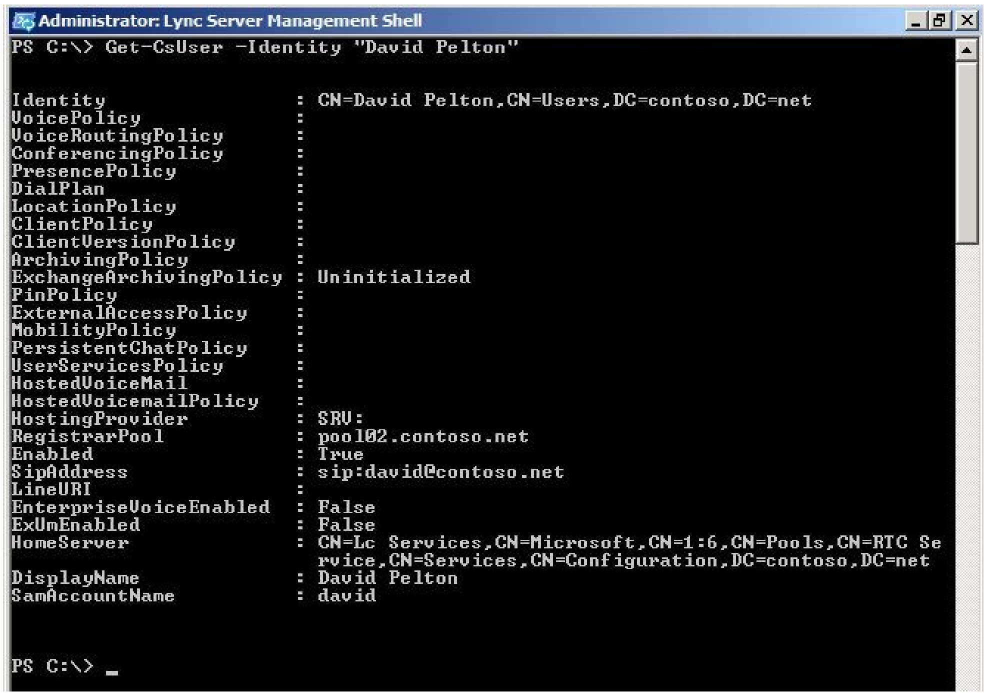
1. Open the Lync Server Management Shell.
2. At the command line, type the following:

```
Move-CsLegacyUser -Identity "David Pelton" -Target "pool02.contoso.net
```

3. Next, at the command line, type the following:

```
Get-CsUser -Identity "David Pelton"
```

4. The **RegistrarPool** identity now points to the Lync Server 2013 pool. The presence of this identity confirms that the user has been successfully moved.



Administrator: Lync Server Management Shell

```
PS C:\> Get-CsUser -Identity "David Pelton"


Identity                  : CN=David Pelton,CN=Users,DC=contoso,DC=net
VoicePolicy               :
VoiceRoutingPolicy        :
ConferencingPolicy        :
PresencePolicy            :
DialPlan                  :
LocationPolicy            :
ClientPolicy              :
ClientVersionPolicy       :
ArchivingPolicy           :
ExchangeArchivingPolicy   : Uninitialized
PinPolicy                 :
ExternalAccessPolicy      :
MobilityPolicy            :
PersistentChatPolicy      :
UserServicesPolicy        :
HostedVoiceMail           :
HostedVoicemailPolicy     :
HostingProvider           : SRV:
RegistrarPool             : pool02.contoso.net
Enabled                   : True
SipAddress                : sip:david@contoso.net
LineURI                   :
EnterpriseVoiceEnabled    : False
ExUmEnabled               : False
HomeServer                : CN=Lc Services,CN=Microsoft,CN=1:6,CN=Pools,CN=RTC Se
                            rvice,CN=Services,CN=Configuration,DC=contoso,DC=net
DisplayName               : David Pelton
SamAccountName            : david


PS C:\> _
```

Note:
For details about the **Get-CsUser** cmdlet, run: **Get-Help Get-CsUser –Detailed**

1.6.2.7.3 Move Multiple Users to the Pilot Pool

Move Multiple Users to the Pilot Pool

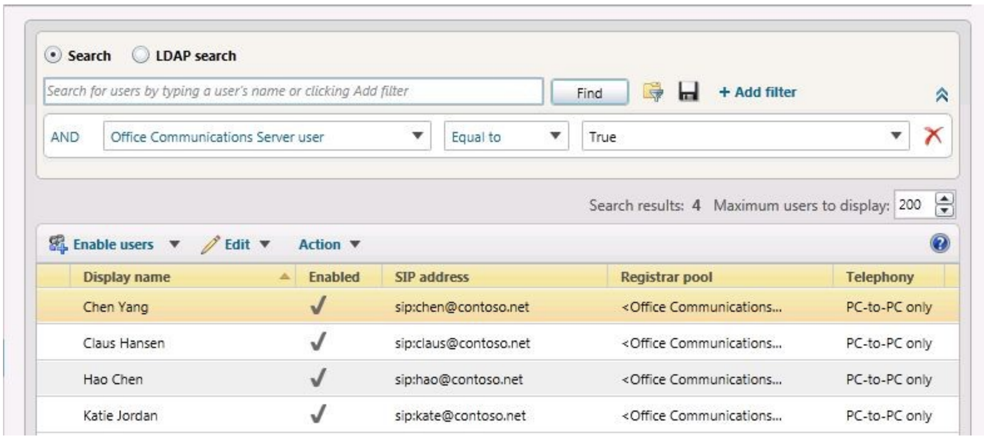
Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 6: Move users to the Pilot Pool >

Topic Last Modified: *2012-10-02*

You can move multiple users from your Office Communications Server 2007 R2 pool to your Lync Server 2013 pilot pool using Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

To move multiple users by using the Lync Server 2013 Control Panel

1. Open **Lync Server Control Panel**.
2. From the **User Search** tab, click the **Search** button.
3. Next, click **Add Filter**.
4. Create a filter where **Office Communications Server user** is equal to **True**.
5. Click **Find** to search for legacy Office Communications Server 2007 R2 users.
6. Select two users that you want to move to the Lync Server 2013 pool. In this example, we will move users Chen Yang and Claus Hansen.

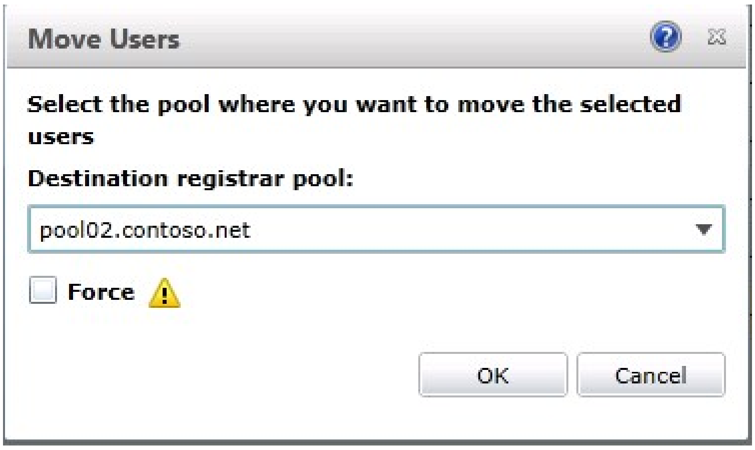


AND | Office Communications Server user ▼ | Equal to ▼ | True ▼

Search results: 4 Maximum users to display: 200

Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	<Office Communications...	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	<Office Communications...	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	<Office Communications...	PC-to-PC only
Katie Jordan	✓	sip:kate@contoso.net	<Office Communications...	PC-to-PC only

7. From the **Action** menu, select **Move selected users to pool**.
8. From the drop-down list, select the Lync Server 2013 pool.
9. Click **Action** and then click **Move selected users to pool**. Click OK.



Move Users

Select the pool where you want to move the selected users

Destination registrar pool:

pool02.contoso.net

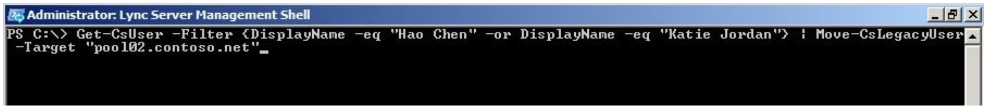
□ Force

10. Verify that the **Registrar pool** column for the users now contains the Lync Server 2013 pool, which indicates that the users have been successfully moved.

To move multiple users by using the Lync Server 2013 Management Shell

1. Open the Lync Server 2013 Management Shell.
2. At the command line, type the following and replace **User1** and **User2** with specific user names you want to move and replace **pool_FQDN** with the name of the destination pool. In this example we will move users Hao Chen and Katie Jordan.

```
Get-CsUser -Filter {DisplayName -eq "User1" -or DisplayName - eq "User
```

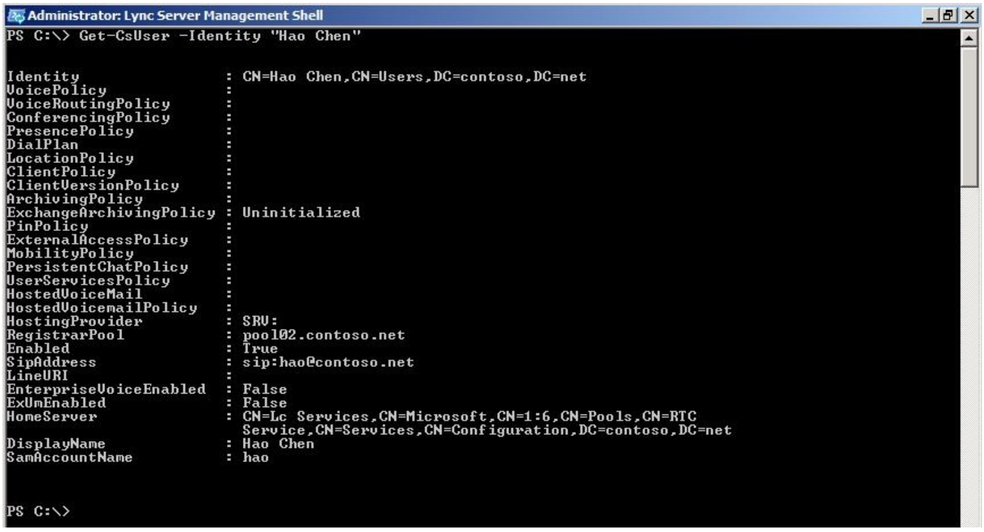


```
PS C:\> Get-CsUser -Filter {DisplayName -eq "Hao Chen" -or DisplayName -eq "Katie Jordan"} | Move-CsLegacyUser
 -Target "pool02.contoso.net"_
```

3. At the command line, type the following

```
Get-CsUser -Identity "User1"
```

4. The **Registrar Pool** identity should now point to the pool you specified as **pool_FQDN** in the previous step. The presence of this identity confirms that the user has been successfully moved. Repeat step to verify **User2** has been moved.



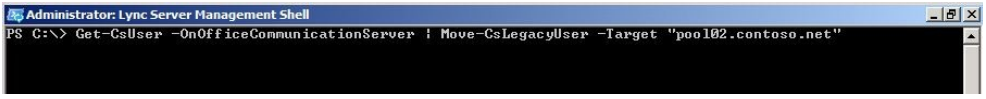
```
PS C:\> Get-CsUser -Identity "Hao Chen"


Identity                  : CN=Hao Chen,CN=Users,DC=contoso,DC=net
VoicePolicy               :
VoiceRoutingPolicy        :
ConferencingPolicy        :
PresencePolicy            :
DialPlan                  :
LocationPolicy            :
ClientPolicy              :
ClientVersionPolicy       :
ArchivingPolicy           :
ExchangeArchivingPolicy   : Uninitialized
PinPolicy                 :
ExternalAccessPolicy      :
MobilityPolicy            :
PersistentChatPolicy      :
UserServicesPolicy        :
HostedVoiceMail           :
HostedVoicemailPolicy     :
HostingProvider           : SRV:
RegistrarPool             : pool02.contoso.net
Enabled                   : True
SipAddress                : sip:hao@contoso.net
LineURI                   :
EnterpriseVoiceEnabled    : False
ExUmEnabled               : False
HomeServer                : CN=Lc Services,CN=Microsoft,CN=1:6,CN=Pools,CN=RTC
                            Service,CN=Services,CN=Configuration,DC=contoso,DC=net
DisplayName               : Hao Chen
SamAccountName            : hao



PS C:\>
```

To move all users at the same time by using the Lync Server 2013 Management Shell

In this example, all users have been returned to the Office Communications Server 2007 R2 pool (pool01.contoso.net). Using the Lync Server 2013 Management Shell, we will move all users at the same time to the Lync Server 2013 pool (pool02.contoso.net).

1. Open the **Lync Server 2013 Management Shell**.
2. At the command line, type the following:

```
Get-CsUser -OnOfficeCommunicationServer | Move-CsLegacyUser -Target "p
```

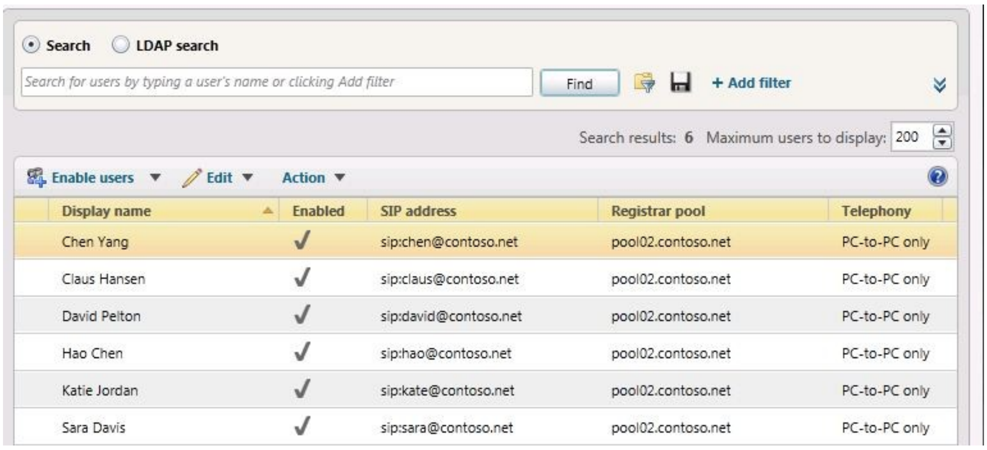


```
PS C:\> Get-CsUser -OnOfficeCommunicationServer | Move-CsLegacyUser -Target "pool02.contoso.net"
```

3. Next, run **Get-CsUser** for one of the pilot users.

```
Get-CsUser -Identity "Hao Chen"
```

4. The **Registrar Pool** identity for each user now points to the pool you specified as "pool_FQDN" in the previous step. The presence of this identity confirms that the user has been successfully moved.
5. Additionally, we can view the list of users in the Lync Server 2013 Control Panel and verify that the Registrar Pool value now points to the Lync Server 2013 pool.


● Search ○ LDAP search
Search for users by typing a user's name or clicking Add filter
Find
+ Add filter
Enable users
Edit
Action

Search results: 6 Maximum users to display: 200

Display name	Enabled	SIP address	Registrar pool	Telephony
Chen Yang	✓	sip:chen@contoso.net	pool02.contoso.net	PC-to-PC only
Claus Hansen	✓	sip:claus@contoso.net	pool02.contoso.net	PC-to-PC only
David Pelton	✓	sip:david@contoso.net	pool02.contoso.net	PC-to-PC only
Hao Chen	✓	sip:hao@contoso.net	pool02.contoso.net	PC-to-PC only
Katie Jordan	✓	sip:kate@contoso.net	pool02.contoso.net	PC-to-PC only
Sara Davis	✓	sip:sara@contoso.net	pool02.contoso.net	PC-to-PC only

1.6.2.8 Phase 7: Add Lync Server 2013 Edge Server to Pilot Pool

Phase 7: Add Lync Server 2013 Edge Server to Pilot Pool

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-09-26*

The topics in this section explain how to add a Lync Server 2013 Edge Server to the pilot pool deployment. The topics provide configuration and verification guidance when running the **Deploy New Edge pool** wizards.

In This Section

- Deploy Pilot Edge Server
- Validate Replication of Configuration Settings

1.6.2.8.1 Deploy Pilot Edge Server

Deploy Pilot Edge Server

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 7: Add Lync Server 2013 Edge Server to Pilot Pool >

Topic Last Modified: *2012-10-19*

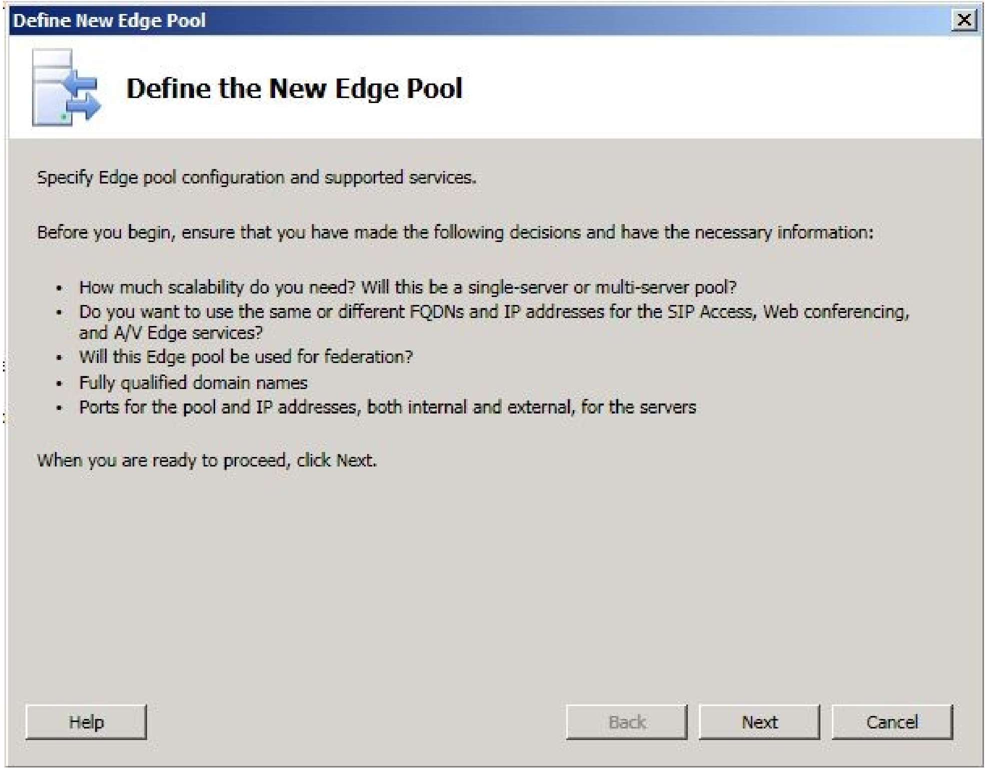
This topic highlights configuration settings you should be aware of prior to deploying your Lync Server 2013 Edge Server. This section only highlights key points you should consider as part of your pilot Edge pool deployment. For detailed steps, see Deploying External User Access in the Deployment documentation, which describes the deployment process and also gives configuration information for external user access.

As you navigate through the **Define New Edge Pool** wizard, review the key configuration settings shown in the following steps. Note that only a few pages of the **Define New Edge Pool** wizard are shown.

Define an Edge Pool

1. Open the pilot pool topology using Topology Builder.
2. Navigate to the Lync Server 2013 node. Right-click **Edge pools**, and click **New**

Edge pool.



Define the New Edge Pool

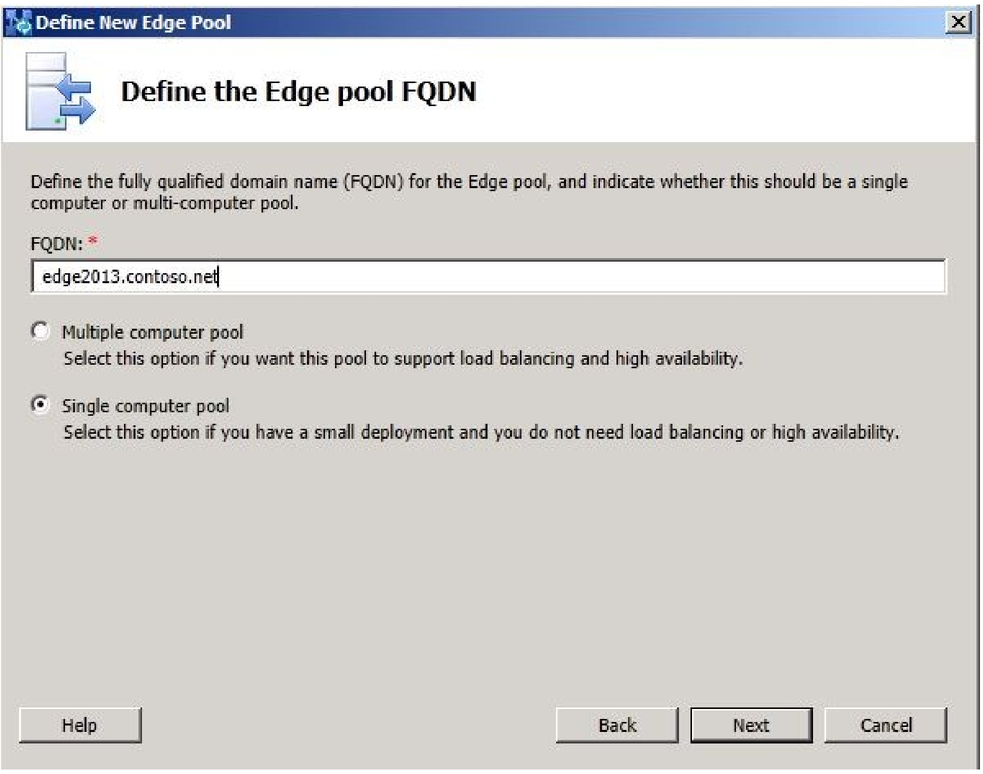
Specify Edge pool configuration and supported services.

Before you begin, ensure that you have made the following decisions and have the necessary information:

- How much scalability do you need? Will this be a single-server or multi-server pool?
- Do you want to use the same or different FQDNs and IP addresses for the SIP Access, Web conferencing, and A/V Edge services?
- Will this Edge pool be used for federation?
- Fully qualified domain names
- Ports for the pool and IP addresses, both internal and external, for the servers

When you are ready to proceed, click Next.

3. An Edge pool can be a **Multiple computer pool** or **Single computer pool**.



Define the Edge pool FQDN

Define the fully qualified domain name (FQDN) for the Edge pool, and indicate whether this should be a single computer or multi-computer pool.

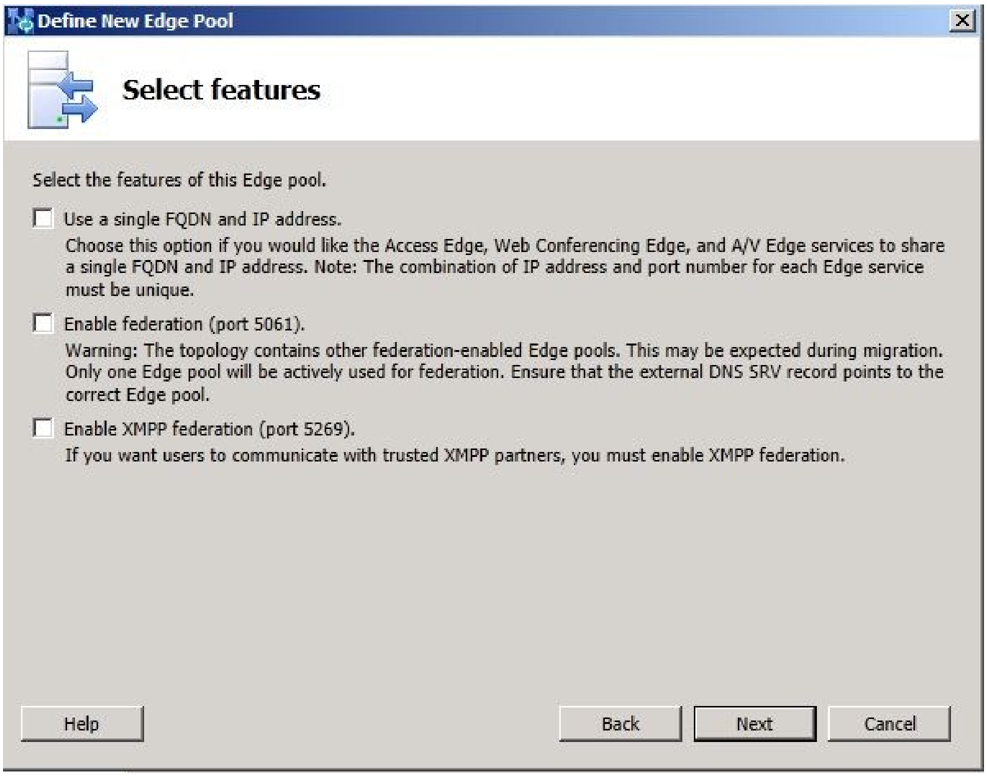
FQDN: *

edge2013.contoso.net

○ Multiple computer pool
Select this option if you want this pool to support load balancing and high availability.

● Single computer pool
Select this option if you have a small deployment and you do not need load balancing or high availability.

4. On the **Select features** page, do not enable federation or XMPP federation. Federation and XMPP federation are currently routed through the legacy Office Communications Server 2007 R2 Edge Server. These features will be configured in a later phase of migration.



Select features

Select the features of this Edge pool.

☐ Use a single FQDN and IP address.

Choose this option if you would like the Access Edge, Web Conferencing Edge, and A/V Edge services to share a single FQDN and IP address. Note: The combination of IP address and port number for each Edge service must be unique.

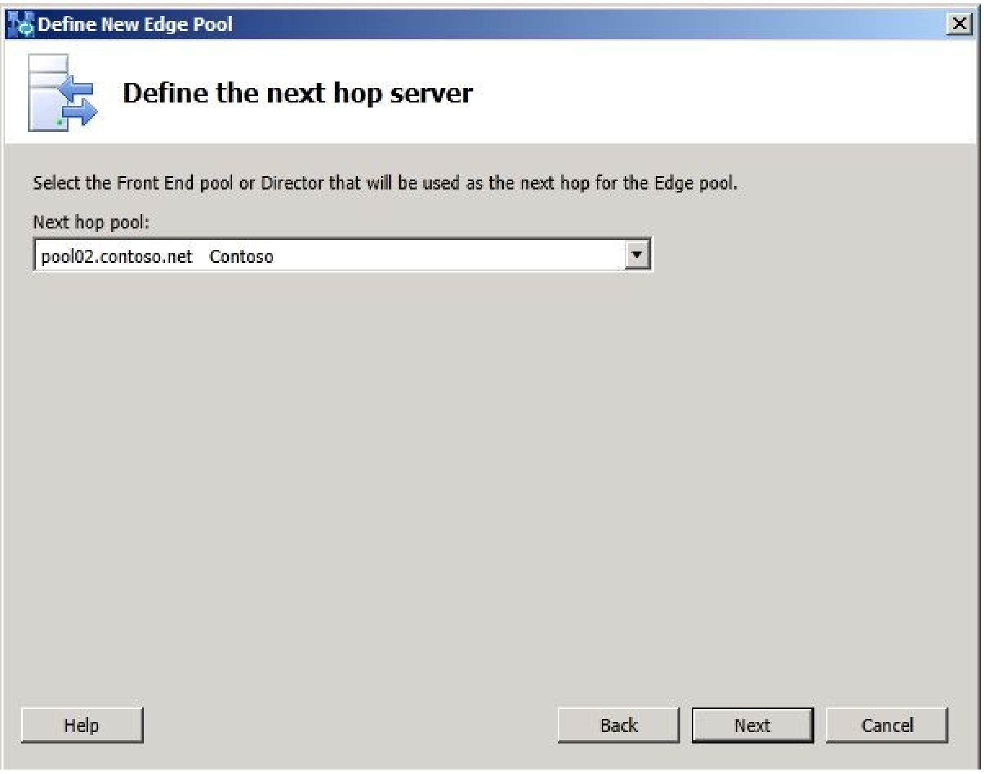
☐ Enable federation (port 5061).

Warning: The topology contains other federation-enabled Edge pools. This may be expected during migration. Only one Edge pool will be actively used for federation. Ensure that the external DNS SRV record points to the correct Edge pool.

☐ Enable XMPP federation (port 5269).

If you want users to communicate with trusted XMPP partners, you must enable XMPP federation.

5. Next, continue completing the following wizard pages: **Select IP options**, **External FQDNs**, **Define the internal IP address**, and **Define the external IP address**.
6. On the **Define the next hop** page, select the Director for the next hop of the Lync Server 2013 Edge pool.



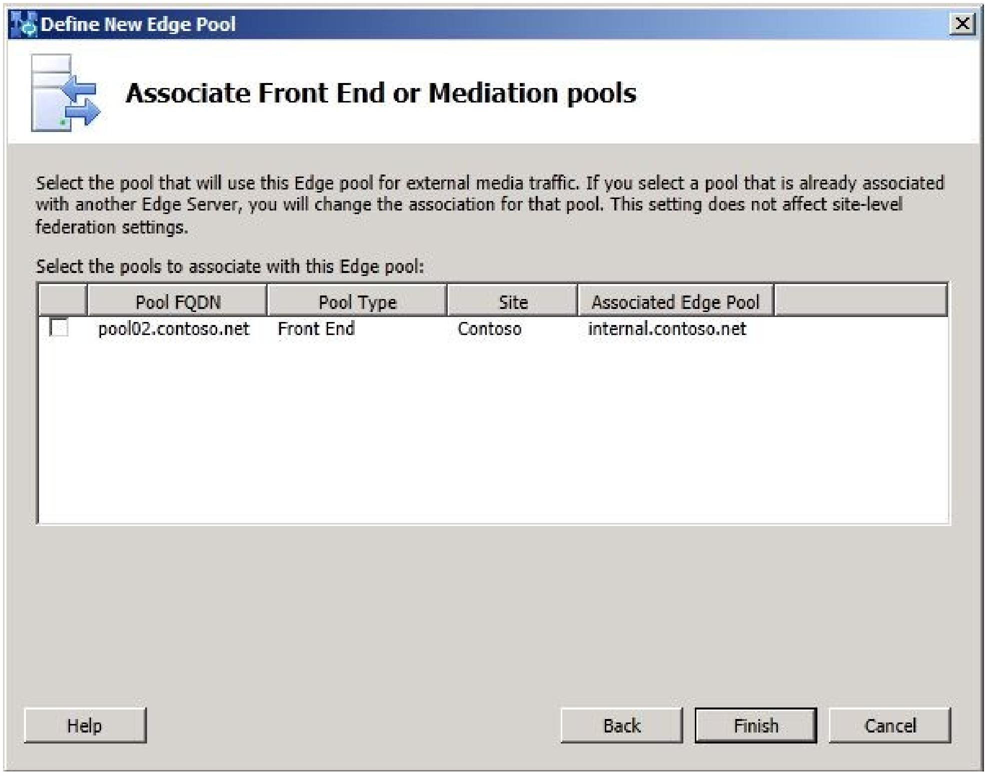
Define the next hop server

Select the Front End pool or Director that will be used as the next hop for the Edge pool.

Next hop pool:

pool02.contoso.net Contoso

7. On the **Associate Front End pools** page, do not associate a pool with this Edge pool at this time. External media traffic is currently routed through the legacy Office Communications Server 2007 R2 Edge Server. This setting will be configured in a later phase of migration.



Define New Edge Pool

Associate Front End or Mediation pools

Select the pool that will use this Edge pool for external media traffic. If you select a pool that is already associated with another Edge Server, you will change the association for that pool. This setting does not affect site-level federation settings.

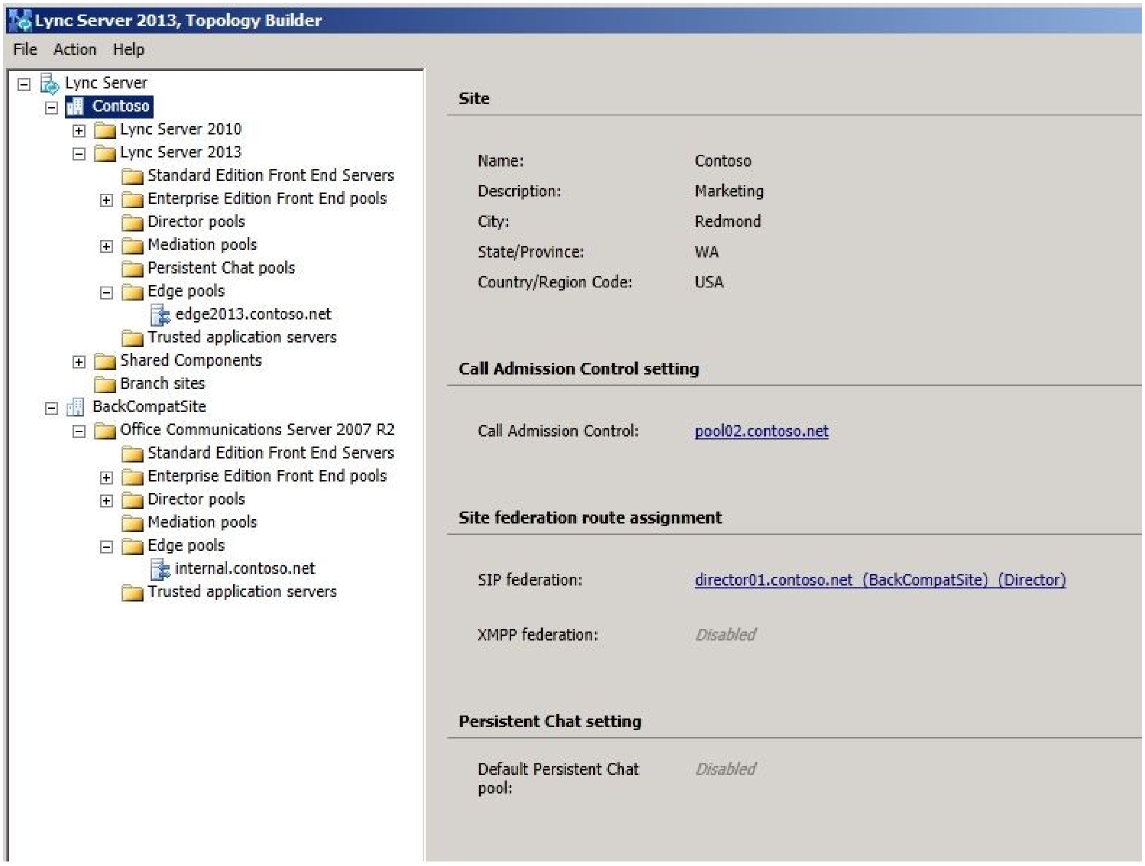
Select the pools to associate with this Edge pool:

	Pool FQDN	Pool Type	Site	Associated Edge Pool
□	pool02.contoso.net	Front End	Contoso	internal.contoso.net

8. Click **Finish** and then **Publish** the topology.
9. Follow the steps in Install Edge Servers in the Deployment documentation to install the files on the new Edge Server, configure certificates, and start the services.

It’s very important that you follow the guidelines in the topics Deploying External User Access in the Deployment documentation. This section merely provided some guidance on configuration settings when installing these server roles.

You should now have a legacy Office Communications Server 2007 R2 Edge server deployment, indicated by the presence of the BackCompatSite, in parallel with a Lync Server 2013 Edge server deployment. Federation is configured to use the Office Communications Server 2007 R2 Director. Verify that both deployments are running properly, services are started, and you can administer each deployment prior to moving to the next phase.


Lync Server 2013, Topology Builder
File
Action
Help
Lync Server
Contoso
Lync Server 2010
Lync Server 2013
Standard Edition Front End Servers
Enterprise Edition Front End pools
Director pools
Mediation pools
Persistent Chat pools
Edge pools
edge2013.contoso.net
Trusted application servers
Shared Components
Branch sites
BackCompatSite
Office Communications Server 2007 R2
Standard Edition Front End Servers
Enterprise Edition Front End pools
Director pools
Mediation pools
Edge pools
internal.contoso.net
Trusted application servers

Site

Name:	Contoso
Description:	Marketing
City:	Redmond
State/Province:	WA
Country/Region Code:	USA

Call Admission Control setting

Call Admission Control:	pool02.contoso.net

Site federation route assignment

SIP federation:	director01.contoso.net (BackCompatSite) (Director)
XMPP federation:	Disabled

Persistent Chat setting

Default Persistent Chat pool:	Disabled

1.6.2.8.2 Validate Replication of Configuration Settings

Validate Replication of Configuration Settings

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 7: Add Lync Server 2013 Edge Server to Pilot Pool >

Topic Last Modified: *2012-10-19*

You can validate the replication of configuration information to the Edge Server by running the Lync Server 2013 **Get-CsManagementStoreReplicationStatus** cmdlet on the internal computer on which the Central Management store is located or any domain joined computer on which Lync Server 2013 Core Components is installed.

Initial results may indicate the status as "False" instead of "True" for replication. If so, run the **Invoke-CsManagementStoreReplication** cmdlet and allow time for the replication to complete before running the **Get-CsManagementStoreReplicationStatus** cmdlet again.

1.6.2.9 Phase 8: Move from Pilot Deployment into Production

Phase 8: Move from Pilot Deployment into Production

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-10-15*

The topics in this section describe tasks you must complete prior to moving your deployment of Lync Server 2013 from a pilot deployment to a production-level deployment.

- Configure Federation Routes and Media Traffic
- Move Remaining Users to Lync Server 2013
- Configure XMPP Gateway on Lync Server 2013

1.6.2.9.1 Configure Federation Routes and Media Traffic

Configure Federation Routes and Media Traffic

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 8: Move from Pilot Deployment into Production >

Topic Last Modified: *2012-10-16*

Federation is a trust relationship between two or more SIP domains that permits users in separate organizations to communicate across network boundaries. After you migrate to your Lync Server 2013 pilot pool, you need to transition from the federation route of your Microsoft Office Communications Server 2007 R2 Edge Servers to the federation route of your Lync Server 2013 Edge Servers.

Use the procedures that follow to transition the federation route and the media traffic route from your Office Communications Server 2007 R2 Edge Server and Director to your Lync Server 2013 Edge Server, for a single-site deployment.

Important:

Changing the federation route and media traffic route requires that you schedule maintenance downtime for the Lync Server 2013 and Office Communications Server 2007 R2 Edge Servers. This entire transition process also means that federated access will be unavailable for the duration of the outage. You should schedule the downtime for a time when you expect minimal user activity. You should also provide sufficient notification to your end users. Plan accordingly for this outage and set appropriate expectations within your organization.

Important:

If your legacy Office Communications Server 2007 R2 Edge Server is configured to use the same FQDN for the Access Edge service, Web Conferencing Edge service, and the A/V Edge service, the procedures in this section to transition the federation setting to a Lync Server 2013 Edge Server are not supported. If the legacy Edge services are configured to use the same FQDN, you must first migrate all your users from Office Communications Server 2007 R2 to Lync Server 2013, then decommission the Office Communications Server 2007 R2 Edge Server before enabling federation on the Lync Server 2013 Edge Server. For details, see the following topics:

- Move Remaining Users to Lync Server 2013
- "Remove Servers and Server Roles" at http://go.microsoft.com/fwlink/p/?LinkId=268790

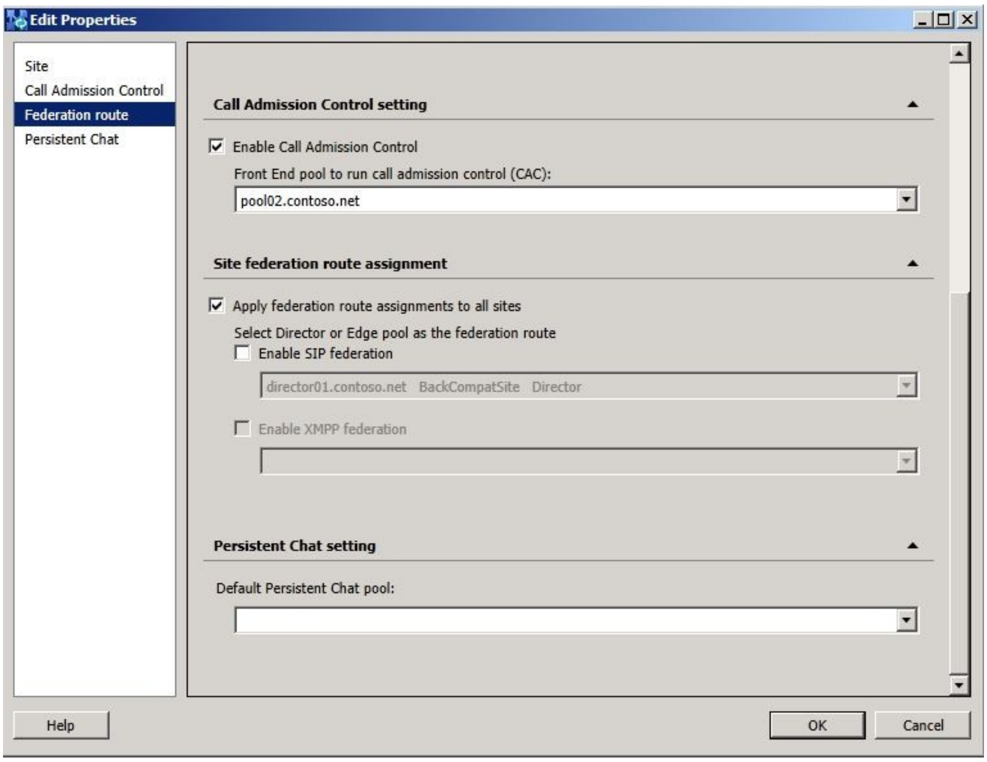
Important:

If your XMPP federation is routed through a Lync Server 2013 Edge Server, legacy Office Communications Server 2007 R2 users will not be able to communicate with the XMPP federated partner until all users have been moved to Lync Server 2013, XMPP policies and certificates have been configured, the XMPP federated partner has been configured on Lync Server 2013, and lastly the DNS entries have been updated.

To successfully publish, enable, or disable a topology when adding or removing a server role, you should be logged in as a user who is a member of the RTCUniversalServerAdmins and Domain Admins groups. It is also possible to delegate the proper user rights and permissions for adding server roles. For details, see Delegate Setup Permissions in the Standard Edition server or Enterprise Edition server Deployment documentation. For other configuration changes, only membership in the RTCUniversalServerAdmins group is required.

⊟To remove the legacy federation association from Lync Server 2013 sites

1. Open the pilot pool topology using Topology Builder.
2. In the left pane, navigate to the site node.
3. Right-click the site, and then click **Edit Properties**.
4. Select **Federation route** in the left pane.
5. Under Site federation route assignment, clear the check box next to **Enable SIP federation** to disable the federation route through the **BackCompatSite**.



Call Admission Control setting

☑ Enable Call Admission Control

Front End pool to run call admission control (CAC): pool02.contoso.net

Site federation route assignment

☑ Apply federation route assignments to all sites

Select Director or Edge pool as the federation route

☐ Enable SIP federation

director01.contoso.net BackCompatSite Director

☐ Enable XMPP federation

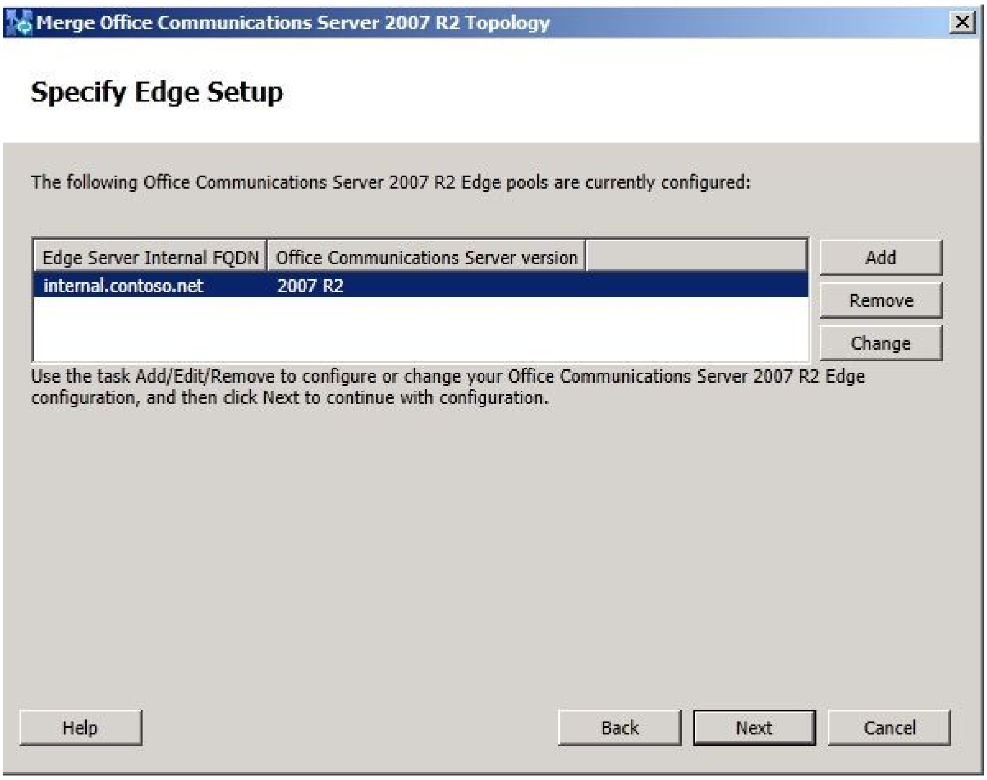
Persistent Chat setting

Default Persistent Chat pool:

6. Click **OK** to close the Edit Properties page.
7. From **Topology Builder**, select the top node **Lync Server**.
8. From the **Action** menu, click **Publish Topology** and complete the wizard.

⊟To configure the legacy Edge Server as a non-federating Edge Server

1. From **Topology Builder**, from the **Action** menu click **Merge Office Communications Server 2007 R2 Topology**.
2. Click **Next** to continue.
3. On the **Specify Edge Setup**, select the **Edge Server Internal FQDN** that is currently configured for federation, and then click **Change**.



Merge Office Communications Server 2007 R2 Topology

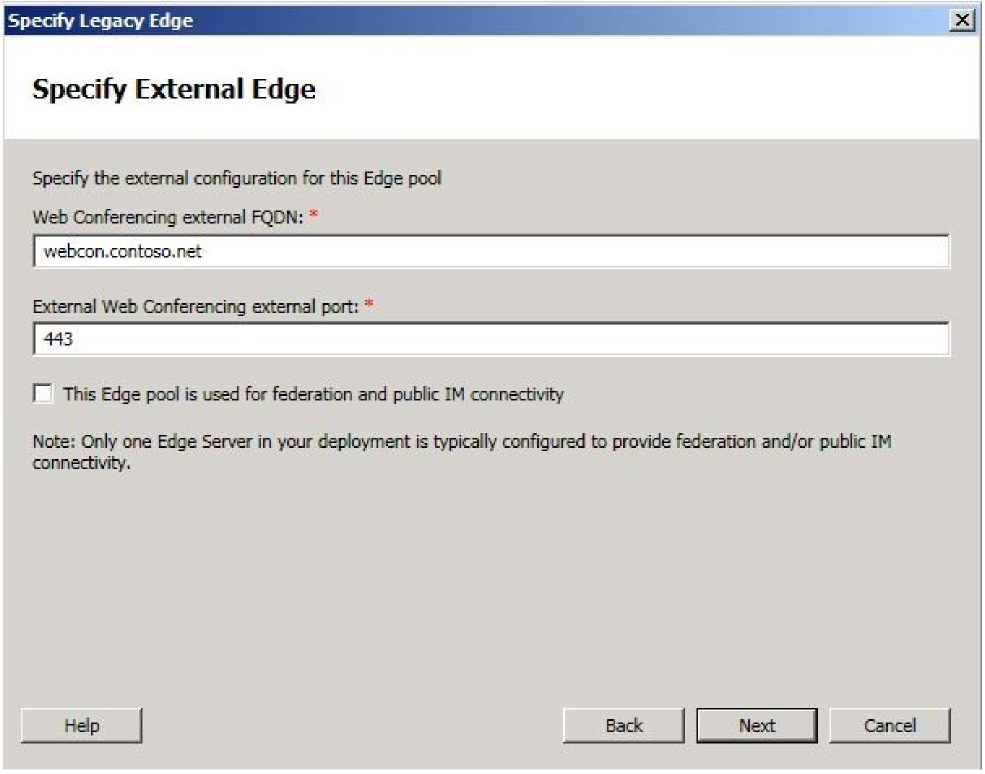
Specify Edge Setup

The following Office Communications Server 2007 R2 Edge pools are currently configured:

Edge Server Internal FQDN	Office Communications Server version
internal.contoso.net	2007 R2

Use the task Add/Edit/Remove to configure or change your Office Communications Server 2007 R2 Edge configuration, and then click Next to continue with configuration.

4. Click **Next** and accept the default settings until you get to the **Specify External Edge** page:



Specify Legacy Edge

Specify External Edge

Specify the external configuration for this Edge pool

Web Conferencing external FQDN: *
webcon.contoso.net

External Web Conferencing external port: *
443

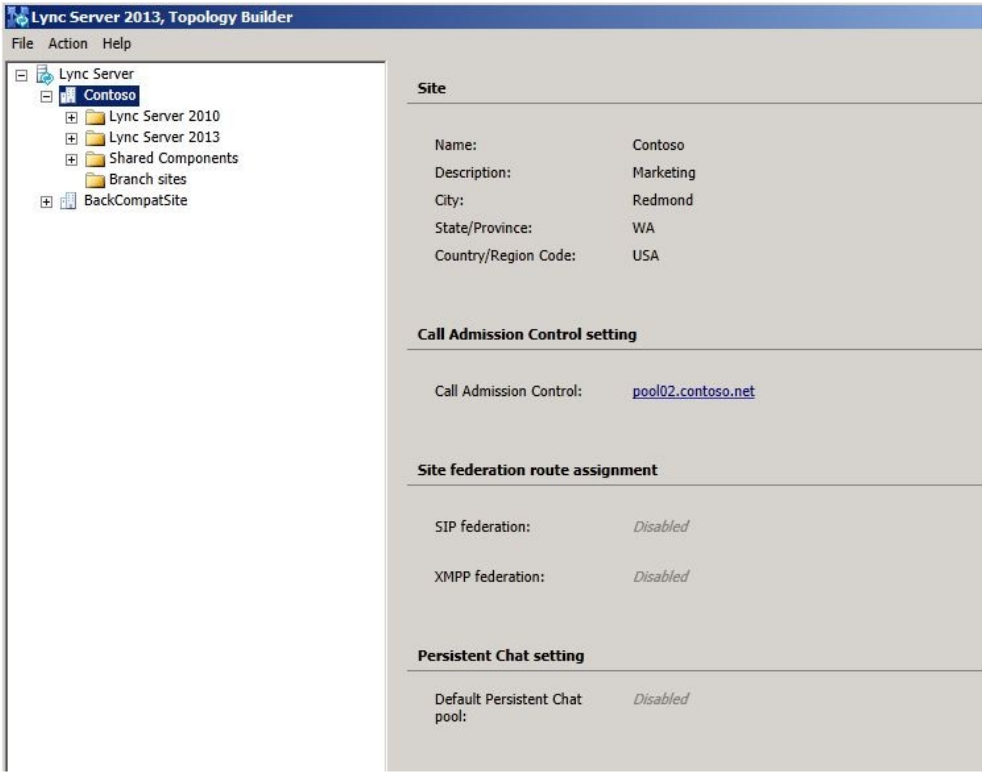
☐ This Edge pool is used for federation and public IM connectivity

Note: Only one Edge Server in your deployment is typically configured to provide federation and/or public IM connectivity.

5. In **Specify External Edge**, clear the **This Edge pool is used for federation and public IM connectivity** check box. This will remove the federation association with the BackCompatSite.

Important:
This step is important. You must clear this option to remove the legacy federation association.

6. Click **Next** and accept the default settings of the remaining pages of the wizard.
7. In **Summary**, click **Next** to begin merging the topologies.
8. In the **Status** column, verify that the value is **Success**, and then click **Finish** to close the wizard.
9. From the **Action** menu, select **Publish Topology**, and then click **Next**.
10. When the **Publishing wizard** completes, click **Finish** to close the wizard.



Site

Name: Contoso
Description: Marketing
City: Redmond
State/Province: WA
Country/Region Code: USA

Call Admission Control setting

Call Admission Control: pool02.contoso.net

Site federation route assignment

SIP federation: *Disabled*

XMPP federation: *Disabled*

Persistent Chat setting

Default Persistent Chat pool: *Disabled*

As shown in the previous figure, the **SIP federation** located under **Site federation route assignment** is set to **Disabled**.

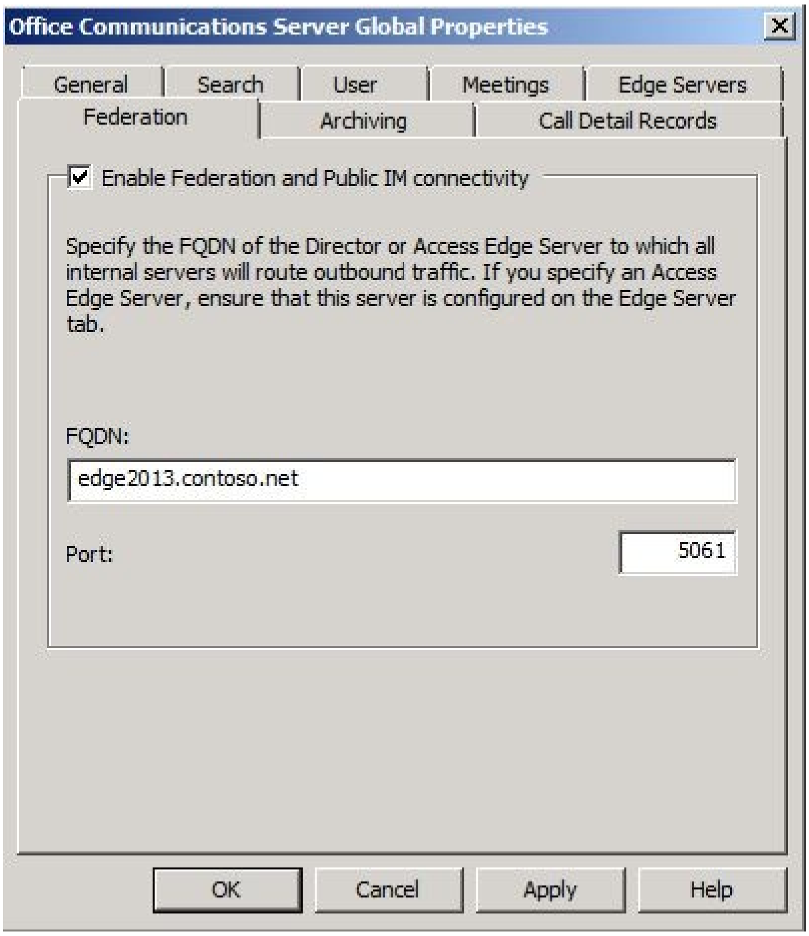
To configure certificates on the Lync Server 2013 Edge Server

1. Export the external Access Proxy certificate, with the private key, from the legacy Office Communications Server 2007 R2 Edge Server.
2. On the Lync Server 2013 Edge Server, import the Access Proxy external certificate from the previous step.
3. Assign the Access Proxy external certificate to the Lync Server 2013 external interface of the Edge Server.
4. The internal interface certificate of the Lync Server 2013 Edge Server should not be changed.

To change Office Communications Server 2007 R2 federation route to use Lync Server 2013 Edge Server

1. On the Office Communications Server 2007 R2 Standard Edition server or Front End Server, open the Office Communications Server 2007 R2 Administrative tool.
2. In the left pane, expand the top node, and then right-click the **Forest** node. Select **Properties**, and then click **Global Properties**.
3. Click the **Federation** tab.

4. Select the check box to enable federation and Public IM connectivity.
5. Enter the FQDN of the Lync Server 2013 Edge Server, and then click **OK**.



Office Communications Server Global Properties

☑ Enable Federation and Public IM connectivity

Specify the FQDN of the Director or Access Edge Server to which all internal servers will route outbound traffic. If you specify an Access Edge Server, ensure that this server is configured on the Edge Server tab.

FQDN: edge2013.contoso.net

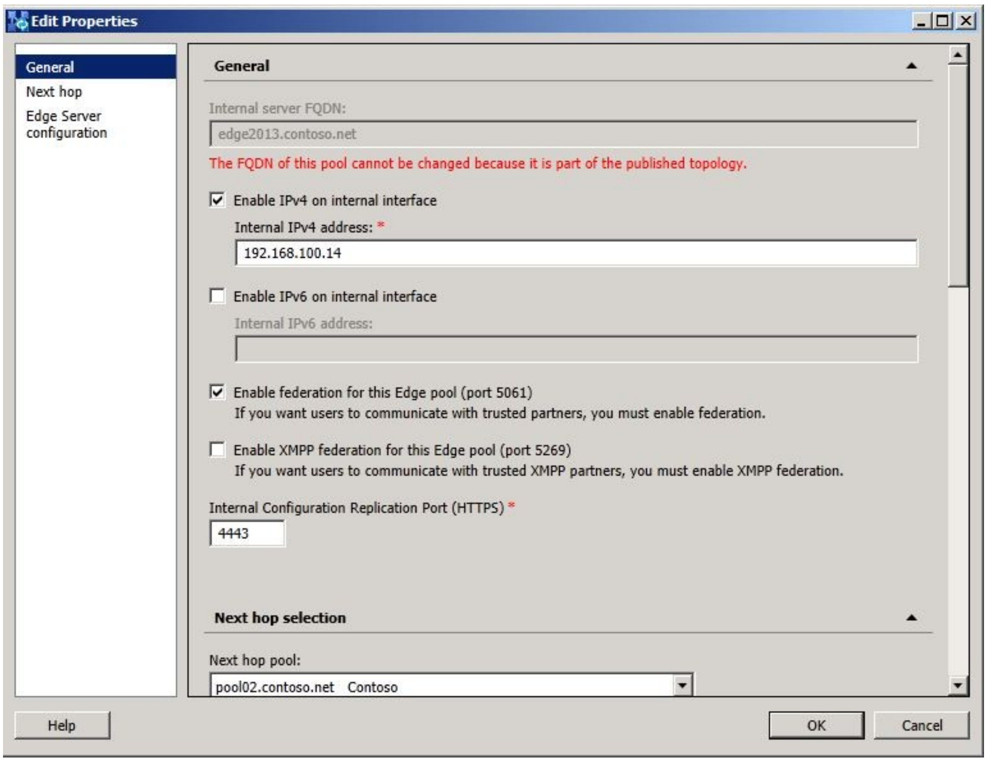
Port: 5061

⊟To turn on Lync Server 2013 Edge Server federation

1. From Topology Builder, in the left pane, navigate to the Lync Server 2013 **Edge pools** node.
2. Expand the node, right-click the Edge Server listed, and then click **Edit Properties**.

Note:
Federation can only be enabled for a single Edge pool. If you have multiple Edge pools, select one to use as the federating Edge pool.

3. On the **General** page, select the **Enable federation for this Edge pool (Port 5061)** check box.



Edit Properties

General

Internal server FQDN:
edge2013.contoso.net

The FQDN of this pool cannot be changed because it is part of the published topology.

☑ Enable IPv4 on internal interface

Internal IPv4 address: *
192.168.100.14

□ Enable IPv6 on internal interface

Internal IPv6 address:

☑ Enable federation for this Edge pool (port 5061)

If you want users to communicate with trusted partners, you must enable federation.

□ Enable XMPP federation for this Edge pool (port 5269)

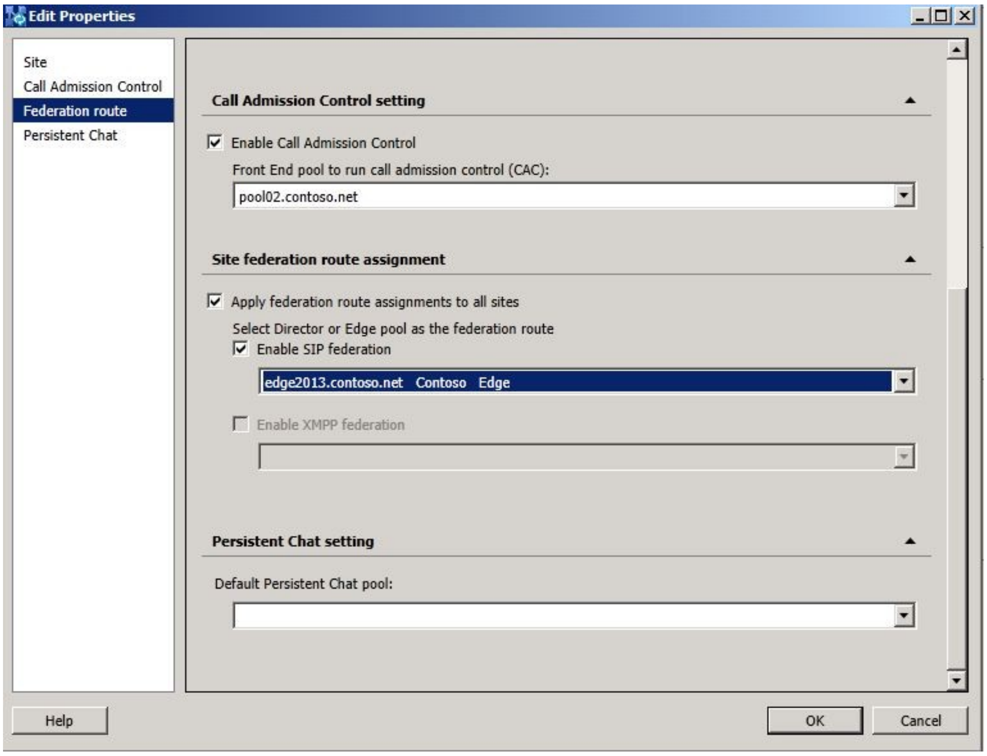
If you want users to communicate with trusted XMPP partners, you must enable XMPP federation.

Internal Configuration Replication Port (HTTPS) *
4443

Next hop selection

Next hop pool:
pool02.contoso.net Contoso

4. Click **OK** to close the Edit Properties page.
5. Next, navigate to the site node.
6. Right-click the site, and then click **Edit Properties**.
7. In the left pane, click **Federation route**.
8. Under **Site federation route assignment**, select **Enable SIP federation**, and then from the list select the Lync Server 2013 Edge Server listed.
9. Click **OK** to close the **Edit Properties** page.



Edit Properties

Call Admission Control setting

☑ Enable Call Admission Control

Front End pool to run call admission control (CAC):
pool02.contoso.net

Site federation route assignment

☑ Apply federation route assignments to all sites

Select Director or Edge pool as the federation route

☑ Enable SIP federation

edge2013.contoso.net Contoso Edge

□ Enable XMPP federation

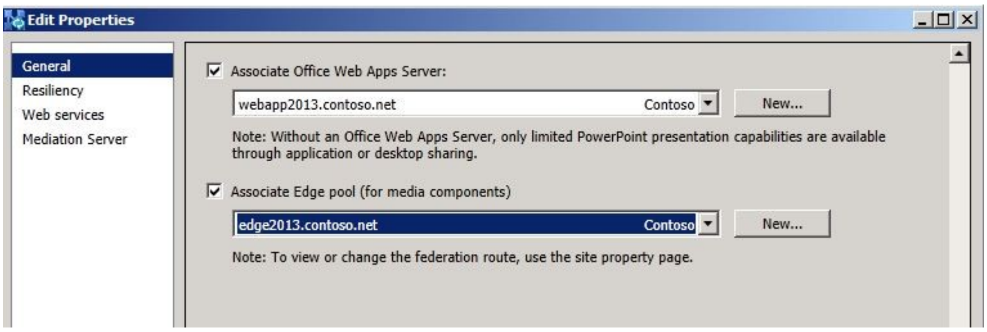
Persistent Chat setting

Default Persistent Chat pool:

For multi-site deployments, complete this procedure at each site.

To configure Lync Server 2013 Edge Server outbound media path

1. From **Topology Builder**, navigate to the Lync Server 2013 pool below **Standard Edition Front End Servers** or **Enterprise Edition Front End pools**.
2. Right-click the pool, and then click **Edit Properties**.
3. In the **Associations** section, select the **Associate Edge pool (for media components)** check box.
4. From the drop down box, select the Lync Server 2013 Edge Server.



☑ Associate Office Web Apps Server:

webapp2013.contoso.net Contoso

Note: Without an Office Web Apps Server, only limited PowerPoint presentation capabilities are available through application or desktop sharing.

☑ Associate Edge pool (for media components)

edge2013.contoso.net Contoso

Note: To view or change the federation route, use the site property page.

5. Click **OK** to close the **Edit Properties** page.

To publish Edge Server configuration changes

1. From **Topology Builder**, select the top node **Lync Server**.
2. From the **Action** menu, select **Publish Topology** and complete the wizard.
3. Wait for Active Directory replication to occur to all pools in the deployment.

> **Note:**
>
> You may see the following message:
> **Warning: The topology contains more than one Federated Edge Server. This can occur during migration to a more recent version of the product. In that case, only one Edge Server would be actively used for federation. Verify that the external DNS SRV record points to the correct Edge Server. If you want to deploy multiple federation Edge Server to be active concurrently (that is, not a migration scenario), verify that all federated partners are using Office Communications Server 2007 R2 or Lync Server. Verify that the external DNS SRV record lists all federation enabled Edge Servers.**
> This warning is expected and can be safely ignored.

To verify federation and remote access for external users

1. From the Lync Server 2013 Front End Server, open the Lync Server Management Shell.
2. To verify the status of federation and remote access, from the command line, type the following:

```
Get-CsAccessEdgeConfiguration
```

3. To enable federation and remote access, from the command line, type the following:

```
Set-CsAccessEdgeConfiguration
```

   For more information on these cmdlets, see the following topics: Get-CsAccessEdgeConfiguration and Set-CsAccessEdgeConfiguration.
4. Wait until replication has completed before bringing the Lync Server 2013 Edge servers online, and testing federation and external access.

To configure Lync Server 2013 Edge Server

1. Bring all of the Lync Server 2013 Edge Servers online.

2. Update the external firewall routing rules or the hardware load balancer settings to send SIP traffic for external access (usually port 443) and federation (usually port 5061) to the Lync Server 2013 Edge Server, instead of the legacy Edge Server.

Note:
If you do not have a hardware load balancer, you need to update the DNS A record for federation to resolve the new Lync Server Access Edge server. To accomplish this with minimum disruption, reduce the TTL value for the external Lync Server Access Edge FQDN so that when DNS is updated to point to the new Lync Server Access Edge server, federation and remote access will be updated quickly.

3. Next, stop the **Lync Server Server Access Edge** from each Edge Server computer.
4. From each legacy Edge Server computer, open the **Services** applet from the **Administrative Tools**.
5. In the services list, find **Office Communications Server Access Edge**.
6. Right-click the services name, and then select **Stop** to stop the service.
7. Set the Startup type to **Disabled**.
8. Click **OK** to close the **Properties** window.

⊟To Test Connectivity of External Users and External access

- Users from at least one federated domain, an internal user on Lync Server 2013 and a user on Office Communications Server 2007 R2. Test instant messaging (IM), presence, audio/video (A/V), and desktop sharing.
- Users of each public IM service provider that your organization supports (and for which provisioning has been completed) communicating with a user on Lync Server 2013 and a user on Office Communications Server 2007 R2.
- Verify anonymous users are able to join conferences.
- A user hosted on Office Communications Server 2007 R2 using remote user access (logging into Office Communications Server 2007 R2 from outside the intranet but without VPN) with a user on Lync Server 2013, and a user on Office Communications Server 2007 R2. Test IM, presence, A/V, and desktop sharing.
- A user hosted on Lync Server 2013 using remote user access (logging into Lync Server 2013 from outside the intranet but without VPN) with a user on Lync Server 2013, and a user on Office Communications Server 2007 R2. Test IM, presence, A/V, and desktop sharing.

1.6.2.9.2 Move Remaining Users to Lync Server 2013

Move Remaining Users to Lync Server 2013

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 8: Move from Pilot Deployment into Production >

Topic Last Modified: *2012-09-26*

You can move users to the new Lync Server 2013 deployment by using either Lync Server Control Panel or Lync Server Management Shell. You must meet some requirements to ensure a smooth transition to Lync Server 2013. For details about prerequisites to completing the procedures in this topic, see Configure Clients for Migration. For detailed steps about moving users, see Phase 6: Move users to the Pilot Pool.

Important:
You cannot use the Active Directory Users and Computers snap-in or the Microsoft Office Communications Server 2007 R2 administrative tools to move users from your legacy environment to Lync Server 2013.

Important:

The **Move-CsLegacyUser** cmdlet requires that user names are properly formed and do not have leading or trailing spaces. You cannot move a user account using the **Move-CsLegacyUser** cmdlet if it contains leading or trailing spaces.

When you move a user to an Lync Server 2013 pool, the data for the user is moved to the back-end database that is associated with the new pool.

Important:

This includes the active meetings created by the legacy user. For example, if a legacy user has configured a **my meeting** conference, that conference will still be available in the new Lync Server 2013 pool, after the user has been moved. The details to access that meeting will still be the same **conference URL and conference ID**. The only difference is that the conference is now hosted in the Lync Server 2013 pool, and not in Office Communications Server 2007 R2 pool.

Note:

Homing users on Lync Server 2013 does not require that you deploy upgraded clients at the same time. New functionality will be available to users only when they have upgraded to the new client software.

⊟Post Migration Task

1. After you move users, verify the conferencing policy that is assigned to them.
2. To ensure that meetings organized by users homed on Lync Server 2013 work seamlessly with federated users who are homed on Office Communications Server 2007 R2, the conferencing policy assigned to the migrated users should allow anonymous participants.
3. Conferencing policies that allow anonymous participants have **Allow participants to invite anonymous users** selected in Lync Server 2013 Control Panel and have **AllowAnonymousParticipantsInMeetings** set to **True** in the output from the **Get-CsConferencingPolicy** cmdlet in the Lync Server Management Shell.
4. For details about configuring conferencing policy by using Lync Server Management Shell, see Set-CsConferencingPolicy in the Lync Server Management Shell documentation.

1.6.2.9.3 Configure XMPP Gateway on Lync Server 2013

Configure XMPP Gateway on Lync Server 2013

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 8: Move from Pilot Deployment into Production >

Topic Last Modified: *2012-10-19*

When you configure policies for support of extensible messaging and presence protocol (XMPP) federated partners, the policies apply to users of XMPP federated domains, but not to users of session initiation protocol (SIP) instant messaging (IM) service providers (for example, Windows Live), or SIP federated domains. You configure an XMPP Federated Partner for each XMPP federated domain that you want to allow your users to add contacts and communicate with. Once the policies are in place, additional tasks include configuring the XMPP Gateway certificates, deploying the Lync Server 2013 XMPP Gateway, and finally updating the DNS records for the XMPP Gateway.

⊟Configure XMPP Gateway Certificates on the Lync Server 2013 Edge Server

1. On the Edge Server, in the Deployment Wizard, next to **Step 3: Request, Install, or Assign Certificates**, click **Run again**.

Tip:
If you are deploying the Edge Server for the first time, you will see Run instead of Run Again.

2. On the **Available Certificate Tasks** page, click **Create a new certificate request**.
3. On the **Certificate Request** page, click **External Edge Certificate**.
4. On the **Delayed or Immediate Request** page, select the **Prepare the request now, but send it later** check box.
5. On the **Certificate Request File** page, type the full path and file name of the file to which the request is to be saved (for example, c:\cert_exernal_edge.cer).
6. On the **Specify Alternate Certificate Template** page, to use a template other than the default WebServer template, select the **Use alternative certificate template for the selected certification authority** check box.
7. On the **Name and Security Settings** page, do the following:
   7.a. In **Friendly name**, type a display name for the certificate.
   7.b. In **Bit length**, specify the bit length (typically, the default of 2048).
   7.c. Verify that the **Mark certificate private key as exportable** check box is selected.
8. On the **Organization Information** page, type the name for the organization and the organizational unit (for example, a division or department).
9. On the **Geographical Information** page, specify the location information.
10. On the **Subject Name/Subject Alternate Names** page, the information to be automatically populated by the wizard is displayed. If additional subject alternative names are needed, you specify them in the next two steps.
11. On the **SIP Domain Setting on Subject Alternate Names (SANs)** page, select the domain check box to add a sip.<sipdomain> entry to the subject alternative names list.
12. On the **Configure Additional Subject Alternate Names** page, specify any additional subject alternative names that are required.

Tip:
If the XMPP proxy is installed, by default the domain name (such as contoso.com) is populated in the SAN entries. If you require more entries, add them in this step.

13. On the **Request Summary** page, review the certificate information to be used to generate the request.
14. After the commands finish running, you can **View Log**, or click **Next** to continue.
15. On the **Certificate Request File** page, you can view the generated certificate signing request (CSR) file by clicking View or exit the Certificate Wizard by clicking **Finish**.
16. Copy the request file and submit to your public certification authority.
17. After receiving, importing and assigning the public certificate, you must stop and restart the Edge Server services. You do this by typing in the Lync Server Management console:

```
Stop-CsWindowsService
```

```
Start-CsWindowsService
```

⊟Configure a new Lync Server 2013 XMPP Gateway

1. Open Lync Server Control Panel.
2. In the left navigation bar, click **Federation and External Access** and then click **XMPP Federated Partners**.
3. To create a new configuration, click **New**.
4. Define the following settings:
5. **Primary domain** (Required). The primary domain is the base domain of the XMPP partner. For example, you would enter **fabrikam.com** for the XMPP partner domain name. This is a required entry.

6. **Description** The description is for notes or other identifying information for this particular configuration. This entry is optional.
7. **Additional domains** Additional domains are domains that are a part of your XMPP partner's domain that should be included as part of the allowed XMPP communication. For example, if the primary domain is **fabrikam.com**, then you would list all other domains that are under fabrikam.com that you will communicate with by way of XMPP.
8. **Partner type** The **Partner type** is a required setting. You must choose one of the following to describe and enforce what contacts can be added. You can select from:
   - **Federated** A **Federated** partner type represents a high level of trust between the Lync Server deployment and the XMPP partner. This partner type is recommended for federating with XMPP servers within the same enterprise or where there is an established business relationship. XMPP contacts in Federated partners can:
     8..a.Add Lync contacts and view their presence without express authorization from the Lync user.
     8..b.Send instant messages to Lync contacts whether or not the Lync user has added them into their contact list.
     8..c.See a Lync user's status notes.
   - **Public verified** A **Public verified** partner is a public XMPP provider that is trusted to verify the identity of its users. XMPP contacts in Public Verified networks can add Lync contacts and view their presence and send instant messages to them without express authorization from the Lync users. XMPP contacts in public verified networks never see a Lync users' status notes. This setting is not recommended.
   - **Public unverified** A **Public unverified** partner is a public XMPP provider that is not trusted to verify the identity of its users. XMPP users on Public Unverified networks cannot communicate with Lync users unless the Lync user has expressly authorized them by adding them to the contact list. XMPP users on public unverified networks never see Lync users' status notes. This setting is recommended for any federation with public XMPP providers such as Google Talk.
9. **Connection Type:** Defines the various rules and dialback settings.
   - **TLS Negotiation** Defines the TLS negotiation rules. An XMPP service can require TLS, can make TLS optional, or you define that TLS is not supported. Choosing Optional leaves the requirement up to the XMPP service for a mandatory-to-negotiate decision. To view all possible settings and details for SASL, TLS and Dialback negotiation – including not valid and known error configurations - see Negotiation Settings for XMPP Federated Partners
     9..a.**Required** The XMPP service requires TLS negotiation.
     9..b.**Optional** The XMPP service indicates that TLS is mandatory-to-negotiate.
     9..c.**Not Supported** The XMPP service does not support TLS.

   - **SASL negotiation** Defines the SASL negotiation rules. An XMPP service can require SASL, can make SASL optional, or you define that SASL is not supported. Choosing Optional leaves the requirement up to the partner XMPP service for a mandatory-to-negotiate decision.
     9..a.**Required** The XMPP service requires SASL negotiation.
     9..b.**Optional** The XMPP service indicates that SASL is mandatory-to-negotiate.
     9..c.**Not Supported** The XMPP service does not support SASL.

   - **Support server dialback negotiation** The support server dialback negotiation process uses the domain name system (DNS) and an authoritative server to verify that the request came from a valid XMPP partner. To do this, the originating server creates a message of a specific type with a generated dialback key and looks up the receiving server in

DNS. The originating server sends the key in an XML stream to the resulting DNS lookup, presumably the receiving server. On receipt of the key over the XML stream, the receiving server does not respond to the originating server, but sends the key to a known authoritative server. The authoritative server verifies that the key is either valid or not valid. If not valid, the receiving server does not respond to the originating server. If the key is valid, the receiving server informs the originating server that the identity and key is valid and the conversation can commence.

There are two valid states for **Dialback negotiation**:

9..a.**True** The XMPP server is configured to use Dialback negotiation if a request should be received from an originating server.

9..b.**False** The XMPP server is not configured to use Dialback negotiation and if a request should be received from an originating server, it will be ignored.

10.Click **Commit** to save your changes to the site or user policy.

⊟Update DNS Records for Lync Server 2013 XMPP Gateway

1. To configure DNS for XMPP federation, you add the following SRV record to your external DNS:_xmpp-server._tcp.<domain name> The SRV record will resolve to the Access Edge FQDN of the Edge server, with a port value of 5269.

1.6.2.10 Phase 9: Complete Post-Migration Tasks

Phase 9: Complete Post-Migration Tasks

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-10-15*

The topics in this section describe tasks that you will need to perform after you have completed your migration to Lync Server 2013.

In This Section

- Migrate Response Groups
- Migrate Dial-in Access Numbers
- Enable Exchange 2013 Outlook Web App and IM Integration
- Migrate Address Book
- Enable Remote Call Control
- Remove Legacy Archiving and Monitoring Servers
- Migrate Mediation Server
- Configure Trusted Application Servers
- Configure the Meeting Join Page
- Deploy Lync Server 2013 Clients
- Move Exchange Unified Messaging Contact Objects
- Verify that all Exchange UM Contact Objects are Removed from the Legacy Pool

1.6.2.10.1 Migrate Response Groups

Migrate Response Groups

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-19*

After your users are moved to Lync Server 2013 pools, you can migrate your response groups. Migrating response groups includes copying agent groups, queues, workflows, and audio files, and moving Response Group contact objects from the legacy deployment to the Lync Server 2013 pool. After you migrate your legacy response groups, calls to the response groups are handled by the Response Group application in the Lync Server 2013 pool. Calls to response groups are no longer handled by the legacy pool.

Note:

Although you can migrate response groups before you move all users to the Lync Server 2013 pool, we recommend that you move all users first. In particular, users who are response group agents will not have full functionality of new features until they are moved to the Lync Server 2013 pool.

Before you migrate response groups, you must have deployed a Lync Server 2013 pool that includes the Response Group application. The Response Group application is installed and activated by default when you deploy Enterprise Voice. You can ensure that the Response Group application is installed by running the **Get-CsService–ApplicationServer** cmdlet.

Note:

You can create new Lync Server 2013 response groups in the Lync Server 2013 pool before you migrate your legacy response groups.

To migrate response groups from a legacy pool to the Lync Server 2013, you run the **Move-CsRgsConfiguration** cmdlet. Before you can run **Move-CsRgsConfiguration**, you must first install the Windows Management Instrumentation (WMI) Backward Compatibility interfaces package. Install this application by running OCSWMIBC.msi. You can find OCSWMIBC.msi on the installation media in the Setup folder.

Important:

The Response Group migration cmdlet moves the Response Group configuration for the entire pool. You cannot select specific groups, queues, or workflows to migrate.

After you migrate the response groups, you need to update the URL that formal agents use to sign into and out of their response groups, and use Lync Server Control Panel or Lync Server Management Shell cmdlets to verify that all agent groups, queues, and workflows moved successfully.

Caution:

When you migrate response groups, the Office Communications Server 2007 R2 response groups are not removed. Do not remove Office Communications Server 2007 R2 response groups. If you remove an Office Communications Server 2007 R2 response group, the response groups in Lync Server 2013 stop working.

Important:

We recommend that you do not remove any data from your previous deployment until you decommission the pool. In addition, we strongly recommend that you export response groups immediately after you migrate. If an Office Communications Server 2007 R2 response group gets removed, you can then restore your response groups from the backup to get Lync Server 2013 response groups running again.

When you run the **Move-CsRgsConfiguration** cmdlet, the agent groups, queues, workflows, and audio files remain in the legacy pool for rollback purposes. If you do need to roll back to the legacy pool, however, you need to run the **Move-CsApplicationEndpoint** cmdlet to move contact objects back to the legacy pool.

Important:

We recommend that you don't delete any response group data from the legacy pool until you decommission the pool.

The procedure that follows for migrating Response Group configurations assumes that you have a one-to-one relationship between your legacy pools and the Lync Server 2013 pools. If you plan to consolidate or split up pools during your migration and deployment, you need to plan which legacy pool maps to which Lync Server 2013 pool.

To Migrate Response Group Configurations

1. Locate OCSWMIBC.msi in the Setup folder of the installation media and install it.
2. Log on to the computer with an account that is a member of the RTCUniversalServerAdmins group or has equivalent administrator rights and permissions.
3. Open the Lync Server Management Shell.
4. At the command line, type the following:

   ```
   Move-CsRgsConfiguration -Source <source pool FQDN> -Destination <desti
   ```

   For example:

   ```
   Move-CsRgsConfiguration -Source pool01.contoso.net -Destination pool02
   ```

5. If you deployed the Response Group tab for Microsoft Office Communicator 2007 R2 in your Office Communications Server 2007 R2 environment, remove the tab from the Office Communicator 2007 R2 tabs.xml file.

   Note:
   Formal agents used the Response Group tab to sign in to their response groups before they could receive calls. If you deployed the Response Group tab, you chose the location for the Office Communicator 2007 R2 tabs.xml file when you deployed it.

6. Provide users with the updated URL that agents need to sign into and out of their response groups.

   Note:
   The URL is typically https://webpoolFQDN/RgsClients/Tab.aspx, where *webpoolFQDN* is the fully qualified domain name (FQDN) of the web pool that is associated with the pool that you just migrated to Lync Server 2013.

   Note:
   This step is not required after users upgrade to Lync 2013 because the URL is available from the **Tools** menu in Lync.

To Verify Response Group Migration by Using Lync Server Control Panel

1. Open the Lync Server Control Panel.
2. In the left navigation pane, click **Response Groups**.
3. On the **Workflow** tab, verify that all the workflows in your Office Communications Server 2007 R2 environment are included in the list.
4. Click the **Queue** tab, and verify that all the queues in your Office Communications Server 2007 R2 environment are included in the list.
5. Click the **Group** tab, and verify that all the agent groups in your Office Communications Server 2007 R2 environment are included in the list.

To Verify Response Group Migration by Using Cmdlets

1. Open the Lync Server Management Shell.

   For details about the following cmdlets, run:

   ```
   Get-Help <cmdlet name> -Detailed
   ```

2. At the command line, type the following:

```
Get-CsRgsAgentGroup
```

3. Verify that all the agent groups in your Office Communications Server 2007 R2 environment are included in the list.
4. At the command line, type the following:

```
Get-CsRgsQueue
```

5. Verify that all the queues in your Office Communications Server 2007 R2 environment are included in the list.
6. At the command line, type the following:

```
Get-CsRgsWorkflow
```

7. Verify that all the workflows in your Office Communications Server 2007 R2 environment are included in the list.

1.6.2.10.2 Migrate Dial-in Access Numbers

Migrate Dial-in Access Numbers

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-09-26*

Migrating dial-in access numbers requires two steps: running the **Import-CsLegacyConfiguration** cmdlet (completed earlier in Import Policies and Settings) to migrate dial plans and other dial-in access number settings, and running the **Move-CsApplicationEndpoint** cmdlet to migrate the contact objects.

To migrate dial-in access numbers

1. Open the Office Communications Server 2007 R2 administrative tool.
2. In the console tree, right-click the forest node, click **Properties**, and then click **Conferencing Attendant Properties**.
3. On the **Access Phone Numbers** tab, click **Serviced by Pool** to sort the access phone numbers by their associated pool, and identify all the access numbers for the pool from which you are migrating.
4. To identify the SIP URI for each access number, double-click the access number to open the **Edit Conferencing Attendant Number** dialog box, and look under **SIP URI**.
5. Open the Lync Server Management Shell.
6. To move each dial-in access number to a pool hosted on Lync Server 2013, run:

```
Move-CsApplicationEndpoint -Identity <SIP URI of the access number to
```

7. In the Office Communications Server 2007 R2 Administrative tool, on the **Access Phone Numbers** tab, verify that no dial-in access numbers remain for the Office Communications Server 2007 R2 pool from which you are migrating.

1.6.2.10.3 Enable Exchange 2013 Outlook Web App and IM Integration

Enable Exchange 2013 Outlook Web App and IM Integration

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-19*

To enable Exchange 2013 Outlook Web Access (OWA) and instant messaging (IM) integration with Lync Server 2013, you must add the Exchange 2013 Client Access Server

(CAS) server to the Lync Server 2013 topology as a trusted application server.

To create a trusted application pool

1. Start the Lync Server 2013 Management Shell.
2. Run the following cmdlet:

   ```
   Get-CsSite
   ```

   This returns the siteID for the siteName in which you are creating the pool. For details, see Get-CsSite in the Lync Server 2013 Management Shell documentation.
3. Run the following cmdlet:

   ```
   New-CsTrustedApplicationPool -Identity <E14 CAS FQDN> -ThrottleAsServe
   ```

   For details, see New-CsTrustedApplicationPool in the Lync Server 2013 Management Shell documentation.

   The Exchange Server FQDN should be configured as the Exchange OWA certificate Subject Name (SN), or the Subject Alternate Name (SAN).

   In Exchange OWA, verify that the pool's FQDN is trusted as well.

   > **Important:**
   >
   > If your CAS server is *not* collocated on the same server that is running Exchange 2013 Unified Messaging (UM), skip the remaining steps in this procedure and perform the "Create a trusted application for the Exchange 2013 CAS server" procedure later in this topic. If your CAS server is collocated on the same server that is running Exchange 2013 Unified Messaging (UM), complete the steps in this procedure and do not perform the "Create a trusted application for the Exchange 2013 CAS server" procedure later in this topic.
4. Run **Enable-CsTopology**.
5. Open Topology Builder and download the existing topology.
6. In the left pane, expand the tree until you reach **Trusted application servers**.
7. Expand the **Trusted application servers** node.
8. You should now see the Exchange 2013 CAS server listed as a trusted application server.

To create a trusted application for the Exchange 2013 CAS server

1. Start the Lync Server 2013 Management Shell.
2. If your CAS server is *not* collocated on the same server that is running Exchange 2013 Unified Messaging (UM), run the following cmdlet:

   ```
   New-CsTrustedApplication -ApplicationId <AppID String> -TrustedApplica
   ```

   For details, see the topic New-CsTrustedApplication in the Lync Server 2013 Management Shell documentation.
3. Run **Enable-CsTopology**.
4. From Topology Builder, in the left pane, expand the tree until you reach **Trusted application servers**.
5. Expand the **Trusted application servers** node.
6. You should now see the Exchange 2013 CAS server listed as a trusted application server.

1.6.2.10.4 Migrate Address Book

Migrate Address Book

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-02*

To migrate Address Book customized normalization rules

1. Find the Company_Phone_Number_Normalization_Rules.txt file in the root of the Address Book shared folder, and copy it to the root of the Address Book shared folder in your Lync Server 2013 pilot pool.

   Note:

   The sample Address Book normalization rules have been installed in your ABS Web component file directory. The path is **$installedDriveLetter:\Program Files\Microsoft Lync Server 2013\Web Components\Address Book Files\Files\ Sample_Company_Phone_Number_Normalization_Rules.txt,**. This file can be copied and renamed as **Company_Phone_Number_Normalization_Rules.txt** to the address book shared folder's root directory. For example, the address book shared in **$serverX**, the path will be similar to: **\\$serverX \LyncFileShare\2-WebServices-1\ABFiles**.

2. Use a text editor, such as Notepad, to open the Company_Phone_Number_Normalization_Rules.txt file.
3. Certain types of entries will not work correctly in Lync Server 2013. Look through the file for the types of entries described in this step, edit them as necessary, and save the changes to the Address Book shared folder in your pilot pool.

   Strings that include required whitespace or punctuation cause normalization rules to fail because these characters are stripped out of the string that is input to the normalization rules. If you have strings that include required whitespace or punctuation, you need to modify the strings. For example, the following string would cause the normalization rule to fail:

   ```
   \s*\(\s*\d\d\d\s*\)\s*\-\s*\d\d\d\s*\-\s*\d\d\d\d
   ```

   The following string would not cause the normalization rule to fail:

   ```

   \s*\(?\s*\d\d\d\s*\)?\s*\-?\s*\d\d\d\s*\-?\s*\d\d\d\d
   ```

1.6.2.10.5 Enable Remote Call Control

Enable Remote Call Control

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-02*

Remote call control enables users to control their desktop private branch exchange (PBX) phones by using Lync Server 2013. If you deployed remote call control in your legacy environment and want to migrate it Lync Server 2013, you need to perform the following tasks:

1. Install a SIP/CSTA gateway and configure it to communicate with your PBX. You need to do this step when you deploy your Lync Server 2013 pilot pool.
2. After you merge your topology and migrate your policies and settings, configure Lync Server 2013 to route CSTA requests to the SIP/CSTA gateway. This step is a manual step that follows the automated migration. To configure

routing for CSTA requests, do the following:

- Remove legacy authorized host entries (known as *trusted server entries* in Lync Server 2013). If you are migrating users from your legacy deployment, ensure that you remove all existing authorized host entries that you created for the SIP/CSTA gateway before you configure new trusted application entries on the Lync Server 2013 pilot pool. For details about how to remove legacy authorized host entries, see Remove an Authorized Host Entry.
- Configure a static route for remote call control. You can configure a static route for individual pools that you want to support remote call control, or you can configure a global static route so that each pool that is not configured with a pool-level static route uses the global static route. For details about how to configure the static route, see Configure a Static Route for Remote Call Control in the Deployment documentation.
- Configure a trusted application entry for remote call control on each pool for which you want to support remote call control. For details about how to configure a trusted application entry, see Configure a Trusted Application Entry for Remote Call Control in the Deployment documentation.

3. If you deployed a SIP/CSTA gateway that uses Transmission Control Protocol (TCP) to connect to Lync Server 2013, define the IP address of the gateway in Topology Builder. For details about defining the IP address, see Define a SIP/CSTA Gateway IP Address in the Deployment documentation.
4. Configure Lync 2013 users for remote call control by enabling remote call control and assigning a line server Uniform Resource Identifier (URI) and a line URI. When you migrate users from your legacy deployment to Lync Server 2013, the remote call control settings are migrated along with the other user settings.
5. If you customized Address Book phone number normalization rules in your legacy deployment, you need to perform some manual tasks after the automated migration of policies and settings is complete to migrate the customized normalization rules. If you did not customize normalization rules, Address Book is migrated along with the rest of your topology. For details about manually migrating customized normalization rules, see Migrate Address Book.

1.6.2.10.5.1 Remove an Authorized Host Entry

Remove an Authorized Host Entry

Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks > Enable Remote Call Control >

Topic Last Modified: *2012-09-26*

This topic describes how to remove a legacy authorized host entry (known as a *trusted application entry* in Lync Server 2013). You must remove existing authorized host entries for any SIP/CSTA gateways in your Office Communications Server 2007 R2 deployment when you migrate remote call control to a Lync Server 2013 deployment. You must use the administrative tools included with Office Communications Server 2007 R2 to remove the existing authorized host entries.

To remove an authorized host entry in an Office Communications Server 2007 R2 deployment

1. Open the Office Communications Server 2007 R2 administrative console.

2. Expand the tree and right-click the pool where the authorized host was created.
3. Click **Properties**, and then click **Front End Properties**.
4. Click the **Host Authorization** tab.
5. Select a server, and then click **Remove**.
6. In **Properties**, click **OK**.

1.6.2.10.6 Remove Legacy Archiving and Monitoring Servers

Remove Legacy Archiving and Monitoring Servers

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-09-26*

If your Office Communications Server 2007 R2 deployment contained an Archiving Server or a Monitoring Server, after migrating to Lync Server 2013, those servers can be removed from the legacy environment provided all users have been removed from any remaining Office Communications Server 2007 R2 pools. You can remove the Archiving Server or Monitoring Server in any sequence. The key requirement is that all users have been removed from any remaining Office Communications Server 2007 R2 pools.

You can move users from Office Communications Server 2007 R2 to Lync Server 2013 by following the procedures outlined in Phase 6: Move users to the Pilot Pool.

After you have confirmed that all users have been removed from any remaining pools, follow the procedure in "Removing Servers and Server Roles" at http://go.microsoft.com/fwlink/p/?linkId=205887.

1.6.2.10.7 Migrate Mediation Server

Migrate Mediation Server

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-09-28*

Your Mediation Server is merged into your Lync Server 2013 pilot topology when you run the Merge wizard. You configure the Lync Server 2013 Mediation Server, however, after all users are migrated because an Office Communications Server 2007 R2 pool cannot communicate with a Lync Server 2013 Mediation Server. During the side-by-side migration, the Lync Server 2013 pool communicates with the Office Communications Server 2007 R2 Mediation Server.

When you configure your Lync Server 2013 Mediation Server, you must also upgrade or replace your Office Communications Server 2007 R2 gateways. Office Communications Server 2007 R2 gateways do not support Lync Server 2013 Mediation Server. You need to deploy gateways that are certified for Lync Server 2013 and associate them with the Lync Server 2013 Mediation Server. This step is required before you can completely decommission your Office Communications Server 2007 R2 deployment.

The topics in this section describe configuration tasks that you need to perform after you have completed your migration of Lync Server 2013 Mediation Server. Transitioning the collocated Mediation Server to a stand-alone Mediation Server is an optional task.

- Configure Mediation Server
- Change Voice Routes to use the new Lync Server 2013 Mediation Server

- Transition a collocated Mediation Server to a Stand-Alone Mediation Server (optional)

1.6.2.10.7.1 Configure Mediation Server

Configure Mediation Server

Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks > Migrate Mediation Server >

Topic Last Modified: *2012-09-28*

This procedure details the steps to configure the Lync Server 2013 pool to use the Lync Server 2013 Mediation Server, instead of the legacy Office Communications Server 2007 R2 Mediation Server.

To successfully publish, enable, or disable a topology when adding or removing a server role, you should be logged in as a user who is a member of the RTCUniversalServerAdmins and Domain Admins groups. It is also possible to delegate the proper administrator rights and permissions for adding server roles. For details, see Delegate Setup Permissions in the Standard Edition server or Enterprise Edition server Deployment documentation. For other configuration changes, only membership in the RTCUniversalServerAdmins group is required.

Note:

For the latest information on finding qualified PSTN gateways, IP-PBXs, and SIP trunking services that work with Lync Server 2013, see "Microsoft Unified Communications Open Interoperability Program" at http://go.microsoft.com/fwlink/p/?linkId=206015.

To configure Mediation Server Using Topology Builder

1. Open an existing topology from Topology Builder.
2. In the left pane, navigate to **PSTN gateways**.
3. Right-click **PSTN gateways**, and then click **New IP/PSTN Gateway**.
4. Complete the **Define New IP/PSTN Gateway** page with the following information:
   - Enter the gateway FQDN or IP address. The FQDN of the gateway is required if the gateway uses the TLS protocol.
   - Accept the default value of the **Listening port for IP/PSTN gateway** or enter the new listening port if it was modified.
   - Set the **Sip Transport Protocol**.
5. In the left pane, navigate to the **Enterprise Edition Front End pool** or the **Standard Edition Server**.
6. Right-click the pool, and then click **Edit Properties**.
7. Under **Mediation Server**, set the **Listening ports**.
8. Next, associate the newly created PSTN gateway by selecting it and clicking **Add**.
9. In **Topology Builder**, select the top-most node **Lync Server**.
10. From the **Action** menu, select **Publish Topology** and then click **Next**.
11. When the **Publishing wizard** completes, click **Finish** to close the wizard.

Note:

It is important that you complete the next topic, Change Voice Routes to use the new Lync Server 2013 Mediation Server to ensure that the voice routes are pointing to the correct Mediation Server.

1.6.2.10.7.2 Change Voice Routes to use the new Lync Server 2013 Mediation Server

Change Voice Routes to use the new Lync Server 2013 Mediation Server

Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks > Migrate Mediation Server >

Topic Last Modified: *2012-09-28*

This procedure changes the voice routes to use the Lync Server 2013 Mediation Server, instead of the legacy Office Communications Server 2007 R2 Mediation Server.

To change the voice routes to use the new Mediation Server

1. Lync Server 2013 Control Panel
2. In the left pane, select **Voice Routing** and then **Route**.
3. Click **New** to create a New Voice Route.
4. Fill in the following fields:
   - **Name**: Type a descriptive name of the voice route. For this document we will use **W15PSTNRoute**.
   - **Description**: Type a short description of the voice route.
5. Skip all remaining sections until you reach **Associated gateways**. Click **Add**. Select the new default gateway and click **OK**.
6. Under **Associated PSTN Usages**, click **Select**.
7. From the **Select PSTN Usage Record** page, select a record name and then click **OK**.
8. From the **New Voice Route** page, click **OK** to create the **Voice Route**.
9. From the **Voice Routing** page, select **Route**.
10. Move the newly created route to the top of the list and then select **Commit**.

1.6.2.10.7.3 Transition a collocated Mediation Server to a Stand-Alone Mediation Server (optional)

Transition a collocated Mediation Server to a Stand-Alone Mediation Server (optional)

Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks > Migrate Mediation Server >

Topic Last Modified: *2012-10-19*

Use the procedure that follows to transition your Mediation Server, collocated on your Standard Edition server or Front End pool, to a stand-alone Mediation Server for a single-site deployment.

To transition a collocated Mediation Server to a stand-alone Mediation Server

1. Open an existing topology from Topology Builder.
2. In the left pane, navigate to **Mediation pools**.
3. Right-click **Mediation pools** and select **New Mediation Server**.
4. On the **Define New Mediation Pool** page, provide the FQDN of the new

Mediation Server pool. Also, select whether this pool will be a single-server or multiple-server pool, and then click **Next**.
5. Select the next hop Front End server pool to which the new Mediation Server will route inbound calls, and then click **Next**.
6. Select the Edge pool to be used by the Mediation Server and then click **Next**.
7. On the **Specify PSTN gateways** page, associate the previous PSTN gateway with the Mediation Server. Select the gateway and then click **Add**.
8. Click **Finish** to close the **Define New Mediation Pool** wizard.
9. From **Topology Builder**, select the top node **Lync Server 2013**.
10. From the **Actions** pane, select **Publish Topology** and complete the wizard.
11. Follow the steps in Install the Files for Mediation Server in the Deployment documentation to install the files on the new Mediation Server.
12. After the files are installed on the Mediation Server, return to Topology Builder, and in the left pane navigate to the pool.
13. Right-click the pool and select **Edit Properties**.
14. Under **Mediation Server**, clear the check box **Collocated Mediation Server enabled** and then click **OK**.
15. From **Topology Builder**, select the top node **Lync Server 2013**.
16. From the **Action** menu, select **Publish Topology** and complete the wizard.

1.6.2.10.8 Configure Trusted Application Servers

Configure Trusted Application Servers

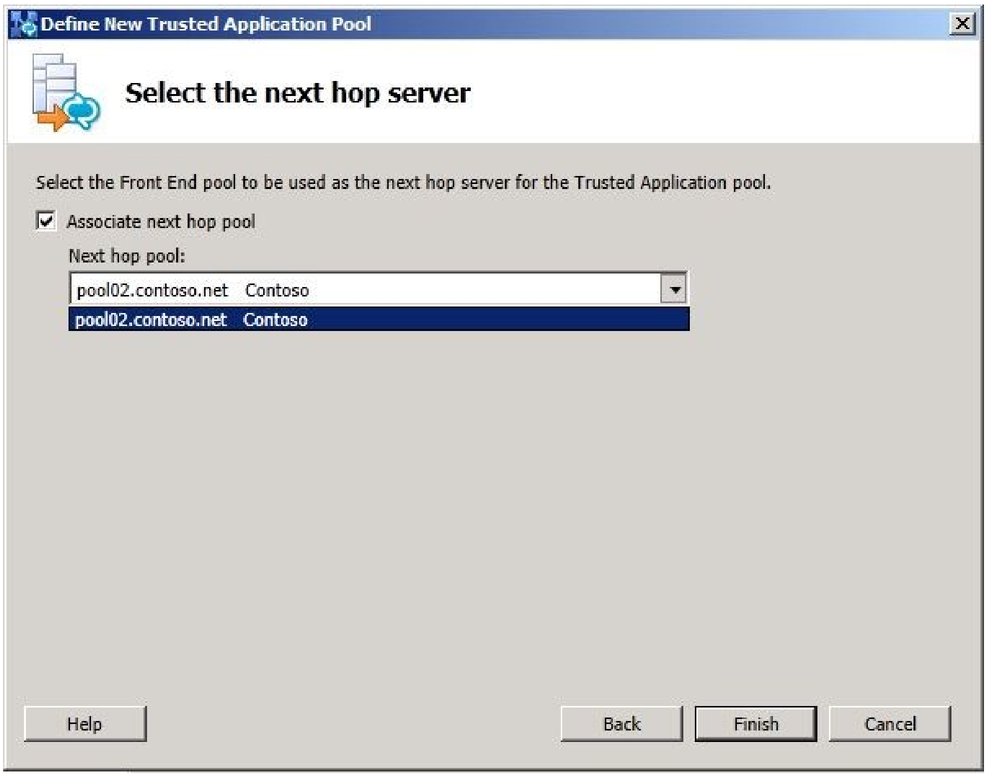
Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-04*

In a mixed environment, if you create a new trusted application server after merging the legacy Office Communications Server topology with Lync Server 2013, and you define a new trusted application server using Topology Builder, you must set the next hop pool to be a Lync Server 2013 pool. In a merged environment, both the legacy Office Communications Server pool and the Lync Server 2013 pool appear in the drop down list. Selecting the legacy pool is *not* supported.

To select Lync Server 2013 as next hop when creating a Trusted application server

1. Open an existing topology in Topology Builder.
2. In the left pane, right click **Trusted application servers** and click **New Trusted Application Pool**.
3. Enter the **Pool FQDN** of the trusted application pool and select whether it will be a single-server or multiple-server deployment.
4. Click **Next**.
5. On the **Select the next hop** page, from the list, select the Lync Server 2013 Front End pool.



Define New Trusted Application Pool

Select the next hop server

Select the Front End pool to be used as the next hop server for the Trusted Application pool.

☑ Associate next hop pool

Next hop pool:

pool02.contoso.net Contoso

6. Click **Finish**.
7. Select the top node **Lync Server** and from the **Actions** pane, select **Publish**.
8. Verify the **Trusted Application Pool** was created successfully and is associated with the correct Front End pool.

1.6.2.10.9 Configure the Meeting Join Page

Configure the Meeting Join Page

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-12-14*

When a user clicks a meeting link in a meeting request, the meeting join page detects whether a Lync 2013 client is already installed on the user's computer. If a client is already installed, that client opens and joins the meeting. If a client is not installed, by default the 2013 version of Microsoft Lync Web App opens.

You can modify the behavior of the meeting join page if you want to allow users to join meetings with Office Communicator 2007 R2 or Lync 2010 Attendant. These configuration options have been removed from the Lync Server 2013 Control Panel, but you configure them by using the CsWebServiceConfiguration cmdlet.

Meeting Join Page CsWebServiceConfiguration Parameters

CsWebServiceConfiguration Parameter	Description
ShowJoinUsingLegacyClientLink	If set to True, users joining a meeting by using a client application other than Lync will be given the opportunity to join the meeting

	by using Office Communicator 2007 R2. The default value is False.
ShowAlternateJoinOptionsExpanded	When set to True then alternate options for joining an online conference (such as Office Communicator 2007 R2) will automatically be expanded and shown to users. When set to False (the default value) these options will be available, but the user will have to display the list of options for themselves.

To configure the meeting join page by using Lync Server 2013 Management Shell

1. Start the Lync Server 2013 Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Run the following cmdlet:

   ```
   Get-CsWebServiceConfiguration
   ```

   This cmdlet returns the web service configuration settings.
3. Run the following command, with the parameters set to True or False, depending on your preference (for details about the parameters for this cmdlet, see the Lync Server 2013 Management Shell documentation):

   ```
   Set-CsWebServiceConfiguration -Identity global -ShowJoinUsingLegacyCli
   ```

1.6.2.10.10 Deploy Lync Server 2013 Clients

Deploy Lync Server 2013 Clients

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-19*

After you migrate users to Lync Server 2013, do the following:

1. Use the Client Version Filter on the new Lync Server 2013 server to only allow clients with the most current updates installed to sign in.
2. If necessary, configure the Group Policy settings that are required for client bootstrapping. For details, see Configuring Client Bootstrapping Policies in the Deployment documentation. Configuration of these settings is only necessary if you want to change existing client bootstrapping policies or if you want to set new client bootstrapping policies. If you do not plan to configure client bootstrapping policies, or you want legacy client bootstrapping policies to remain in effect, no action is necessary.
3. Configure other user and client policies for specific users or groups of users by using Lync Server 2013 Control Panel, Lync Server 2013 Management Shell, or both. For details, see New and Changed Settings for Lync 2013 in the Planning documentation.
4. Deploy the latest version of Lync Server 2013 clients along with the latest cumulative updates. For details, see Deploying Clients and Devices in the Deployment documentation.
5. (Optional) If your organization requires Lync Server 2013 enhanced presence privacy mode, after migration is complete, define a Client Version Policy Rule to prevent earlier client versions from signing in. Then, enable enhanced

presence privacy mode.

Important:
Do not enable Lync 2013 enhanced presence privacy mode until every user on a given server pool has the most current client versions installed.

1.6.2.10.11 Move Exchange Unified Messaging Contact Objects

Move Exchange Unified Messaging Contact Objects

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-10-19*

To migrate Auto Attendant (AA) and Subscriber Access (SA) contact objects to the new Lync Server 2013 deployment, you first move the objects from the legacy Office Communications Server 2007 R2 deployment to the new the Lync Server 2013 deployment using the **Get-CsExUmContact** and **Move-CsExUmContact** cmdlets. On the Exchange Server, you then run the **ExchUCUtil** Windows PowerShell script to do the following for the newly deployed Lync pool:

- Add it to the Unified Messaging IP gateways.
- Add it to the Unified Messaging hunt groups.

Note:
In order to use the **Get-CsExUmContact** and **Move-CsExUmContact** cmdlets, you must be a member of the RTCUniversalUserAdmins group and have organizational unit (OU) permission to the OU where the contacts objects are stored. OU permission can be granted using the **Grant-OUPermission** cmdlet.

⊟To move contact objects by using the Lync Server Management Shell

1. Open the Lync Server Management Shell.
2. For each pool registered with Exchange UM (where pool1.contoso.net is a pool from the Office Communications Server 2007 R2 deployment and pool2.contoso.net is the pool from the Lync Server 2013 deployment) at the command line, type the following:

```
Get-CsExUmContact -Filter {RegistrarPool -eq "pool01.contoso.net"} | M
```

   To verify that the contact objects are moved, run the **Get-CsExumContact** cmdlet and confirm that **RegistrarPool** is now pointing to the new pool.

⊟To run the ExchUCUtil Windows PowerShell script

1. Log on to the Exchange UM Server as a user with Exchange Organization Administrator privileges.
2. Navigate to the ExchUCUtil Windows PowerShell script.
   In Exchange 2007, ExchUCUtil.ps1 is located at: **%Program Files%\Microsoft\Exchange Server\Scripts\ExchUCUtil.ps1**
   In Exchange 2010, ExchUCUtil.ps1 is located at: **%Program Files%\Microsoft\Exchange Server\V14\Scripts\ExchUCUtil.ps1**
3. If Exchange is deployed in a single forest, type:

```
exchucutil.ps1
```

   Or, if Exchange is deployed in multiple forests, type:

```
exchucutil.ps1 -Forest:" <forest FQDN>"
```

   where *forest FQDN* specifies the forest in which Lync Server 2013 is deployed.

Important:

Be sure to restart the **Lync Server Front-End** service (rtcsrv.exe) *after* you run exchucutil.ps1. Otherwise, Lync Server 2013 will not detect Unified Messaging in the topology.

1.6.2.10.12 Verify that all Exchange UM Contact Objects are Removed from the Legacy Pool

Verify that all Exchange UM Contact Objects are Removed from the Legacy Pool

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 9: Complete Post-Migration Tasks >

Topic Last Modified: *2012-09-26*

Use either the **OCSUmUtil** tool or the **Get-CsExumContact** cmdlet to verify that Exchange UM contact objects have been removed from the legacy Office Communications Server 2007 R2 pool. **OCSUmUtil** is located in the following folder:

%Program Files%\Common Files\Lync Server 2013\Support\OcsUMUtil.exe

OCSUmUtil must be run from a user account that has:

- Membership in the RTCUniversalServerAdmins and RTCUniversalUserAdmins group (which includes rights to read Exchange Server Unified Messaging settings)
- Domain rights to create contact objects in the specified organizational unit (OU) container

For details about using the **Get-CsExumContact** cmdlet, see Get-CsExUmContact in the Lync Server Management Shell documentation.

1.6.2.11 Phase 10: Decommission Legacy Site

Phase 10: Decommission Legacy Site

Microsoft Lync Server 2013 > Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 >

Topic Last Modified: *2012-10-16*

The following topics provide guidance in decommissioning pools, and deactivating and removing servers and pools from a legacy deployment of Office Communications Server 2007 R2. Not all of the procedures listed in this section are required. Read the information in each of these topics to determine which decommissioning procedure to use.

Caution:

If you imported conference directories for dial-in conferencing to Lync Server 2013, it is important to transition conference directory ownership to Lync Server 2013 before you begin to decommission your pools. If you decommission a pool without first transitioning conference directory ownership, the dial-in feature for all migrated meetings will no longer work. You must perform the step to transition ownership once for each conference directory in your legacy pool.

Important:

For information on migrating and upgrading Microsoft Unified Communications Managed API (UCMA) applications, prior to decommissioning your legacy environment, see http://

go.microsoft.com/fwlink/p/?LinkId=269555

In This Section

- Move Conference Directories
- Update DNS SRV Records
- Decommissioning Servers and Pools
- Remove BackCompatSite

1.6.2.11.1 Move Conference Directories

Move Conference Directories

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 10: Decommission Legacy Site >

Topic Last Modified: *2012-10-04*

Before decommissioning a pool, you need to perform the following procedure for each conference directory in your Office Communications Server 2007 R2 pool.

To move a conference directory to Lync Server 2013

1. Open the Lync Server Management Shell.
2. To obtain the identity of the conference directories in your organization, run the following commands:

   ```
   Get-CsConferenceDirectory
   ```

   Because this cmdlet returns all the conference directories in your organization, you may want to limit the results to only the pool you want to decommission. For example, if you want to decommission a pool with the fully qualified domain name (FQDN) pool01.contoso.net:

   ```
   Get-CsConferenceDirectory | Where-Object {$_.ServiceID -match "pool01.
   ```

   This cmdlet returns all the conference directories where service ID contains the FQDN pool01.contoso.net.
3. To move conference directories, run the following for each conference directory in the pool:

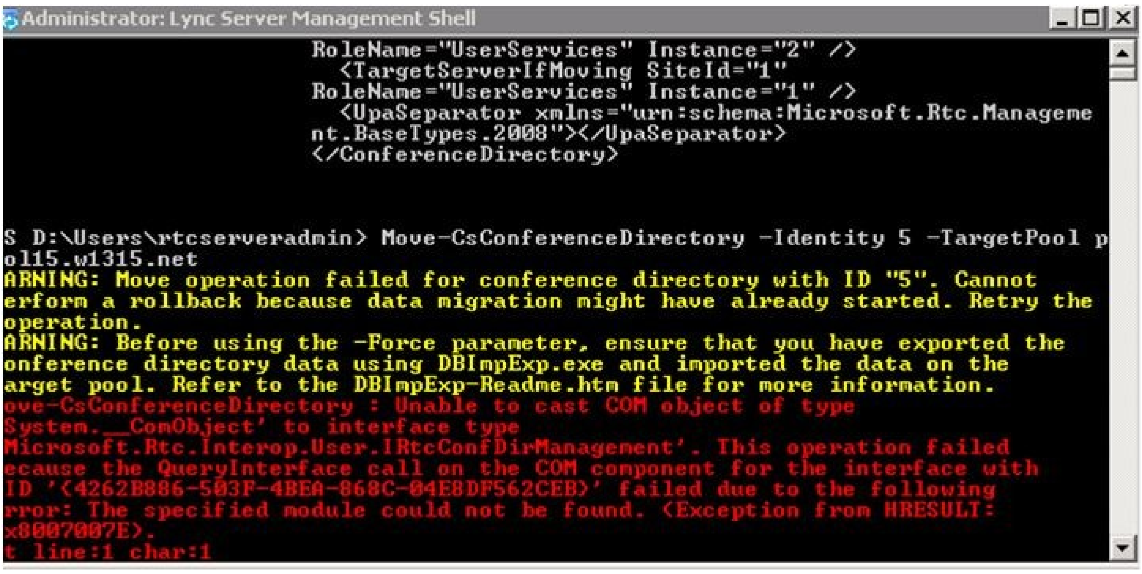
   ```
   Move-CsConferenceDirectory -Identity <Numeric identity of conference d
   ```

   For example:

   ```
   Move-CsConferenceDirectory -Identity 3 -TargetPool pool02.contoso.net
   ```

Note:

You may experience an error, shown below, that is caused by the Lync Server Management Shell requiring an updated set of permissions from Active Directory. To resolve the error, closed the current window and open a new Lync Server Management Shell and run the command again.



```
                     RoleName="UserServices" Instance="2" />
                       <TargetServerIfMoving SiteId="1"
                     RoleName="UserServices" Instance="1" />
                       <UpaSeparator xmlns="urn:schema:Microsoft.Rtc.Manageme
                     nt.BaseTypes.2008"></UpaSeparator>
                     </ConferenceDirectory>


S D:\Users\rtcserveradmin> Move-CsConferenceDirectory -Identity 5 -TargetPool p
ol15.w1315.net
ARNING: Move operation failed for conference directory with ID "5". Cannot
erform a rollback because data migration might have already started. Retry the
operation.
ARNING: Before using the -Force parameter, ensure that you have exported the
onference directory data using DBImpExp.exe and imported the data on the
arget pool. Refer to the DBImpExp-Readme.htm file for more information.
ove-CsConferenceDirectory : Unable to cast COM object of type
System.__ComObject' to interface type
Microsoft.Rtc.Interop.User.IRtcConfDirManagement'. This operation failed
ecause the QueryInterface call on the COM component for the interface with
ID '{4262B886-503F-4BEA-868C-04E8DF562CEB}' failed due to the following
rror: The specified module could not be found. (Exception from HRESULT:
x8007007E).
t line:1 char:1
```

1.6.2.11.2 Update DNS SRV Records

Update DNS SRV Records

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 10: Decommission Legacy Site >

Topic Last Modified: *2012-09-29*

To successfully complete this procedure, you should be logged on to the server or domain as a member of the Domain Admins group or a member of the DnsAdmins group.

This topic describes how to update the Domain Name System (DNS) records after migrating to Lync Server 2013. After all users have been moved to Lync Server 2013, but before the legacy Office Communications Server 2007 R2 pool or Director is decommissioned, you must update the DNS SRV records in your internal DNS for every SIP domain. This procedure assumes that your internal DNS has zones for your SIP user domains.

To configure a DNS SRV record

1. On the DNS server, click **Start**, click **Administrative Tools**, and then click **DNS**.
2. In the console tree for your SIP domain, expand **Forward Lookup Zones**, expand the SIP domain in which Lync Server 2013 is installed, and navigate to the **_tcp** setting.
3. In the right pane, right click **_sipinternaltls** and select **Properties**.
4. In **Host offering this service**, update the host FQDN to point to the Lync Server 2013 pool.
5. Click **OK**.

To verify that the FQDN of the Front End pool or Standard Edition server can be resolved

1. Log on to a client computer in the domain.
2. Click **Start**, and then click **Run**.
3. In the **Open** box, type **cmd**, and then click **OK**.
4. At the command prompt, type **nslookup** *<FQDN of the Front End pool>* or *<FQDN of the Standard Edition server>*, and then press ENTER.
5. Verify that you receive a reply that resolves to the appropriate IP address for the FQDN.

1.6.2.11.3 Decommissioning Servers and Pools

Decommissioning Servers and Pools

Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 10: Decommission Legacy Site >

Topic Last Modified: *2012-09-26*

The following webpages contain details about decommissioning Office Communications Server 2007 R2 Standard Edition or Enterprise Edition servers and pools.

- Decommissioning Standard Edition at http://go.microsoft.com/fwlink/p/?linkId=205889
- Removing Servers and Server Roles at http://go.microsoft.com/fwlink/p/?linkId=205887
- Removing an Enterprise Pool at http://go.microsoft.com/fwlink/p/?linkId=205888

1.6.2.11.4 Remove BackCompatSite

Remove BackCompatSite

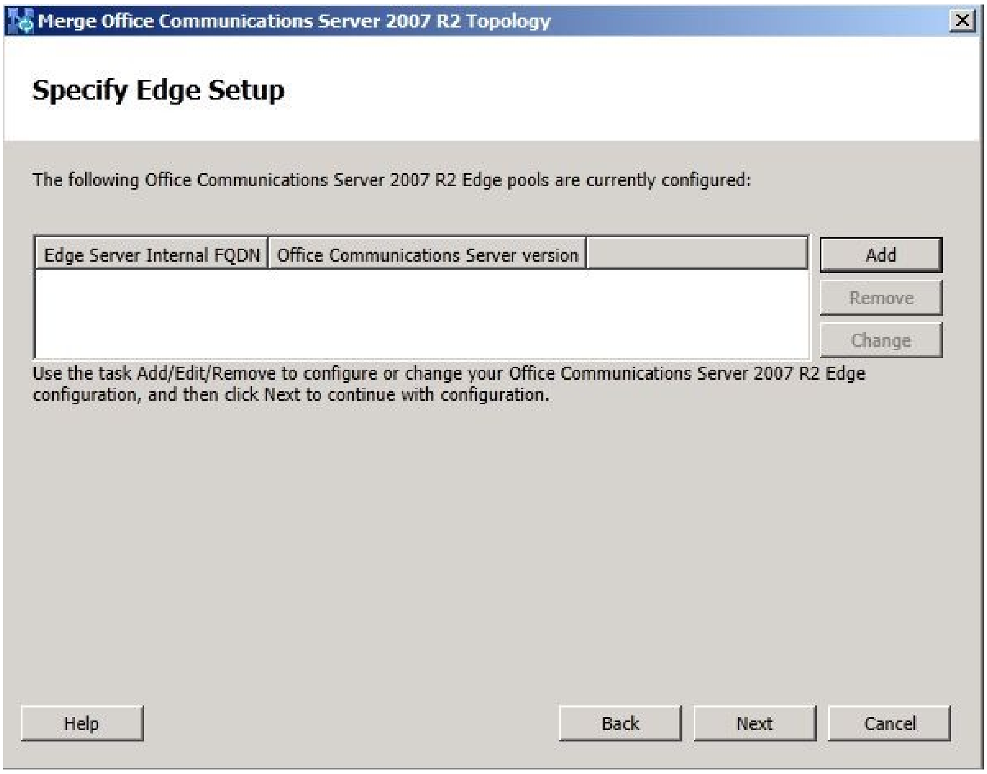
Migration > Migration from Office Communications Server 2007 R2 to Lync Server 2013 > Phase 10: Decommission Legacy Site >

Topic Last Modified: *2012-09-28*

After all pools are deactivated and all Edge Servers have been uninstalled, run the Topology Builder Merge wizard to remove the **BackCompatSite**.

To remove BackCompat site from Topology Builder

1. Open an existing deployment from Topology Builder.
2. In the **Action** menu, click **Merge 2007 R2 Topology**.
3. Click **Next** to continue.
4. On the **Specify Legacy Edge** page, ensure that list of Edge Servers is empty. If the list is not empty, use the **Remove** button to remove all the legacy Edge Servers, and then click **Next**.


Merge Office Communications Server 2007 R2 Topology
Specify Edge Setup
Edge Server Internal FQDN
Office Communications Server version
Add
Remove
Change
Help
Back
Next
Cancel

The following Office Communications Server 2007 R2 Edge pools are currently configured:

Use the task Add/Edit/Remove to configure or change your Office Communications Server 2007 R2 Edge configuration, and then click Next to continue with configuration.

5. On the **Specify Internal SIP port setting** page, click **Next**.
6. On the **Summary** page, click **Next** to begin merging the topologies to remove the legacy site.
7. In the **Status** column, verify that the value is **Success** and then click **Finish** to close the wizard.
8. In the left pane of Topology Builder, expand the BackCompatSite and ensure no servers are listed.
9. Right-click the **BackCompatSite**, and then click **Delete**.
10. In **Topology Builder**, select the top-most node **Lync Server**.
11. From the **Action** menu, select **Publish Topology** and then click **Next**.
12. When the **Publishing wizard** completes, click **Finish** to close the wizard.

1.6.3 Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server

Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server

Microsoft Lync Server 2013 > Migration >

Topic Last Modified: *2012-10-06*

The topics in this section guide you through the process of migrating either Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server. If you intend for your Lync Server 2013, Persistent Chat Server deployment to coexist with a Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat deployment, this guide also includes some essential information for operating in this mixed environment. This guide primarily focuses on data migration for Persistent Chat Server. For users who are migrating from legacy versions of Lync Server to Lync Server 2013, see Migration from Lync Server 2010 to Lync Server 2013 and Migration from Office Communications Server 2007 R2 to Lync Server 2013.

◆Important:
This topic assumes that you have already installed Lync Server 2013 in coexistence with Lync Server 2010 or Office Communications Server 2007 R2.

◆Important:
This guide describes the steps generally required to accomplish each phase of migration. It does not address every possible legacy deployment topology or every possible migration scenario. Therefore, you may not need to perform every step that is described, or you may need to perform additional steps, depending on your deployment. The guide also provides examples of verification steps. These verification steps are provided to help you understand what you need to look for to be sure that each phase completes successfully as you progress through your migration. You can modify these verification steps to your specific migration process.

This guide provides information specific to upgrading your existing deployment. It does not explain how to change your existing topology. This guide does not cover the implementation of new features. When a detailed procedure is documented elsewhere, this guide directs you to the appropriate document or document section.

This document defines terms as specified in the following list.

migration

Moving your deployment from a previous version of Persistent Chat Server, formerly known as Group Chat Server, to Lync Server 2013, Persistent Chat Server.

upgrade

Installing a newer version of software on a server or client computer.

coexistence

The temporary environment that exists during migration, when some functionality has been migrated to Lync Server 2013, Persistent Chat Server, and other functionality still remains on a prior version of Group Chat Server.

Persistent Chat Server is an extension of the Lync Server 2013 infrastructure. Depending on your topology, you can migrate Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013 Persistent Chat Server. For details about available topologies and the technical and software requirements for migrating Group Chat Server, see Planning for Persistent Chat Server in the Planning documentation.

If your organization requires compliance support, it is now automatically installed with each Persistent Chat Server. A separate server is no longer needed for compliance.

◆Important:
Persistent Chat Server must be installed on an NTFS file system to help enforce file system security. FAT32 is not a supported file system for Persistent Chat Server.
If your organization requires compliance support, it is now automatically installed with each Persistent Chat Server. A separate server is no longer needed for compliance. For more details about changes in Lync Server 2013 Persistent Chat Server, see New Persistent Chat Server Features in the Getting Started documentation.

In This Section

- Standard Migration Scenario - High-Level

- Migration Process - Details
- Coexistence Considerations

1.6.3.1 Standard Migration Scenario - High-Level

Standard Migration Scenario - High-Level

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server >

Topic Last Modified: *2013-01-30*

Use the following items as a starting point when migrating Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server. The standard Lync Server 2013 migration path is as follows:

- Your organization has previously deployed Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat, and you want to deploy Lync Server 2013, Persistent Chat Server.
- Deploy Lync Server 2013, and then deploy Persistent Chat Server pool(s).
- Prepare and plan for migration of your Persistent Chat rooms, and determine an appropriate time to shut down the system for migration.
- Run the Windows PowerShell cmdlets for migration (**Export-CsPersistentChatData** and **Import-CsPersistentChatData**) to move content to Persistent Chat Server.
- Verify that migration has succeeded.
- Decommission your legacy deployment.
- Configure Persistent Chat Server so that legacy clients can connect to Lync Server 2013, Persistent Chat Server. This is necessary because it takes time to deploy new clients, and you want to enable existing users with legacy clients to have access to their chat rooms as soon as possible.
- Deploy new clients, while continuing to help ensure that workers with legacy Group Chat (clients) can get to their chat rooms.

1.6.3.2 Migration Process - Details

Migration Process - Details

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server >

Topic Last Modified: *2012-10-19*

Use the following prerequisites and detailed steps to migrate either Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server.

Prerequisites for Migration

Be sure that you’ve met the following prerequisites before migrating either Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server.

1. Deploy at least one Lync Server 2013 pool. If you have multiple Lync Server 2013 pools, decide which Lync Server 2013 pool will be the home pool for the new Lync Server 2013 Persistent Chat Server pool.
2. Install the Lync Server 2013, Persistent Chat Server pool. It will be empty (no categories, rooms, or add-ins). Before you migrate your legacy categories, rooms, or add-ins, you can create rooms, categories, or add-ins in your Lync Server 2013, Persistent Chat Server deployment.

Important:

Be aware that these newly created items may conflict with legacy items that you migrate. Avoid any naming conflicts; otherwise, they will be overwritten when the legacy data is migrated.

Preparing the Source Data for Migration

Perform the following steps to properly prepare your source data for migration.

1. Back up the source databases for either Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat. For details about backing up SQL Server, see "Backup Overview (SQL Server)" at http://go.microsoft.com/fwlink/p/?linkid=254851.

   Important:

   Active Directory Domain Services (AD DS) should be the same. As a condition for migration, you cannot migrate to a pool in a different deployment (specifically, in a different Active Directory forest).

2. Inspect your Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat chat rooms and category configuration. Any changes to categories, rooms, or add-ins in your existing legacy deployment will be done by the Group Chat Admin Tool.

   Tip:

   Any changes to categories, rooms, or add-ins in your Lync Server 2013, Persistent Chat Server deployment are performed by the Lync Server Control Panel or Windows PowerShell cmdlets.

   Follow these steps to prepare your legacy system for migration.

   2.a. Persistent Chat Server supports a single level of categories, unlike a deep hierarchical set of categories. After migration, the subcategories are prefixed with full parent category names. You might want to simplify and flatten your existing category structure so that the resulting structure meets your requirements.

   2.b. Verify the **Managers** at the root Category. If any Managers exist at this level, these users will be added as **Managers to all rooms** after migration. If this is not a requirement for your organization, you need to remove these Managers from the root Category.

   2.c. Verify the length of room names. After migration, due to simplified category structures, if the rooms exist under a child category, they are prefixed with full parent category names. The naming limit is 256 characters, including parent category names. You must verify the length of the room names and possibly shorten the length, if they are too long.

   2.d. In Lync Server 2013, if the category **invitations** settings are set to true, you can choose true or false for invitations to rooms under that category. However if the category invitations settings are set to false, rooms under that category have invitations turned off. Before migration, you must reset the invitation settings in your legacy Lync Server Group Chat Server version, if you want room(s) to exist under a specific category. Otherwise, during migration, Lync Server 2013 displays warnings and sets rooms to the default value of false.

   2.e. If you used files in chat rooms, you must XCOPY the files manually to the new Persistent Chat file store after migration. The tools don’t do this.

   2.f. If you had federated users and rooms with federated users, be aware that Persistent Chat Server does not support federation. Rooms with federated users will be migrated; however, the users themselves won’t be able to access the content, because federated access is not supported.

   2.g. Identify those rooms that you do not want to migrate, and mark them as disabled.

   2.h. Identify the date beyond which you want to migrate the chat room content. For example, you may not want to migrate messages earlier than

January 1, 2010, because these messages may be obsolete or not relevant for migration.

Performing the Migration

Perform the following steps to migrate your legacy Group Chat Server.

1. Shut down the Lync Server 2010, Group Chat, Office Communications Server 2007 R2 Group Chat or Lync Server 2013, Persistent Chat Server services. All services must be stopped, so plan to do this at a time when there is enough downtime. As previously described, make sure to back up your current Group Chat database.
2. Run the Windows PowerShell **Export-CsPersistentChatData** cmdlet as a member of the Persistent Chat administrator RBAC role (CsPersistentChatAdministrator). For details about the export/import cmdlets, see Troubleshooting Persistent Chat Server Configuration using Windows PowerShell Cmdlets.
   Inspect the exported contents.
3. Before you're ready to import, shut down Lync Server 2013, Persistent Chat Server services. All services need to be stopped, so plan to do this at a time when there is enough downtime.
4. Perform a backup of the Persistent Chat database if you had created any categories, rooms, or add-ins in your Lync Server 2013 deployment before the migration. The export/import process will be able to merge the legacy data into the Lync Server 2013 deployment, but you'll want to back up the database in case that content is inadvertently overwritten (for example, if naming conflicts still exist).
5. Run the Windows PowerShell **Import-CsPersistentChatData** cmdlet (import tool), with a **WhatIf** command to populate the Back End Server of the Persistent Chat Server pool with migrated data. Some conversions happen in the process to accommodate the simplified administration model. Fix any errors or warnings that appear.
6. Run the Persistent Chat Server Windows PowerShell **Import-CsPersistentChatData** cmdlet as a member of the Persistent Chat administrator RBAC role (CsPersistentChatAdministrator). For details about the export/import cmdlets, see Troubleshooting Persistent Chat Server Configuration using Windows PowerShell Cmdlets.
7. You must XCOPY all uploaded files (the entire folder) to the new Lync Server 2013, Persistent Chat file store.

Important:
The Lync 2013 (client) does not support uploading or viewing files in chat rooms. You can still use the legacy client to post and view files in the room.

8. Port the Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat Lookup Server URI to the Lync Server 2013, Persistent Chat Server contact object. The following steps are required if either your Lync 2010 Group Chat or Office Communicator 2007 R2 Group Chat clients need to connect to the latest Lync 2013, Persistent Chat (client) after migration without any client-side configuration changes:
   - Delete the ocschat@<*domainName*>.com Lookup Server user account. This was used to point to the Lookup Service in Lync Server 2010, Group Chat. You can uninstall the pool and remove trusted entries later.
   - Create a legacy endpoint (Persistent Chat Server contact object) by running the Windows PowerShell cmdlet, **New-CsPersistentChatEndpoint**, with the identical SIP URI so that the legacy client will work effectively when the service is restarted.

   The mandatory migration process is complete at this point. Lync 2010 Group Chat (clients) or Office Communicator 2007 R2 Group Chat (clients) can connect to the new Persistent Chat Server pool now, transparently.
   Follow these additional decommissioning steps for Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat.

9. Start the Persistent Chat Server services by turning on all computers in the new Persistent Chat Server pool.
10. Use the Lync Server Control Panel and Windows PowerShell cmdlets to verify that the data has migrated successfully.
11. Uninstall Lync 2010 Group Chat or Office Communicator 2007 R2 Group Chat from the computers in the Group Chat Server pool.
12. Delete the trusted application and trusted application pool using Windows PowerShell cmdlets. This deletes these items from the Central Management store and the associated Trusted Service Entries (TSEs) from the Active Directory. Alternatively, this step works by using the Topology Builder (the trusted applications/pools have a dedicated node there, also).
13. You can now begin to enable Persistent Chat Server functionality through the new clients. For details about enabling Persistent Chat Server, see Deploying Persistent Chat Server.

Important:
Lync Server 2013 supports multiple Persistent Chat Server pools. However, we support migrating a Lync 2010 Group Chat or Office Communications Server 2007 R2 Group Chat pool to a single Lync Server 2013, Persistent Chat Server pool. You can add additional new Persistent Chat Server pools in your deployment to meet the regulatory needs (for example, keeping data within a given geography).

1.6.3.3 Coexistence Considerations

Coexistence Considerations

Microsoft Lync Server 2013 > Migration > Migration from Lync Server 2010, Group Chat or Office Communications Server 2007 R2 Group Chat to Lync Server 2013, Persistent Chat Server >

Topic Last Modified: *2012-10-06*

After migration, only a Lync Server 2013, Persistent Chat Server pool will exist, and you can decommission your legacy deployment.

Before migration completes and before you have decommissioned your current Group

Chat Server deployment completely, you may have any of the following deployments:

- Lync Server 2013, Persistent Chat Server pool, which must be homed on a Lync Server 2013 pool.
- Lync Server 2010, Group Chat pool, which must be homed on a Lync Server 2010 pool.
- Office Communications Server 2007 R2 Group Chat pool, which must be homed on an Office Communications Server 2007 R2 pool.

These deployments can exist side by side. However the categories, rooms, and add-ins in one deployment do not interact with those in the accompanying deployment.

Using manual configuration, a legacy client (Group Chat client) can connect to one pool at a time for Office Communications Server 2007 R2, Lync Server 2010, Group Chat, or Lync Server 2013.

The Lync 2013 (client) can interact only with the Lync Server 2013, Persistent Chat Server pool, not with legacy Group Chat Server pools. To use Persistent Chat in a Lync 2013 (client), the user must be homed on Lync 2013 and enabled by policy.

1.7 Operations

Operations

Microsoft Lync Server 2013 >

Topic Last Modified: *2013-02-20*

The topics in this section explain how to use management tools to configure and manage your Lync Server 2013 deployment.

In This Section

- Lync Server Administrative Tools
- Managing Users in Lync Server 2013
- Managing the Lync Server 2013 Topology
- Delegating Administrative Control of Lync Server 2013
- Managing IM and Presence Settings
- Managing Lync Server 2013, Persistent Chat Server
- Managing Voice Routing
- Managing Call Management Features
- Managing Meetings and Conferences
- Managing Devices, Phones, and Client Applications
- Managing Federation and External Access to Lync Server 2013
- Managing Lync Server 2013 Archiving
- Managing Lync Server 2013 Security and Authentication
- Managing the Lync Server 2013 Network Infrastructure
- Managing Enhanced 9-1-1 and the Location Service
- Managing Lync Server 2013 Services and Server Roles
- Managing Applications
- Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service
- Backing Up and Restoring Lync Server 2013
- Monitoring and Health Configuration
- Lync Server Management Shell
- Lync Server 2013 Best Practices Analyzer

⊟See Also

Other Resources

Deployment

1.7.1 Lync Server Administrative Tools

Lync Server Administrative Tools

See Also

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2013-02-21*

This topic describes the administrative tools for Lync Server 2013.

The administrative tools are installed by default on each Lync Server server. Additionally, you can install the administrative tools on other computers, such as dedicated administrative consoles. For procedures to install the administrative tools, see Install Lync Server Administrative Tools. For procedures to open the tools to perform management tasks, see Open Lync Server Administrative Tools.

Ensure that you review infrastructure, operating system, software, and administrator rights requirements before you install or use the Lync Server administrative tools. For details about infrastructure requirements, see Administrative Tools Infrastructure Requirements. For details about operating system and software requirements to install the Lync Server administrative tools, see Server and Tools Operating System Support, Additional Software Requirements, and Additional Server Support and Requirements. The user rights and permissions required to install and use the tools are described in Administrator Rights and Permissions Required for Setup and Administration.

The administrative tools consist of the following:

- **Lync Server Deployment Wizard** Use to deploy Lync Server and to install all administrative tools.
- **Lync Server Topology Builder** Use to define components in your deployment.
- **Lync Server Control Panel** Use for ongoing management of your deployment by using a web-based interface.
- **Lync Server Management Shell** Use for ongoing management of your deployment by using the command line.
- **Lync Server Logging tool** Use to troubleshoot problems in your deployment.
- **Centralized Logging Service** Collect logs and trace files from one computer, pool, site or global. Select and define scenarios that contain providers, flags and trace levels. Logging is collected, aggregated and displayed with tools such as any text-based tool or Snooper.exe.

You can manage your deployment by primarily using Topology Builder and Lync Server Control Panel.

Deployment Wizard

You must use the Lync Server Deployment Wizard included on the installation media to install all administrative tools onto a computer on which you have not already installed Lync Server. During the administrative tools installation process, the Lync Server Deployment Wizard is installed locally along with the other tools so that you can later use it to install files for additional components or remove files for components that you do not want on the computer.

For details about how to run the Lync Server Deployment Wizard for the first time from the Lync Server installation media, see Install Lync Server Administrative Tools.

Topology Builder

For details about deployment tasks that you can you perform by using Topology Builder, see the Deployment documentation for each server role.

Lync Server Control Panel

You can use Lync Server 2013 Control Panel to perform most of the administrative tasks required to manage and maintain Lync Server 2013. Lync Server Control Panel provides you with a graphical user interface (GUI) to manage the configuration of the servers running Lync Server, in addition to the users, clients, and devices in your organization. Lync Server Management Shell uses Lync Server Control Panel as the underlying mechanism to perform Lync Server configuration.

Lync Server Control Panel is automatically installed on every Lync Server Front End Server or Standard Edition server. In this release, you administer Edge Servers remotely. You can also install Lync Server Control Panel on another computer, such as a management console from which you want to centrally manage Lync Server. For details, see Install Lync Server Administrative Tools.

Important:

- To configure settings using Lync Server Control Panel, you must be logged in using an account that is assigned to the CsAdministrator role. For details about the predefined administrative roles available in Lync Server 2013, see Planning for Role-Based Access Control.
- To configure settings using Lync Server Control Panel, you must also use a computer with a minimum screen resolution of 1024 x 768.

Lync Server Management Shell

In Lync Server, the Lync Server Management Shell provides a new method for administration and management. Lync Server Management Shell is a powerful management interface, built on the Windows PowerShell command-line interface, that includes a comprehensive set of cmdlets that are specific to Lync Server. With Lync Server Management Shell, you gain a rich set of configuration and automation controls. Topology Builder and Lync Server Control Panel both implement subsets of these cmdlets to support management of Lync Server. The Lync Server Management Shell includes cmdlets for all Lync Server administration tasks, and you can use the cmdlets individually to manage your deployment. For details, see Lync Server Management Shell documentation or the command-line help for each cmdlet.

Logging Tool

The Lync Server Logging Tool facilitates troubleshooting by capturing logging and tracing information from the product while the product is running. You can use the tool to run debug sessions on any Lync Server server role. For details about the Logging Tool, see the Lync Server 2010 Logging Tool documentation on the TechNet Library at http://go.microsoft.com/fwlink/p/?linkId=199265.

Important:

The Centralized Logging Service is recommended for all logging collection over the Lync Server Logging Tool in all circumstances. The Lync Server Logging Tool will still work, but it will interfere or be rendered mostly ineffective if the Centralized Logging Service is already running. You should use only the Centralized Logging Service or the Lync Server Logging Tool, but never both concurrently. For more information on the Centralized Logging Service and why you should use it exclusively, see Using the Centralized Logging Service.

In This Section

- Administrative Tools Infrastructure Requirements
- Server and Tools Operating System Support
- Administrative Tools Software Requirements
- Administrator Rights and Permissions Required for Setup and Administration
- Requirements to Publish a Topology
- Install Lync Server Administrative Tools
- Open Lync Server Administrative Tools
- Troubleshooting Lync Server 2013 Control Panel
- Using the Centralized Logging Service

See Also

Other Resources

Lync Server Management Shell

1.7.1.1 Administrative Tools Infrastructure Requirements

Administrative Tools Infrastructure Requirements

See Also

Microsoft Lync Server 2013 > Operations > Lync Server Administrative Tools >

Topic Last Modified: *2012-09-27*

There are no additional infrastructure requirements for you to install Microsoft Lync Server 2013 administrative tools or perform most management tasks using these tools. For infrastructure requirements for specific scenarios, see the topics in this section.

- Requirements to Publish a Topology
- Planning for Simple URLs
- DNS Requirements for Simple URLs
- Edit or Configure Simple URLs

Related Sections

- Lync Server Management Shell

See Also

Tasks

Install Lync Server Administrative Tools

Concepts

Administrative Tools Software Requirements

Other Resources

Administrator Rights and Permissions Required for Setup and Administration

1.7.1.1.1 Requirements to Publish a Topology

Requirements to Publish a Topology

See Also

Deploying Lync Server 2013 > System Requirements > System Requirements for Administration Tools >

Topic Last Modified: *2013-02-21*

This topic describes the infrastructure and software requirements that are specific to publishing a topology, whether by using Topology Builder or the Lync Server 2013 Management Shell command-line interface. These requirements are in addition to the general operating system, software, and permissions requirements applicable to all Lync Server 2013 administrative tools. Make sure that you satisfy all administrative tools requirements before you publish a topology.

- You must run Topology Builder on a computer that is joined to the same domain or forest of the Lync Server 2013 deployment you are creating so that Active Directory Domain Services (AD DS) preparation steps are already completed, enabling you to use the administrative tools on that computer to successfully publish your topology.
- The computers defined in the topology must be joined to the domain, except for Edge Servers, and in AD DS. However, the computers do not need to be online when you publish the topology.
- The file share for the pool must be created and available to remote users.
- In order to publish an Enterprise Edition Front End pool, the SQL Server-based Back End Server must be joined to the domain in which you are deploying the servers, online, and configured with the appropriate firewall rules to make it available to remote users. For details about specifying firewall exceptions, see Understanding Firewall Requirements for SQL Server. For other details about configuring SQL Server, see Configure SQL Server for Lync Server 2013.

Note:

Standard Edition server has a collocated database that will accept the published configuration. You must first run the **Prepare first Standard Edition server** setup task in the Lync Server Deployment Wizard.

Tasks

Publish the Topology
Delegate Setup Permissions

Concepts

Administrative Tools Software Requirements
Server and Tools Operating System Support

Other Resources

Administrator Rights and Permissions Required for Setup and Administration

1.7.1.1.2 Planning for Simple URLs

Planning for Simple URLs

See Also

Microsoft Lync Server 2013 > Planning > Planning for Manageability and Virtualization >

Topic Last Modified: *2013-02-21*

Simple URLs make joining meetings easier for your users, and make getting to Lync Server administrative tools easier for your administrators.

Lync Server supports three simple URLs:

- **Meet** is used as the base URL for all conferences in the site or organization. An example of a Meet simple URL is https://meet.contoso.com. A URL for a particular meeting might be https://meet.contoso.com/*username*/7322994. With the Meet simple URL, links to join meetings are easy to comprehend, and easy to communicate and distribute.

- **Dial-in** enables access to the Dial-in Conferencing Settings webpage. This page displays conference dial-in numbers with their available languages, assigned conference information (that is, for meetings that do not need to be scheduled), and in-conference DTMF controls, and supports management of personal identification number (PIN) and assigned conferencing information. The Dial-in simple URL is included in all meeting invitations so that users who want to dial in to the meeting can access the necessary phone number and PIN information. An example of the Dial-in simple URL is https://dialin.contoso.com.
- **Admin** enables quick access to the Lync Server Control Panel. From any computer within your organization's firewalls, an admin can open the Lync Server Control Panel by typing the Admin simple URL into a browser. The Admin simple URL is internal to your organization. An example of the Admin simple URL is https://admin.contoso.com

Simple URL Scope

You can configure your simple URLs to have global scope, or you can specify different simple URLs for each central site in your organization. If both a global simple URL and a site simple URL are specified, the site simple URL has precedence.

In most cases, we recommend that you set simple URLs only at the global level, so that a user's Meet simple URL does not change if they move from one site to another. The exception would be organizations that need to use different telephone numbers for dial-in users at different sites. Note that if you set one simple URL (such as the Dial-in simple URL) at a site to be a site-level simple URL, you must also set the other simple URLs at that site to be site-level as well.

You can set global simple URLs in Topology Builder. To set a simple URL at the site level, you must use the Set-CsSimpleURLConfiguration cmdlet.

Naming Your Simple URLs

There are three recommended options for naming your simple URLs. Which option you choose has implications for how you set up your DNS A records and certificates which support simple URLs. In each option, you must configure one Meet simple URL for each SIP domain in your organization.

You always need just one simple URL in your whole organization for Dial-in, and one for Admin, no matter how many SIP domains you have.

For details about the necessary DNS A records and certificates, see DNS Requirements for Simple URLs and Certificate Requirements for Internal Servers in the Planning documentation.

In Option 1, you create a new SIP domain name for each simple URL.

If you use this option, you need a separate DNS A record for each simple URL, and each Meet simple URL must be named in your certificates.

Simple URL Naming Option 1

Simple URL	**Example**
Meet	https://meet.contoso.com, https://meet.fabrikam.com, and so on (one for each SIP domain in your organization)
Dial-in	https://dialin.contoso.com

Admin	https://admin.contoso.com

With Option 2, simple URLs are based on the domain name lync.contoso.com. Therefore, you need only one DNS A record which enables all three types of simple URLs. This DNS A record references lync.contoso.com. Additionally, you still need separate DNS A records for other SIP domains in your organization.

Simple URL Naming Option 2

Simple URL	Example
Meet	https://lync.contoso.com/Meet, https://lync.fabrikam.com/Meet, and so on (one for each SIP domain in your organization)
Dial-in	https://lync.contoso.com/Dialin
Admin	https://lync.contoso.com/Admin

Option 3 is most useful if you have many SIP domains, and you want them to have separate Meet simple URLs but want to minimize the DNS record and certificate requirements for these simple URLs.

Simple URL Naming Option 3

Simple URL	Example
Meet	https://lync.contoso.com/contosoSIPdomain/Meet https://lync.contoso.com/fabrikamSIPdomain/Meet
Dial-in	https://lync.contoso.com/Dialin
Admin	https://lync.contoso.com/Admin

Simple URL Naming and Validation Rules

Topology Builder and the Lync Server Management Shell cmdlets enforce several validation rules for your simple URLs. You are required to set simple URLs for Meet and Dialin, but setting one for Admin is optional. Each SIP domain must have a separate Meet simple URL, but you need only one Dialin simple URL and one Admin simple URL for your whole organization.

Each simple URL in your organization must have a unique name, and cannot be a prefix of another simple URL (for example, you could not set lync.contoso.com/Meet as your Meet simple URL and lync.contoso.com/Meet/Dialin as your Dialin simple URL). Simple URL names cannot contain the FQDN of any of your pools, or any port information (for example, https://FQDN:88/meet is not allowed). All simple URLs must start with the https:// prefix.

Simple URLs can contain only alphanumeric characters (that is, a-z, A-Z, 0-9, and the period (.). If you use other characters, the simple URLs might not work as expected.

Changing Simple URLs after Deployment

If you change a simple URL after initial deployment, you must be aware of how the change impacts your DNS records and certificates for simple URLs. If the base of a simple URL changes, then you must change the DNS records and certificates as well. For example, changing from https://lync.contoso.com/Meet to https://meet.contoso.com changes the base URL from lync.contoso.com to meet.contoso.com, so you would need to change the DNS records and certificates to refer to meet.contoso.com. If you changed the simple URL from https://lync.contoso.com/Meet to https://lync.contoso.com/Meetings, the base URL of lync.contoso.com stays the same, so no DNS or certificate changes are needed.

Whenever you change a simple URL name, however, you must run **Enable-CsComputer** on each Director and Front End Server to register the change.

⊟See Also

Concepts

DNS Requirements for Simple URLs

1.7.1.1.3 DNS Requirements for Simple URLs

DNS Requirements for Simple URLs

Planning > Network Planning for Lync Server > Domain Name System (DNS) Requirements >

Topic Last Modified: *2013-02-22*

Lync Server 2013 supports simple URLs, which make joining meetings easier for your users, and make getting to Lync Server administrative tools easier for your administrators. For details about simple URLs, see Planning for Simple URLs.

Lync Server supports the following three simple URLs: Meet, Dial-In, and Admin. You are required to set up simple URLs for Meet and Dial-In, and the Admin simple URL is optional. The Domain Name System (DNS) records that you need to support simple URLs depend on how you have defined these simple URLs, and whether you want to support disaster recovery for Simple URLs.

Simple URL Option 1

In Option 1, you create a new base URL for each simple URL.

Note:

When a user clicks a simple URL meeting link, the server that the DNS A record resolves to determines the correct client software to start. After the client software is started, it automatically communicates with the pool where the conference is hosted. This way, users are directed to the appropriate server for meeting content no matter which server or pool the simple URL DNS A records resolve to.

Simple URL Option 1

Simple URL	Example
Meet	https://meet.contoso.com, https://meet.fabrikam.com, and so on (one for each SIP domain in your organization)
Dial-in	https://dialin.contoso.com
Admin	https://admin.contoso.com

If you use Option 1, you must define the following:

- For each Meet simple URL, you need a DNS A record that resolves the URL to the IP address of the Director, if you have one deployed. Otherwise, it should resolve to the IP address of the load balancer of a Front End pool. If you have not deployed a pool and are using a Standard Edition server deployment, the

DNS A record must resolve to the IP address of one Standard Edition server in your organization.

If you have more than one SIP domain in your organization and you use this option, you must create Meet simple URLs for each SIP domain and you need a DNS A record for each Meet simple URL. For example, if you have both contoso.com and fabrikam.com, you will create DNS A records for both https://meet.contoso.com and https://meet.fabrikam.com.

Alternatively, if you have multiple SIP domains and you want to minimize the DNS record and certificate requirements for these simple URLs, use Option 3 as described later in this topic.

- For the Dial-in simple URL, you need a DNS A record that resolves the URL to the IP address of the Director, if you have one deployed. Otherwise, it should resolve to the IP address of the load balancer of a Front End pool. If you have not deployed a pool and are using a Standard Edition server deployment, the DNS A record must resolve to the IP address of one Standard Edition server in your organization.
- The Admin simple URL is internal only. It requires a DNS A record that resolves the URL to the IP address of the Director, if you have one deployed. Otherwise, it should resolve to the IP address of the load balancer of a Front End pool. If you have not deployed a pool and are using a Standard Edition server deployment, the DNS A record must resolve to the IP address of one Standard Edition server in your organization.

Simple URL Option 2

With Option 2, the Meet, Dial-in, and Admin simple URLs all have a common base URL, such as lync.contoso.com. Therefore, you need only one DNS A record for these simple URLs, which resolves lync.contoso.com to the IP address of a Director pool or Front End pool. If you have not deployed a pool and are using a Standard Edition server deployment, the DNS A record must resolve to the IP address of one Standard Edition server in your organization.

Note that if you have more than one SIP domain in your organization, you must still create Meet simple URLs for each SIP domain and you need a DNS A record for each Meet simple URL. In this example, while three simple URLs are all based on lync.contoso.com, an additional Meet simple URL for fabrikam.com is set up with a different base URL. In this example, you must create DNS A records for both https://lync.contoso.com and https://lync.fabrikam.com. Simple URL Option 3 shows another way to handle naming and DNS A records if you have multiple SIP domains.

Simple URL Option 2

Simple URL	Example
Meet	https://lync.contoso.com/Meet, https://lync.fabrikam.com/Meet, and so on (one for each SIP domain in your organization)
Dial-in	https://lync.contoso.com/Dialin
Admin	https://lync.contoso.com/Admin

Simple URL Option 3

Option 3 is most useful if you have many SIP domains, and you want them to have separate simple URLs but want to minimize the DNS record and certificate requirements for these simple URLs. In this example, you need only one DNS A record, which resolves lync.contoso.com to the IP address of a Director pool or Front End pool.

Simple URL Option 3

Simple URL	Example
Meet	https://lync.contoso.com/contosoSIPdomain/Meet https://lync.contoso.com/fabrikamSIPdomain/Meet
Dial-in	https://lync.contoso.com/contosoSIPdomain/Dialin
Admin	https://lync.contoso.com/contosoSIPdomain/Admin

Disaster Recovery Option for Simple URLs

If you have multiple sites that contain Front End pools and your DNS provider supports GeoDNS, you can set up your DNS records for Simple URLs to support disaster recovery, so that Simple URL functionality continues even if one entire Front End pool goes down. This disaster recovery feature supports the Meet and Dial-In simple URLs.

To configure this, create two GeoDNS addresses. Each address has two DNS A or CNAME records that resolve to two pools which are paired together for disaster recovery purposes. One GeoDNS address is used for internal access, and resolves to the internal web FQDN or load balancer IP address for the two pools. The other GeoDNS address is used for external access and resolves to the external web FQDN or load balancer IP address for the two pools. The following is an example for the Meet simple URL, using the FQDNs for the pools.

```
Meet-int.geolb.contoso.com
     Pool1InternalWebFQDN.contoso.com
     Pool2InternalWebFQDN.contoso.com
```

```
Meet-ext.geolb.contoso.com
     Pool1ExternalWebFQDN.contoso.com
     Pool2ExternalWebFQDN.contoso.com
```

Then create CNAME records that resolve your Meet simple URL (such as meet.contoso.com) to the two GeoDNS addresses.

Note:

If your network uses *hairpinning* (routing all your Simple URL traffic through the external link, including traffic that comes from within your organization), then you can just configure the external GeoDNS address and resolve your Meet simple URL to only that external address.

When you use this method, you can configure each GeoDNS address to use either a round robin method to distribute requests to the two pools, or to connect primarily to one pool (such as the pool located geographically closer) and use the other pool only in case of connectivity failure.

You can set up the same configuration for the Dial-In simple URL. To do so, create additional records like those in the previous example, substituting `dialin` for `meet` in the DNS records. For the Admin simple URL, use one of the three options listed earlier in this section.

Once this configuration is set up, you must use a monitoring application to set up HTTP monitoring to watch for failures. For external access, monitor to make sure that HTTPS

GET autodiscovery requests to the the external web FQDN or load balancer IP address for the two pools are successful. For example, the following requests must not contain any **ACCEPT** header and must return **200 OK**.

```
HTTPS GET Pool1ExternalWebFQDN.contoso.com/autodiscover/autodiscoverservice.svc/r
HTTPS GET Pool2ExternalWebFQDN.contoso.com/autodiscover/autodiscoverservice.svc/r
```

For internal access, you must monitor port 5061 on the internal web FQDN or load balancer IP address for the two pools. If any connectivity failures are detected, the VIP for these pools must close ports 80, 443 and 444.

1.7.1.1.4 Edit or Configure Simple URLs

Edit or Configure Simple URLs

See Also

Deployment > Deploying Lync Server 2013 > Defining and Configuring the Topology >

Topic Last Modified: *2013-02-21*

This procedure does not require membership in a local administrator or privileged domain group. You should log on to a computer as a standard user.

Lync Server 2013 uses simple URLs to direct internal and external calls to services on the Front End Server or on the Director, if one has been deployed. For more information about simple URLs, see Planning for Simple URLs in the Planning documentation. You can select the format for your simple URLs from several options. For details about these options, see DNS Requirements for Simple URLs in the Planning documentation.

By default, simple URLs will be configured in the form of (for example, the dial-in simple URL): https://dialin.<SIP Domain>

To configure simple URLs

1. In Topology Builder, right-click the **Lync Server 2013** node, and then click **Edit Properties**.
2. In the **Simple URLs** pane, select either **Phone access URLs:** (Dial-in) or **Meeting URLs:** (Meet) to edit, and then click **Edit URL**.
3. Update the URL to the value you want, and then click **OK** to save the edited URL. The example shown here has modified the Dial-in URL to https://pool01.contoso.net/dialin.
4. Edit the Meet URL by using the same steps, if necessary.

To define the optional Admin simple URL

1. In Topology Builder, right-click the **Lync Server 2013** node, and then click **Edit Properties**.
2. In the **Administrative access URL** box, enter the simple URL you want for administrative access to Lync Server 2013 Control Panel, and then click **OK**.

Tip:

We recommend using the simplest possible URL for the Admin URL. The simplest option is **https://admin.***<domain>*.

Important:

If you change a simple URL after initial deployment, you must be aware of what changes impact your Domain Name System (DNS) records and certificates for simple URLs. If the change impacts the base of a simple URL, then you must change the DNS records and certificates as well. For example, changing from https://lync.contoso.com/Meet to https://meet.contoso.com changes the base URL from lync.contoso.com to meet.contoso.com, so you would need to change the DNS records and certificates to refer to meet.contoso.com. If you changed the simple URL from https://lync.contoso.com/Meet to https://lync.contoso.com/Meetings, the base URL of lync.contoso.com stays the same, so no DNS or certificate changes are needed. Whenever you change a simple URL name, however, you must run the **Enable-CsComputer** cmdlet on each Director and Front End Server to register the change.

Concepts

Planning for Simple URLs

1.7.1.2 Server and Tools Operating System Support

Server and Tools Operating System Support

Microsoft Lync Server 2013 > Supportability > Server Software and Infrastructure Support >

Topic Last Modified: *2012-10-22*

All server roles support the same Windows Server operating systems. The required operating system support for other server roles, such as database servers, depends on what software you install on those servers.

Lync Server 2013 administrative tools are installed by default on the server running Lync Server 2013, but you can install administrative tools separately on other computers running Windows operating systems. For example, you can use a client computer running Windows 7 with Service Pack 1 (SP1) as an administrative console for planning purposes.

Important:

Lync Server 2013 is available only in 64-bit, which requires 64-bit hardware and 64-bit editions of Windows Server. This means that all server roles and computers running Lync Server 2013 administrative tools run a 64-bit edition operating system.

Operating Systems for Server Roles

Lync Server 2013 supports the 64-bit editions of the following operating systems:

- The Windows Server 2008 R2 with Service Pack 1 (SP1) Standard operating system (required) or latest service pack (recommended)
- The Windows Server 2008 R2 with SP1 Enterprise operating system (required) or latest service pack (recommended)
- The Windows Server 2008 R2 with SP1 Datacenter operating system (required) or latest service pack (recommended)
- The Windows Server 2012 Standard operating system
- The Windows Server 2012 Datacenter operating system

Lync Server 2013 is not supported on the following:

- The Server Core installation option of Windows Server 2008 R2 or Windows Server 2012
- The Windows Web Server 2008 R2 operating system or the Windows Web Server 2012 operating system
- Windows Server 2008 R2 HPC Edition or Windows Server 2012 HPC Edition

Operating Systems for Other Servers

Operating system support for servers other than those on which you deploy Lync Server

2013 server roles depends on the software that you plan to install on those servers. For details about requirements for Back End Servers and other database servers, see Database Software Support in the Supportability documentation. For details about requirements for reverse proxy servers (for Edge deployment), see Internet Information Services (IIS) Support in the Supportability documentation. For details about other software requirements, including infrastructure and virtualization support, see the other topics in the Server Software and Infrastructure Support section of the Supportability documentation.

Additional Operating Systems for Administrative Tools

Lync Server 2013 supports installation of the administrative tools, which includes the Topology Builder, on computers running any of the 64-bit editions of the operating systems supported for deployment of server roles (as described in the previous section). Additionally, you can install administrative tools on the 64-bit editions of the following operating systems:

- The Windows 7 operating system with SP1 operating system (required) or latest service pack (recommended)
- The Windows 8 operating or latest service pack (recommended)

1.7.1.3 Administrative Tools Software Requirements

Administrative Tools Software Requirements

Deploying Lync Server 2013 > System Requirements > System Requirements for Administration Tools >

Topic Last Modified: *2013-02-21*

This topic describes the software required to install and use Lync Server 2013 administrative tools in addition to the operating system requirements.

Microsoft .NET Framework 4.5

The 64-bit edition of Microsoft .NET Framework 4.5 is required for Lync Server 2013.

Windows PowerShell 3.0

Windows PowerShell 3.0 is required for running any component of Microsoft Lync Server 2013. For more information, see Installing Windows PowerShell 3.0.

Windows Installer Version 4.5

Lync Server 2013 uses Windows Installer technology to install, uninstall, and maintain various server roles. Windows Installer version 4.5 is available as a redistributable component for the Windows Server operating system. Windows Installer 4.5 ships with Windows Server 2012 and Windows Server 2008 R2, meaning that you do not need to download the utility for any computer that is running Lync Server 2013. (Lync Server 2013 can only be installed on computers running Windows Server 2012 or Windows Server 2008 R2.)

However, if you want to install Lync Server Management Shell or Lync Server Topology

Builder on an administrator workstation you might need to download Windows Installer 4.5. That utility ships with Windows 7 and Windows 2008 R2 but not with any previous versions of the Windows operating system. You can download Windows Installer 4.5 from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?linkid=197395.

Microsoft Silverlight 5 browser plug-in

Lync Server 2013 Control Panel is a web-based tool and requires that you install the latest version of Microsoft Silverlight 5 browser plug-in. When you start Lync Server 2013 Control Panel, if this software is not installed or if an earlier version is installed, Lync Server 2013 Control Panel prompts you to install the required version.

See Also

Concepts

Server and Tools Operating System Support

Other Resources

Administrative Tools Infrastructure Requirements
Administrator Rights and Permissions Required for Setup and Administration

1.7.1.4 Administrator Rights and Permissions Required for Setup and Administration

Administrator Rights and Permissions Required for Setup and Administration

Deployment > Deploying Lync Server 2013 > System Requirements >

Topic Last Modified: *2012-06-29*

Setup and deployment of Lync Server 2013 requires that the person installing and deploying the software be a member of local or domain-level groups. Administrative tools for Lync Server 2013 can require additional permissions.

- Group Membership Requirements
- Delegate Setup Permissions

1.7.1.4.1 Group Membership Requirements

Group Membership Requirements

Deploying Lync Server 2013 > System Requirements > Administrator Rights and Permissions Required for Setup and Administration >

Topic Last Modified: *2012-10-05*

The following table summarizes the group or groups that a person should belong to in order to successfully install, manage, and troubleshoot Lync Server 2013.

Lync Server 2013 Executable	Group Membership Required
Setup.exe – Executable that starts the installation of the Lync Server 2013 administrative tools.	Member of the Local Administrators group on the computer from which the executable is run. Member of Domain Users group to read information in Active Directory Domain Services (AD DS). This level of permission is required because the automatic installation of required MSI packages on

	the local computer requires privileges that allow reading from and writing to protected local computer resources such as Program Files directories, and protected registry such as the Local Machine hive. **Tip:** You can also delegate setup permissions to users or groups to whom you do not want to grant membership in the Domain Admins group. For details, see Granting Setup Permissions in the Deployment documentation.
Deploy.exe – Called by setup.exe, deploy.exe is responsible for the deployment of the software components for the server roles.	Member of the Local Administrators group on the computer from which the executable is run. Member of Domain Users group to read information in AD DS. This level of permission is required because the automatic installation of required MSI packages on the local computer requires privileges that allow reading from and writing to protected local computer resources such as Program Files directories, and protected registry such as the Local Machine hive. Membership in RtcUniversalReadOnlyAdmins group is necessary to read the Central Management store. **Note:** If you are running the Windows Vista operating system or Windows 7 operating system, you will be prompted by User Account Control (UAC) to proceed with installation. If you are logged on with a standard user account, you will need someone who is a member of the Local Administrators group to provide credentials when prompted for an account with permissions to install the software.
Bootstrapper.exe – Called by setup.exe, bootstrapper.exe is responsible for deployment and configuration of server roles.	Member of the Local Administrators group on the computer from which the executable is run. Member of the RTCUniversalServerAdmins group to run Bootstrapper.exe. Member of Domain Users group to read information in AD DS. This level of permission is required because the automatic installation of required MSI packages on the local computer requires privileges that allow reading from and writing to protected local computer resources such as Program Files directories, and protected registry such as the Local Machine hive.
TopologyBuilder – Wizard-driven user interface to create, view, adjust, and validate Lync Server 2013 topologies.	Member of the Local Administrators group on the computer from which the executable is run to view the topology. Member of the RTCUniversalServerAdmins group to change configuration settings. Member of the RTCUniversalServerAdmins group and Domain Admins group, or member of the RTCUniversalServerAdmins group (only if the group has been granted delegate setup permissions), to publish the topology. For details about delegating setup permissions to allow members of the RTCUniversalServerAdmins group to publish the

	topology without being members of the Domain Admins group, see Granting Setup Permissions in the Deployment documentation.
AdminUIHost – Web-based graphical user interface for managing Lync Server 2013.	Member of CsAdministrator group or member of another role-based access control (RBAC) role to which the specific administrative task is assigned. Lync Server 2013 Control Panel implements configuration changes by running Lync Server 2013 Management Shell cmdlets. For a list of predefined roles and the cmdlets members are permitted to run, see Planning for Role-Based Access Control in the Planning documentation.
PowerShell.exe with the Lync Server 2013 module loaded – Command-line administrative tool with cmdlets specific to management of Lync Server 2013.	Member of CsAdministrator group or member of another RBAC role to which the specific cmdlet has been assigned. For a list of predefined roles and the cmdlets members are permitted to run, see Planning for Role-Based Access Control in the Planning documentation. Or, member of one or more of the following groups, depending on the cmdlet: • RTCUniversalServerAdmins • RTCUniversalUserAdmins • RTCUniversalReadOnlyAdmins

1.7.1.4.2 Delegate Setup Permissions

Delegate Setup Permissions

Deploying Lync Server 2013 > System Requirements > Administrator Rights and Permissions Required for Setup and Administration >

Topic Last Modified: *2012-10-01*

If you do not want to grant membership in the Domain Admins group to users or groups who are deploying Lync Server 2013, you can enable members of the RTCUniversalServerAdmins group to run the **Enable-CsTopology** Windows PowerShell cmdlet on servers running Lync Server 2013. By default, members of the RTCUniversalServerAdmins group do not have the ability to run this cmdlet. You grant administrator rights and permissions to run **Enable-CsTopology** on servers running Lync Server by using the **Grant-CsSetupPermission** cmdlet and specifying an organizational unit (OU) where computer objects for the server running Lync Server 2013 are located.

Note:

Enable-CsTopology is the key cmdlet to allow the RTCUniversalServerAdmins group members to set up and deploy Lync Server 2013.

To add the ability to run Enable-CsTopology to the RTCUniversalServerAdmins group

1. Log on to a server as a member of the Domain Admins group for the domain on which the delegated user will run **Enable-CsTopology**.
2. Open the Lync Server 2013 Management Shell. The Lync Server 2013 Management Shell is automatically installed on each Front End Server or any computer where the Lync Server 2013 administrative tools have been installed. For details about the Lync Server 2013 Management Shell, see Lync

Server Management Shell in the Operations documentation.

3. Run the following cmdlet from the Lync Server 2013 Management Shell:

```
Grant-CsSetupPermission -ComputerOU <DN of the OU> -Domain <Domain FQD
```

Note:

If the OU is not top level, you must provide the full domain name.

In the following example, the OU is “Lync Servers,” which is in the contoso.com domain.

```
Grant-CsSetupPermission -ComputerOU "OU=Lync Servers" -Domain contoso.
```

1.7.1.5 Requirements to Publish a Topology

Requirements to Publish a Topology

See Also

Deploying Lync Server 2013 > System Requirements > System Requirements for Administration Tools >

Topic Last Modified: *2013-02-21*

This topic describes the infrastructure and software requirements that are specific to publishing a topology, whether by using Topology Builder or the Lync Server 2013 Management Shell command-line interface. These requirements are in addition to the general operating system, software, and permissions requirements applicable to all Lync Server 2013 administrative tools. Make sure that you satisfy all administrative tools requirements before you publish a topology.

- You must run Topology Builder on a computer that is joined to the same domain or forest of the Lync Server 2013 deployment you are creating so that Active Directory Domain Services (AD DS) preparation steps are already completed, enabling you to use the administrative tools on that computer to successfully publish your topology.
- The computers defined in the topology must be joined to the domain, except for Edge Servers, and in AD DS. However, the computers do not need to be online when you publish the topology.
- The file share for the pool must be created and available to remote users.
- In order to publish an Enterprise Edition Front End pool, the SQL Server-based Back End Server must be joined to the domain in which you are deploying the servers, online, and configured with the appropriate firewall rules to make it available to remote users. For details about specifying firewall exceptions, see Understanding Firewall Requirements for SQL Server. For other details about configuring SQL Server, see Configure SQL Server for Lync Server 2013.

Note:

Standard Edition server has a collocated database that will accept the published configuration. You must first run the **Prepare first Standard Edition server** setup task in the Lync Server Deployment Wizard.

Tasks

Publish the Topology
Delegate Setup Permissions

Concepts

Administrative Tools Software Requirements
Server and Tools Operating System Support

Other Resources

Administrator Rights and Permissions Required for Setup and Administration

1.7.1.6 Install Lync Server Administrative Tools

Install Lync Server Administrative Tools

See Also

Deployment > Deploying Lync Server 2013 > Preparing the Infrastructure and Systems >

Topic Last Modified: *2013-02-21*

This topic describes how to install the administrative tools you need to use to deploy and manage Lync Server 2013. The administrative tools are installed by default on each server running Lync Server 2013. Additionally, you can install the administrative tools on other computers, such as dedicated administrative consoles. We strongly recommend that you install the administrative tools on a computer that is in the same domain or forest as the Lync Server 2013 deployment you are creating because by doing so you make sure that Active Directory Domain Services (AD DS) preparation steps are already complete, which enables you to use the administrative tools on that computer later to publish your topology.

Make sure that you review infrastructure, operating system, software, and administrator rights requirements before you install or use the Lync Server 2013 administrative tools. For details about infrastructure requirements, see Administrative Tools Infrastructure Requirements. For details about operating system and software requirements to install the Lync Server 2013 administrative tools, see Server and Tools Operating System Support, Additional Software Requirements, and Additional Server Support and Requirements. For details about the user rights and permissions required to install and use the tools, see Administrator Rights and Permissions Required for Setup and Administration.

> ◆**Important:**
>
> If your organization requires that you locate Internet Information Services (IIS) and all Web Services on a drive other than the system drive, you can change the installation location path for the Lync Server files in the Setup dialog box. If you install the Setup files to this path, including OCSCore.msi, the rest of the Lync Server 2013 files will be deployed to this drive as well.

⊟To install the Lync Server 2013 administrative tools

1. Log on as a local administrator (minimum requirement) to the computer where you want to install the administrative tools. If you are logged on as an a standard user on the Windows Vista or Windows 7 operating systems, and User Account Control (UAC) is enabled, you will be prompted for the local administrator or a domain equivalent user name and password.
2. Locate the installation media on your computer, and then double-click \Setup\amd64\Setup.exe.
3. If you are prompted to install the Microsoft Visual C++ 2008 distributable, click **Yes**.
4. On the **Microsoft Lync Server 2013 Installation Location** page, click **OK**. Change this path to another location or drive if you need to have the files installed to another location.

   > ◆**Important:**
   >
   > If your organization requires that you locate Internet Information Services (IIS) and all Web Services on a drive other than the system drive, you can change the installation location path for the Lync Server 2013 files in the Setup dialog box. If you install the Setup files to this path, including OCSCore.msi, the rest of the Lync Server 2013 files will be deployed to this drive too.

5. On the **End User License Agreement** page, review the license terms, click **I accept**, and then click **OK**. This step is required before you can continue.

6. On the **Microsoft Lync Server 2013 – Deployment Wizard** page, click **Install Administrator Tools**.
7. When the installation successfully completes, click **Exit**.

Tasks

Open Lync Server Administrative Tools

Concepts

Lync Server Administrative Tools

1.7.1.7 Open Lync Server Administrative Tools

Open Lync Server Administrative Tools

See Also

Microsoft Lync Server 2013 > Operations > Lync Server Administrative Tools >

Topic Last Modified: *2012-06-28*

You can use the procedures in this topic to open administrative tools to deploy, configure, or troubleshoot your Lync Server 2013 topology.

- Deployment Wizard
- Topology Builder
- Lync Server Control Panel
- Lync Server Management Shell

Deployment Wizard

Use the following procedure to start the Deployment Wizard locally to add or remove Lync Server 2013 component files.

⊟To start Lync Server 2013 Deployment Wizard

1. Log on to the computer where the Lync Server Deployment Wizard is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Deployment Wizard**.

Topology Builder

Use the following procedure to open the Topology Builder to define the servers that you want to deploy in your Lync Server 2013 topology.

⊟To open Lync Server 2013 Topology Builder to design the topology

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.

Note:
You can define a topology by using an account that is a member of the local Users group, but to read, publish, or enable a topology, which is required to install Lync Server 2013 on a server, you must use an account that is a member of the Domain Admins group and the RTCUniversalServerAdmins group, and that has full control permissions (that is, read, write, and modify) on the file share that you are going to use for the archiving file store so that Topology Builder can configure the required discretionary access control list (DACLs), or an account with equivalent user rights.

2. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync**

Server 2013, and then click **Lync Server Topology Builder**.

Lync Server 2013 Control Panel

Use one of the following procedures to open Lync Server 2013 Control Panel to manage the configuration of servers, users, clients, and devices in your environment.

Note:

You can use a user account that is assigned to the CsAdministrator role to perform any task in Lync Server 2013 Control Panel. You can use other roles to log on to Lync Server 2013 Control Panel to perform specific administration tasks, dependent on the task you need to perform. For example, you can use CSArchivingAdministrator to administer Archiving in Lync Server 2013 Control Panel. For details about roles, see Planning for Role-Based Access Control in the Planning documentation. For details about the roles that you can use to perform a specific task, see the documentation for the task.

⊟To open Lync Server 2013 Control Panel from any computer inside your organization’s firewall

1. From a user account that is assigned to the CsAdministrator role or other role that has appropriate user rights and permissions for the task to be performed, log on to any computer in your internal deployment with a minimum screen resolution of 1024 x 768.

   Important:

   If you have configured an administration simple uniform resource locator (URL), you can access Lync Server 2013 Control Panel from an Internet browser that is running on any computer within your organization’s firewall. For details about configuring the administration simple URL, see Planning for Simple URLs in the Planning documentation and Edit or Configure Simple URLs in the Deployment documentation.

2. Open a browser window, and then enter the Admin URL configured for your organization.

⊟To open Lync Server 2013 Control Panel on a computer running Lync Server 2013

1. From a user account that is a member of the CsAdministrator role or other role that has appropriate user rights and permissions for the task to be performed, log on to a computer on which you have installed Lync Server 2013 or, at a minimum, the Lync Server 2013 administrative tools. To configure settings, the computer must have a minimum screen resolution of 1024 x 768.
2. Start Lync Server 2013 Control Panel: Click **Start**, click **All Programs**, point to **Administrative Tools**, point to **Microsoft Lync Server 2013**, and then click **Lync Server 2013 Control Panel**.

Lync Server 2013 Management Shell

Use the following procedure to open Lync Server 2013 Management Shell to administer servers, users, clients, and devices in your environment by using the command line.

Note:

You can use a user account that is assigned to the CsAdministrator role to perform any task in Lync Server 2013 Management Shell. You can log on using other roles to perform specific administration tasks, depending on the task you need to perform. For example, you can use CSArchivingAdministrator to run cmdlets related to Archiving administration. For details about roles, see Planning for Role-Based Access Control in the Planning documentation. For details about the roles that you can use to run a specific cmdlet, see the documentation for the cmdlet.

You can also run certain cmdlets by using a user account in the RTCUniversalServerAdmins, RTCUniversalUserAdmins, or RTCUniversalReadOnlyAdmins groups, depending on the cmdlet.

⊟To open the Lync Server 2013 Management Shell

- If you open a Windows PowerShell window rather than the Lync Server 2013 Management Shell, by default you cannot run the Lync Server 2013 cmdlets. To run the Lync Server 2013 cmdlets from within Windows PowerShell, type the following at the Windows PowerShell command prompt:
  ```
  Import-Module Lync
  ```
- Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

⊟See Also

Tasks

Install Lync Server Administrative Tools

Concepts

Lync Server Administrative Tools

1.7.1.8 Troubleshooting Lync Server 2013 Control Panel

Troubleshooting Lync Server 2013 Control Panel

See Also

Microsoft Lync Server 2013 > Operations > Lync Server Administrative Tools >

***Topic Last Modified:** 2013-02-21*

This topic provides information and procedures that can help you troubleshoot access to Lync Server 2013 Control Panel.

Internet Browser Requirements

Lync Server Control Panel requires that Microsoft Silverlight browser plug-in version 4.0.50524.0 or latest version is installed. If Silverlight is not installed or if an earlier version is installed, follow the instructions in the message to install the required version.

Note:

Other software requirements for Lync Server Control Panel pertain to the operating system on which Lync Server Control Panel and all other Lync Server 2013 administrative tools can be installed. For details, see Server and Tools Operating System Support in the Supportability documentation.

If your Internet browser blocks installation of Silverlight due to security considerations, add the Uniform Resource Locator (URL) that opens Lync Server Control Panel to the list of trusted sites. In Internet Explorer security settings, ensure that **Run ActiveX controls and plug-ins** is set to **Enabled**. For details, see http://go.microsoft.com/fwlink/p/?linkId=214060. Furthermore, ensure that the browser is configured to use SSL 3.0.

If the Internet browser is configured to use a proxy server, verify that the browser is configured to bypass the proxy server for sites that are automatically detected as internal sites. Or, add the address to the browser's exception list in the proxy server configuration settings.

DNS Record and Certificate Requirements for the Administrative Access URL

If you configured a simple URL to access Lync Server Control Panel, ensure that you also configured the static Domain Name System (DNS) host (A) resource record and certificate necessary to use that administrative access URL. If you change the base URL at any time, ensure that the change is reflected in the appropriate DNS record and certificate and that you run the *Enable-CsComputer* on each Director and Front End Server to register the change. For details, see the following topics in the Planning documentation:

- Planning for Simple URLs
- DNS Requirements for Simple URLs
- Certificate Requirements for Internal Servers

For step-by-step procedures to configure the administrative access URL, see Edit or Configure Simple URLs in the Deployment documentation.

Note:

If you have more than one network adapter on the web server, you must manually configure DNS for each additional network adapter in order for DNS resolution to function properly.

Internet Information Services (IIS) Requirements

Lync Server Control Panel is one of the components of Lync Server 2013 that requires Internet Information Services (IIS). In particular, ensure that HTTP redirection and Windows authentication features are enabled, and that the World Wide Web Publishing Service (W3SVC) is running.

World Wide Publishing Service (Windows Service) Dependency

When the World Wide Web Publishing Service is stopped, you cannot access Lync Server Control Panel. You can restart the service by using the Windows Services Microsoft Management Console (MMC).

To start the World Wide Web Publishing Service

1. Log on to the computer where the World Wide Web Publishing Service is installed as part of Internet Information Services (IIS).
2. Click **Start**, click **Administrative Tools**, and then click **Services**.
3. Right-click **World Wide Web Publishing Service**, and then click **Start**.

Application Pool Mode

Configure IIS so that the CsManagementAppPool application pool uses the Network Service account as its process model identity.

User Rights and Permissions

You must sign in to Lync Server Control Panel either by using a domain account that is a member of the CsAdministrator group or by using an account to which you have delegated user rights and permissions. You cannot sign in to Lync Server Control Panel by using a local machine account. For details about delegating administrative tasks through role-based access control (RBAC), see Planning for Role-Based Access Control in the Planning documentation.

If you use a simple URL to access Lync Server Control Panel, ensure that web servers are added to the RTCUniversalServerAdmins and RTCUniversalUserAdmins groups.

⊟See Also

Concepts

Lync Server Administrative Tools

1.7.1.9 Using the Centralized Logging Service

Using the Centralized Logging Service

Microsoft Lync Server 2013 > Operations > Lync Server Administrative Tools >

Topic Last Modified: *2012-11-01*

The Centralized Logging Service is a new feature in Lync Server 2013. It is an enhanced replacement for the **OCSLogger** and **OCSTracer** tools that were provided in previous releases. You can use the Centralized Logging Service to perform the following tasks:

- Start logging on one or more computers and pools from a single location and command.
- Stop logging on one or more computers and pools from a single location and command.
- Search logs on one or more computers and pools for a single location and command. You can tailor the search command to return the entire aggregation of logs that were captured and stored on all machines, or return a trimmed-down result that captures specific data.
- Configure logging sessions as follows:
  - Define a **Scenario**, or use a default scenario. A *scenario* in Centralized Logging Service is made up of scope (global or site), a scenario name to identify the purpose of the scenario, and one or more providers. You can run two scenarios at any given time on a computer.
  - Use an existing *provider* or create a new provider. A *provider* defines what the logging session collects, what level of detail, what components to trace, and what flags are applied.

    Tip:

    If you are familiar with OCSLogger, the term *providers* refers to the collection of **components** (for example, S4, SIPStack), a **logging type** (for example, WPP, EventLog, or IIS logfile), a **tracing level** (for example, All, verbose, debug), and **flags** (for example, TF_COMPONENT, TF_DIAG). These items are defined in the provider (a Windows PowerShell variable) and passed into the Centralized Logging Service command.

  - Configure the computers and pools that you want to collect logs from.
  - Define the scope for the logging session from the options **Site** (run logging captures on computers in that site only), or **Global** (run logging capture on all computers in the deployment).

The Centralized Logging Service is extremely powerful and can meet nearly all of the needs for troubleshooting problems—large or small. From root cause analysis to performance problems, the Centralized Logging Service can be an important tool for any administrator. All examples are shown using the Lync Server Management Shell. There is a command-line component for the Centralized Logging Service called **CLSController.exe**. Help is provided for the command-line tool through the tool itself. However, there is a limited set of functions that you can execute from the command line. By using Lync Server Management Shell, you have access to a much larger and much more configurable set of features. You should always consider Lync Server Management Shell as the first and foremost method when using the Centralized Logging Service.

The topics in this section explain how to use the Centralized Logging Service and examples of how to use its many features.

- Overview of the Centralized Logging Service
- Managing the Centralized Logging Service Configuration Settings
- Understanding Centralized Logging Service Configuration Settings
- Using Start for the Centralized Logging Service to Capture Logs
- Using Stop for the Centralized Logging Service
- Using Search on Capture Logs Created by the Centralized Logging Service
- Reading Capture Logs From the Centralized Logging Service

1.7.1.9.1 Overview of the Centralized Logging Service

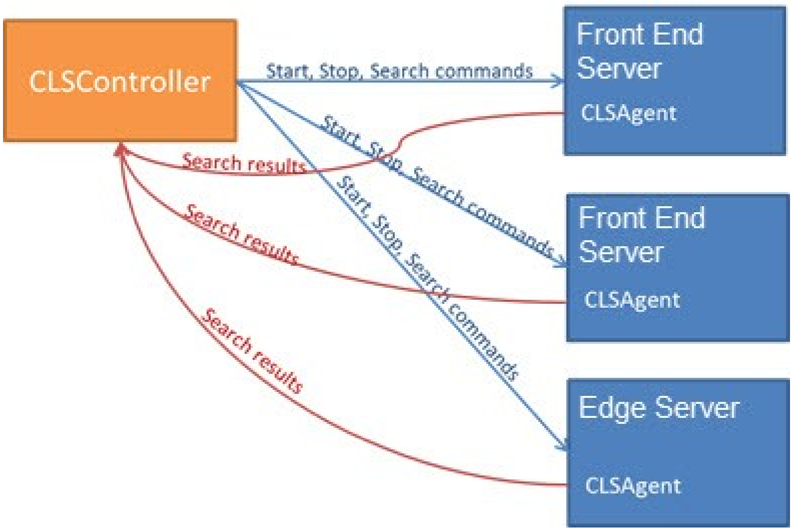
Overview of the Centralized Logging Service

Operations > Lync Server Administrative Tools > Using the Centralized Logging Service >

Topic Last Modified: *2013-02-22*

The Centralized Logging Service is designed to provide a means for controlled collection of data—with a broad or narrow scope. You can collect data from all servers in the deployment concurrently, define specific elements to trace, set trace flags and return search results from a single computer or an aggregation of all data from all servers. The Centralized Logging Service runs on all servers in your deployment. The architecture of the Centralized Logging Service is comprised of the following agents and services:

- *Centralized Logging Service Agent* ClsAgent.exe is the service executable that communicates with the controller and receives the commands that the controller is issued by the administrator. The agent is run as a service on each Lync Server computer. When the agent receives a command, it executes the command, sends messages to the defined components for tracing, and writes the trace logs to disk. It also reads the trace logs for its computer and sends the trace data back to the controller when requested. The ClsAgent listens for commands on the following ports: **TCP 50001**, **TCP 50002**, and **TCP 50003**.
- *Centralized Logging Service Controller* ClsControllerLib.dll is the command execution engine for the Lync Server Management Shell and for ClsController.exe. CLSControllerLib.dll sends Start, Stop, Flush, and Search commands to the ClsAgent. When search commands are sent, the resulting logs are returned to the ClsControllerLib.dll and aggregated. The controller is responsible for sending commands to the agent, receiving the status of those commands and managing the search log file data as it is returned from all agents on any computer in the search scope, and aggregating the log data into a meaningful and ordered output set. The information in the following topics is focused on using the Lync Server Management Shell. ClsController.exe is limited to a subset of the features and functions that are available in the Lync Server Management Shell. Help for ClsController.exe is available at the command line by typing `ClsController` in the default directory C:\Program Files\Common Files\Microsoft Lync Server 2013\ClsAgent.



You issue commands using the Windows Server command-line interface or using the Lync Server Management Shell. The commands are executed on the computer you are logged in to and sent to the ClsAgent locally or to the other computers and pools in your deployment.

ClsAgent maintains an index file of all .CACHE files that it has on the local machine. ClsAgent allocates them so that they are evenly distributed across volumes defined by the option CacheFileLocalFolders, never consuming more than 80% of each volume (that is, the local cache location and the percentage is configurable using the **Set-CsClsConfiguration** cmdlet). ClsAgent is also responsible for aging old cached event trace log (.etl) files off the local machine. After two weeks (that is, the timeframe is configurable using the **Set-CsClsConfiguration** cmdlet) these files are copied to a file share and deleted from the local computer. For details, see Set-CsClsConfiguration. When a search request is received, the search criteria is used to select the set of cached .etl files to perform the search based on the values in the index maintained by the agent.

Note:

Files that are moved to the file share from the local computer can be searched by ClsAgent. Once ClsAgent moves the files to the file share, the aging and removal of files is not maintained by ClsAgent. You should define an administrative task to monitor the size of the files in the file share and delete them or archive them.

The resulting log files can be read and analyzed using a variety of tools, including **Snooper.exe** and any tool that can read a text file, such as **Notepad.exe**. Snooper.exe is part of the Lync Server 2013 Debug Tools and is available as a Web download from http://go.microsoft.com/fwlink/?LinkId=285257.

Like OCSLogger, the Centralized Logging Service has several components to trace against, and provides options to select flags, such as TF_COMPONENT and TF_DIAG. Centralized Logging Service also retains the logging level options of OCSLogger.

The most important advantage to using the Lync Server Management Shell over the command-line ClsController is that you can configure and define new scenarios using selected providers that target the problem space, custom flags, and logging levels. The scenarios available to ClsController are limited to those that are defined for the executable.

In previous versions, OCSLogger.exe was provided to enable administrators and support personnel to collect trace files from computers in the deployment. OCSLogger, for all of its strengths, had a shortcoming. You could only collect logs on one computer at a given time. You could log on to multiple computers by using separate copies of OCSLogger, but you ended up with multiple logs and no easy way to aggregate the results.

When a user requests a log search, the ClsController determines which machines to send the request to (that is, based on the scenarios selected). It also determines whether the search needs to be sent to the file share where the saved .etl files are located. When the search results are returned to the ClsController, the controller merges the results into a single time-ordered result set that is presented to the user. Users can save the search results to their local machine for further analysis.

When you start a logging session, you specify scenarios that are relative to the problem that you are trying to resolve. You can have two scenarios running at any time. One of these two scenarios should be the AlwaysOn scenario. As the name implies, it should always be running in your deployment, collecting information on all computers, pools, and components.

Important:

By default, the AlwaysOn scenario is not running in your deployment. You must explicitly start the scenario. Once started, it will continue to run until explicitly stopped, and the running state will persist through reboots of the computers. For details on starting and stopping scenarios, see Using Start for the Centralized Logging Service to Capture Logs and Using Stop for the Centralized Logging Service.

When a problem occurs, start a second scenario that relates to the problem reported. Reproduce the problem, and stop the logging for the second scenario. Begin your log searches relative to the problem reported. The aggregated collection of logs produces a log file that contains trace messages from all computers in your site or global scope of your deployment. If the search returns more data than you can feasibly analyze (typically known as a signal-to-noise ratio, where the noise is too high), you run another search with narrower parameters. At this point, you can begin to notice patterns that show up and can help you get a clearer focus on the problem. Ultimately, after you perform a couple of refined searches you can find data that is relevant to the problem and figure out the root cause.

Tip:

When presented with a problem scenario in Lync Server, start by asking yourself “What do I already know about the problem?” If you quantify the problem boundaries, you can eliminate a large part of the operational entities in Lync Server.
Consider an example scenario where you know that users are not getting current results when looking for a contact. There is no point in looking for problems in the media components, Enterprise Voice, conferencing, and a number of other components. What you may not know is where the problem actually is: on the client, or is this a server-side problem? Contacts are collected from Active Directory by the User Replicator and delivered to the client by way of the Address Book Server (ABServer). The ABServer gets its updates from the RTC database (where User Replicator wrote them) and collects them into address book files, by default – 1:30 AM. The Lync Server clients retrieve the new address book on a randomized schedule. Because you know how the process works, you can reduce your search for the potential cause to an issue related to data being collected from Active Directory by the User Replicator, the ABServer not retrieving and creating the address book files, or the clients not downloading the address book file.

1.7.1.9.2 Managing the Centralized Logging Service Configuration Settings

Managing the Centralized Logging Service Configuration Settings

See Also

Operations > Lync Server Administrative Tools > Using the Centralized Logging Service >

Topic Last Modified: *2012-11-01*

The Centralized Logging Service is controlled and configured by settings and parameters that are created and used by the Centralized Logging Service Controller (CLSController) to send commands to the individual computer's Centralized Logging Service Agent (CLSAgent). The agent processes the commands that are sent to it and (in the case of a Start command) uses the configuration of the scenarios, providers, log size, trace duration, and flags to begin collecting trace logs according to the configuration information provided.

Important:

Not all Windows PowerShell cmdlets listed for the Centralized Logging Service are intended for use with Lync Server 2013 on-premises deployments. Although they may appear to work, the following cmdlets are not designed to function with Lync Server 2013 on-premises deployments:

- **CsClsRegion cmdlets:** Get-CsClsRegion, Set-CsClsRegion, New-CsClsRegion, and Remove-CsClsRegion.
- **CsClsSearchTerm cmdlets:** Get-CsClsSearchTerm and Set-CsClsSearchTerm.
- **CsClsSecurityGroup cmdlets:** Get-CsClsSecurityGroup, Set-CsClsSecurityGroup, New-CsClsSecurityGroup, and Remove-CsClsSecurityGroup.

The settings defined in these cmdlets will not hinder or cause any adverse behavior, but they are designed for use with Microsoft Office 365 and will not yield the expected results in on-premises deployments. This is not to say that there is no use for these cmdlets in on-premises deployments, but their use is a more advanced topic that is not covered in this documentation.

The topics in this section define the configuration options, parameters, and settings for the Centralized Logging Service. Information about how to configure the Centralized Logging Service, how to retrieve the configuration settings, creation of scenarios, management of security groups for Centralized Logging Service, searching, and more is contained in the following topics.

- Managing Computer, Site and Global Centralized Logging Service Configuration
- Configuring Providers for Centralized Logging Service
- Configuring Scenarios for the Centralized Logging Service

See Also

Concepts

Overview of the Centralized Logging Service
Centralized Logging Cmdlets

1.7.1.9.2.1 Managing Computer, Site and Global Centralized Logging Service Configuration

Managing Computer, Site and Global Centralized Logging Service Configuration

See Also

Lync Server Administrative Tools > Using the Centralized Logging Service > Managing the Centralized Logging Service Configuration Settings >

Topic Last Modified: *2013-02-21*

The Centralized Logging Service can be run at a scope that includes a single computer, a pool of computers, at a site scope (that is, a defined site such as the site Redmond that contains a collection of computer and pools in your deployment), or at a global scope (that is, all computers and pools in your deployment).

To configure the Centralized Logging Service scope by using the Lync Server Management

Shell, you must be a member of either the CsAdministrator or the CsServerAdministrator role-based access control (RBAC) security groups, or a custom RBAC role that contains either of these two groups. To return a list of all the RBAC roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Lync Server Management Shell or the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "<Lync Server 2013 cmdlet>"}
```

For example:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Set-CsClsConfiguration"}
```

Note:

Windows PowerShell provides you more options and additional configuration options that are not available by using CLSController.exe. CLSController offers a quick, concise method to run commands, but is limited to the set of commands available for the CLSController. Windows PowerShell is not limited to just the command available to the command processor of the CLSController, and provides a wider set of commands and a richer set of options. For example, CLSController.exe does provide you with a scope options for –computers and –pools. With Windows PowerShell, you can indicate computers or pools in most commands, and when you define new scenarios (CLSController has a finite number of scenarios that are not user modifiable) you can define a site or global scope. This powerful feature of Windows PowerShell enables you to define a scenario a site or global scope, but limit the actual logging to a computer or pool.

There are fundamental differences between the command-line commands that you can run in Windows PowerShell or CLSController. Windows PowerShell provides a rich method to configure and define scenarios, and to reuse those scenarios in a meaningful way for your troubleshooting scenarios. While CLSController does provide a fast and efficient way to issue commands and get results, the command set for CLSController is limited by the finite commands that you have available from the command line. Unlike the Windows PowerShell cmdlets, CLSController cannot define new scenarios, manage scope at a site or global level, and many other limitations of a finite command set that cannot be dynamically configured. While CLSController provides a means for fast execution, Windows PowerShell provides a means to extend the Centralized Logging Service functionality beyond what is possible with CLSController.

A single computer scope can be defined during the execution of a Search-CsClsLogging, Show-CsClsLogging, Start-CsClsLogging, Stop-CsClsLogging, Sync-CsClsLogging and Update-CsClsLogging command using the –Computers parameter. The –Computers parameter accepts a comma separated list of fully qualified domain names (FQDNs) for the target computer.

Tip:

You can also define –Pools and a comma separated list of pools that you want to run the logging commands on.

Site and Global scopes are defined in the **New-**, **Set-**, and **Remove-** Centralized Logging Service cmdlets. The following examples demonstrate how to set a site and a global scope.

Important:

The commands shown may contain parameters and concepts that are covered in other sections. The example commands are intended to demonstrate the use of the **–Identity** parameter to define scope, and the other parameters are included for completeness and to specify the scope. For details about the **Set-CsClsConfiguration** cmdlets, see Set-CsClsConfiguration in the Operations documentation.

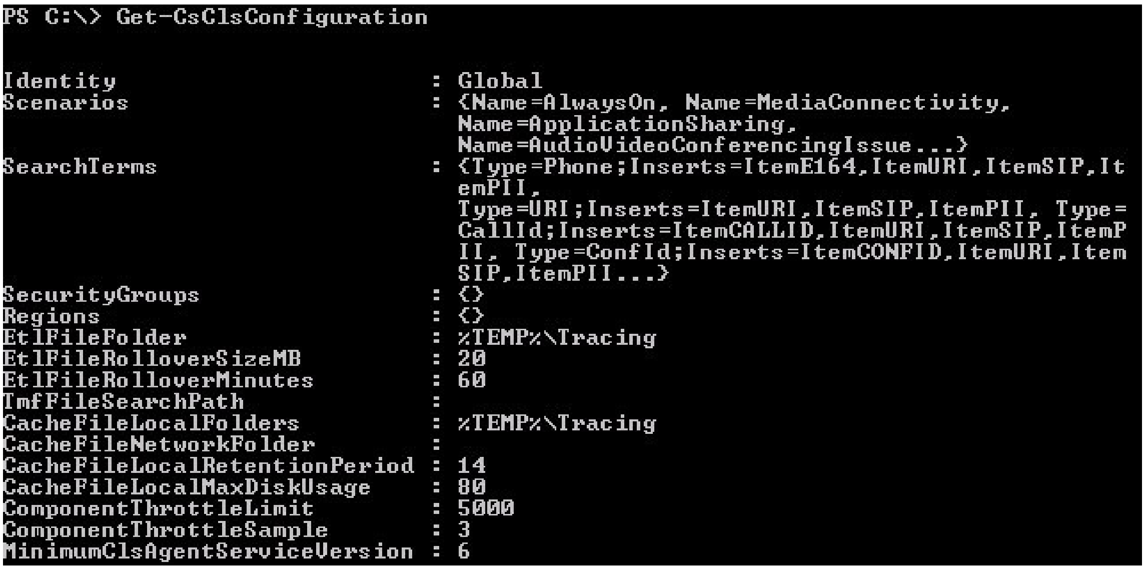
To retrieve the current Centralized Logging Service configuration

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Type the following at the command-line prompt:

```
Get-CsClsConfiguration
```

Use the **New-CsClsConfiguration** and **Set-CsClsConfiguration** cmdlets to create a new configuration or to update an existing configuration.

When you run **Get-ClsCsConfiguration**, it displays information similar to the following screen shot, where the deployment currently has the default Global configuration, but no site configurations defined:



```
PS C:\> Get-CsClsConfiguration


Identity                        : Global
Scenarios                       : {Name=AlwaysOn, Name=MediaConnectivity,
                                  Name=ApplicationSharing,
                                  Name=AudioVideoConferencingIssue...}
SearchTerms                     : {Type=Phone;Inserts=ItemE164,ItemURI,ItemSIP,It
                                  emPII,
                                  Type=URI;Inserts=ItemURI,ItemSIP,ItemPII, Type=
                                  CallId;Inserts=ItemCALLID,ItemURI,ItemSIP,ItemP
                                  II, Type=ConfId;Inserts=ItemCONFID,ItemURI,Item
                                  SIP,ItemPII...}
SecurityGroups                  : {}
Regions                         : {}
EtlFileFolder                   : %TEMP%\Tracing
EtlFileRolloverSizeMB           : 20
EtlFileRolloverMinutes          : 60
TmfFileSearchPath               :
CacheFileLocalFolders           : %TEMP%\Tracing
CacheFileNetworkFolder          :
CacheFileLocalRetentionPeriod   : 14
CacheFileLocalMaxDiskUsage      : 80
ComponentThrottleLimit          : 5000
ComponentThrottleSample         : 3
MinimumClsAgentServiceVersion   : 6
```

To retrieve the current Centralized Logging Service configuration from the computer local store

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Type the following at the command-line prompt:

```
Get-CsClsConfiguration -LocalStore
```

When you use the first example where **Get-CsClsConfiguration** does not specify any parameters, the command references the Central Management store for the data. If you specify the parameter –LocalStore, the command references the computer LocalStore instead of the Central Management store.

To retrieve a listing of scenarios currently defined

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Type the following at the command-line prompt:

```
Get-CsClsConfiguration -Identity <scope and name> | Select-Object -Exp
```

For example, to retrieve the scenarios that is defined at the global scope:

```
Get-CsClsConfiguration -Identity "global" | Select-Object -ExpandPrope
```

The cmdlet **Get-CsClsConfiguration** always displays the scenarios that are a part of a given scope's configuration. In most cases, all scenarios are not displayed, and are truncated. The command used here lists all of the scenarios and partial information about what providers, settings, and flags are used.

To update a global scope for the Centralized Logging Service by using Windows PowerShell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Type the following at the command-line prompt:

   ```
   Set-CsClsConfiguration -Identity <scope> -EtlFileRolloverSizeMB <size
   ```

   For example:

   ```
   Set-CsClsConfiguration -Identity "global" -EtlFileRolloverSizeMB 40
   ```

The command tells the CLSAgent on each computer and pool in the deployment to set the size of the rollover value on the tracing file to 40 megabytes. Computers and pools in all sites are affected by the command, and will set their configured trace log rollover value to 40 megabytes.

To update a site scope for the Centralized Logging Service by using Windows PowerShell

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Type the following at the command-line prompt:

   ```
   Set-CsClsConfiguration -Identity <scope/site name> -EtlFileRolloverSiz
   ```

   For example:

   ```
   Set-CsClsConfiguration -Identity "site/Redmond" -EtlFileRolloverSizeMB
   ```

   Note:
   As noted in the example, the default location of the log files is %TEMP%\Tracing. However, because it is actually CLSAgent that is writing the file and CSLAgent runs as Network Service, the %TEMP% variable expands to %WINDIR%\ServiceProfiles\NetworkService\AppData\Local.

The command tells the CLSAgent on each computer and pool in the site Redmond to set the size of the rollover value on the tracing file to 40 megabytes. Computers and pools in other sites will not be affected by the command, and will continue to use the currently configured trace log rollover value defined either by default (20 megabytes) or during the start of the logging session.

To create a new Centralized Logging Service configuration

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Type the following at the command-line prompt:

   ```
   New-CsClsConfiguration -Identity <scope and name> [CsClsConfiguration
   ```

   Note:
   New-CsClsConfiguration provides access to a large number of optional configuration settings. For details about the configuration options, see Get-

CsClsConfiguration and Understanding Centralized Logging Service Configuration Settings.

For example, to create a new configuration that defines a network folder for cache files, rollover time period for the log files and rollover size for the log files, you would type:

```
New-CsClsConfiguration -Identity "site:Redmond" -CacheFileNetworkFolde
```

You should carefully plan the creation of new configurations and how you define new properties for the Centralized Logging Service. You should be cautious about making changes and make sure you understand the impact on your ability to properly log problem scenarios. You should make changes to the configuration that will enhance your ability to manage logs to a size and a rollover period that will allow problem solving when it arises.

To remove an existing Centralized Logging Service configuration

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Type the following at the command-line prompt:

```
Remove-CsClsConfiguration -Identity <scope and name>
```

For example, to remove a Centralized Logging Service configuration that you created to increase the log file rollover time, increase the rollover log file size, and set the log file cache location to a network share as follows:

```
Remove-CsClsConfiguration -Identity "site:Redmond"
```

Note:
This is the new configuration that was created in the procedure "To create a new Centralized Logging Service configuration."

If you choose to remove a site-level configuration, the site will use the global settings.

Concepts

Overview of the Centralized Logging Service

Other Resources

Managing the Centralized Logging Service Configuration Settings
Set-CsClsConfiguration
Get-CsClsConfiguration
New-CsClsConfiguration
Remove-CsClsConfiguration

1.7.1.9.2.2 Configuring Providers for Centralized Logging Service

Configuring Providers for Centralized Logging Service

See Also

Lync Server Administrative Tools > Using the Centralized Logging Service > Managing the Centralized Logging Service Configuration Settings >

Topic Last Modified: *2012-12-24*

The concepts and configuration of *providers* in Centralized Logging Service is one of the most important to grasp. The *providers* map directly to Lync Server server role components in the Lync Server tracing model. The provider defines the components of a Lync Server 2013 that will be traced, the type of messages (for example, fatal, error, or warning) to collect, and the flags (for example, TF_Connection or TF_Diag). Providers are the traceable components in each Lync Server server role. By using providers, you define the level and type of tracing on components (for example, S4, SIPStack, IM and Presence). The defined provider is used in a scenario to group all of the providers for a given logical collection that address a specific problem condition.

To run the Centralized Logging Service functions using the Lync Server Management Shell, you must be a member of either the CsAdministrator or the CsServerAdministrator role-based access control (RBAC) security groups, or a custom RBAC role that contains either of these two groups. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Lync Server Management Shell or the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Lync Server 2013 cmdlet"}
```

For example:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Set-CsClsConfiguration"}
```

The remainder of this topic focuses on how to define providers, modify a provider and what a provider definition contains to optimize your troubleshooting. There are two ways to issue Centralized Logging Service commands. You can use the CLSController.exe that is located, by default, in the directory C:\Program Files\Common Files\Microsoft Lync Server 2013\CLSAgent. Or, you can use the Lync Server Management Shell to issue Windows PowerShell commands. The important distinction is that when you use CLSController.exe at the command line there is a finite selection of scenarios available in which the providers are already defined and are not changeable, but you can define the log level. By using Windows PowerShell, you can define new providers for use in your logging sessions, and have complete control over their creation, what they collect, and at what level they collect data.

> **Important:**
>
> As mentioned, providers are very powerful. However, scenarios are more powerful because they contain the embodiment of all information needed to set and execute tracing on the components that the providers represent. With scenarios being a collection of providers, this could be loosely compared to running a batch file containing hundreds of commands to collect a lot of information versus issuing hundreds of commands, one at a time, at the command line.
>
> Instead of requiring you to dig deeply into the details of providers, the Centralized Logging Service provides a number of scenarios that are already defined for you. The provided scenarios cover the vast majority of possible issues that you will encounter. In rare cases, you may need to create and define providers and assign them to scenarios. We strongly recommend that you become familiar with each of the scenarios provided before you investigate the need to create new providers and scenarios. While information about creating providers is found here to familiarize you with how the scenarios use the provider elements to collect trace information, details on the providers themselves are not provided at this time.

Introduced in Overview of the Centralized Logging Service, the key elements of defining a provider for use in a scenario are:

- **Providers** If you are familiar with OCSLogger, providers are the components that you choose to tell OCSLogger what the tracing engine should collect logs from. The providers are the same components, and in many cases have the same name as the components in OCSLogger. If you are not familiar with OCSLogger, providers are server-role specific components that the Centralized Logging Service can collect logs from. In the case of the Centralized Logging Service, the CLSAgent is the architectural part of the Centralized Logging Service that is doing the tracing of the components that you define in the providers configuration.
- **Logging levels** OCSLogger provided the option to choose a number of levels

  of detail for the data collected. This feature is an integral part of the Centralized Logging Service and scenarios, and is defined by the **Type** parameter. You can choose from the following:
  - **All** Collects trace messages of type fatal, error, warning, and info to the log for the defined provider.
  - **Fatal** Collects only the trace messages that indicate a failure for the defined provider.
  - **Error** Collects only the trace messages that indicate an error for the defined provider, plus fatal messages.
  - **Warning** Collects only the trace messages that indicate a warning for the defined provider, plus fatal and error messages.
  - **Info** Collects only the trace messages that indicate an informational message for the defined provider, plus fatal, error, and warning messages.
  - **Verbose** Collects all trace messages of type fatal, error, warning and info for the defined provider.
- **Flags** OCSLogger provided the option to choose flags for each provider that defined what type of information you could retrieve from the trace files. You can chose the following flags, based on the provider:
  - **TF_Connection** Provides connection-related log entries. These logs include information about connections established to and from a particular component. This may also include significant network-level information (that is, for components without the concept of a connection).
  - **TF_Security** Provides all events/log entries related to security. For example, for SipStack, these are security events such as domain validation failure, and client authentication/authorization failures.
  - **TF_Diag** Provides diagnostics events that you can use to diagnose or troubleshoot the component. For example, for SipStack, these are certificate failures, or DNS warnings/errors.
  - **TF_Protocol** Provides protocol messages such as SIP and CCCP messages.
  - **TF_Component** Enables logging on the components specified as part of the providers.
  - **All** Sets all available flags available for the provider.

To review information about existing Centralized Logging Service scenario providers

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. To review the configuration of existing providers, type the following:

   ```
   Get-CsClsScenario -Identity <scope and scenario name>
   ```

   For example, to review information about the global conferencing attendant, type:

   ```
   Get-CsClsScenario -Identity "global/CAA"
   ```

   The command displays a list of providers with the associated flags, settings, and components. If the information displayed is not enough or the list is too long for the default Windows PowerShell list format, you can display additional information by defining a different output method. To do this, type:

   ```
   Get-CsClsScenario -Identity "global/CAA" | Select-Object -ExpandProper
   ```

   The output of this command displays each provider displayed in a five line format with the provider name, type of logging, logging level, flags, GUID, and role, each one on a separate line.

To define a new Centralized Logging Service scenario provider

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

2. A scenario provider consists of a component to trace, flags to use, and a level of detail to collect. You do this by typing:

   ```
   $<variableName> = New-CsClsProvider -Name <provider component> -Type <
   ```

   For example, a trace provider definition that defines what to collect and to what level of detail from the Lyss provider looks like the following:

   ```
   $LyssProvider = New-CsClsProvider -Name "Lyss" -Type "WPP" -Level "Inf
   ```

The –Level collects fatal, error, warning, and information messages. The flags used are all of those defined for the Lyss provider, and include TF_Connection, TF_Diag and TF_Protocol.

After the variable $LyssProvider is defined, you can use it with the **New-CsClsScenario** cmdlet to collect traces from the Lyss provider. To complete the creation and assignment of the provider to a new scenario, type:

```
New-CsClsScenario -Identity "site:Redmond/RedmondLyssInfo" -Provider $LyssProvide
```

Where $LyssProvider is the variable containing the defined scenario created with **New-CsClsProvider**.

⊟To change an existing Centralized Logging Service scenario provider

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. To update or change the configuration of an existing provider, type:

   ```
   $LyssProvider = New-CsClsProvider -Name "Lyss" -Type "WPP" -Level "Deb
   ```

   You then update the scenario to assign the provider by typing the following:

   ```
   Set-CsClsScenario -Identity "site:Redmond/RedmondLyssInfo" -Provider $
   ```

The end result of the command is that the scenario site:Redmond/RedmondLyssInfo will have updated flags and level for the provider assigned to it. You can view the new scenario by using Get-CsClsScenario. For details, see Get-CsClsScenario.

> ⚠**Warning:**
>
> **New-ClsCsProvider** does not check to determine whether the flags are valid. Make sure that the spelling of the flags (for example, TF_DIAG or TF_CONNECTION) is spelled correctly. If the flags are not spelled correctly, the provider cannot return the expected log information.

If you want to add additional providers to this scenario, type the following:

```
Set-CsClsScenario -Identity "site:Redmond/RedmondLyssInfo" -Provider @{Add=$ABSPr
```

Where each provider defined with the Add directive has already been defined using the **New-CsClsProvider** process.

⊟To remove a scenario provider

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. The cmdlets provided allow you to update existing providers and create new providers. To remove a provider, you must use the Replace directive for the Provider parameter to **Set-CsClsScenario**. The only way to completely remove a provider is to replace it with a redefined provider of the same name and use the Update directive. For example, our provider LyssProvider is

defined with WPP as the log type, level set to Debug, and flags set are TF_CONNECTION and TF_DIAG. You need to change the flags to “All”. To change the provider, type the following:

```
$LyssProvider = New-CsClsProvider -Name "Lyss" -Type "WPP" -Level "Deb
```

```
Set-CsClsScenario -Identity "site:Redmond/RedmondLyssInfo" -Provider @
```

3. If you want to completely remove a scenario and the providers associated with it, type the following:

```
Remove-CsClsScenario -Identity <scope and name of scenario>
```

For example:

```
Remove-CsClsScenario -Identity "site:Redmond/RedmondLyssInfo"
```

> **Warning:**
> The cmdlet **Remove-CsClsScenario** does not prompt you for confirmation. The scenario is deleted, along with the providers that were assigned to it. You can recreate the scenario by re-running the commands used to create it initially. There is no procedure to recover removed scenarios or providers.

When you remove a scenario by using the **Remove-CsClsScenario** cmdlet, you completely remove the scenario from the scope. To use the scenarios that you created and the providers that were a part of the scenario, you create new providers and assign them to a new scenario.

Other Resources

Get-CsClsScenario
New-CsClsScenario
Remove-CsClsScenario
Set-CsClsScenario
New-CsClsProvider

1.7.1.9.2.3 Configuring Scenarios for the Centralized Logging Service

Configuring Scenarios for the Centralized Logging Service

Lync Server Administrative Tools > Using the Centralized Logging Service > Managing the Centralized Logging Service Configuration Settings >

Topic Last Modified: *2013-02-21*

Scenarios define the scope (that is, global, site, pool, or computer) and what providers to use in the Centralized Logging Service. By using scenarios, you enable or disable tracing on providers (for example, S4, SIPStack, IM, and Presence). By configuring a scenario, you can group all of the providers for a given logical collection that address a specific problem condition. If you find that a scenario needs to be modified to meet your troubleshooting and logging needs, the Lync Server 2013 Debug Tools provides you a Windows PowerShell module named *ClsController.psm1* that contains a function named *Edit-CsClsScenario*. The purpose of the module is to edit the properties of the named scenario. Examples of how this module works are provided in this topic. The Lync Server 2013 Debug Tools are downloaded from the following link: http://go.microsoft.com/fwlink/?LinkId=285257

> **Important:**
> For any given scope—site, global, pool or computer—you can run a maximum of two scenarios at any given time. To determine which scenarios are currently running, use Windows PowerShell and Get-CsClsScenario. By using Windows PowerShell and Set-CsClsScenario, you can dynamically change which scenarios are running. You can modify which scenarios are running during a logging session to adjust or refine the data you are

collecting and from which providers.

To run the Centralized Logging Service functions by using the Lync Server Management Shell, you must be a member of either the CsAdministrator or the CsServerAdministrator role-based access control (RBAC) security groups, or a custom RBAC role that contains either of these two groups. To return a list of all the RBAC roles this cmdlet has been assigned to, including any custom RBAC roles you have created yourself, run the following command from the Lync Server Management Shell or the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Lync Server 2013 cmdlet"}
```

For example:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Set-CsClsConfiguration"}
```

The remainder of this topic focuses on how to define a scenario, modify a scenario, retrieve what scenarios are running, remove a scenario, and specify what a scenario contains to optimize your troubleshooting. There are two ways to issue Centralized Logging Service commands. You can use the CLSController.exe that is located, by default, in the directory C:\Program Files\Common Files\Microsoft Lync Server 2013\CLSAgent. Or, you can use the Lync Server Management Shell to issue Windows PowerShell commands. The important distinction is that when you use CLSController.exe at the command line there is a finite selection of scenarios available. When you use Windows PowerShell, you can define new scenarios for use in your logging sessions.

As introduced in Overview of the Centralized Logging Service, the elements of a scenario are:

- **Providers** If you are familiar with OCSLogger, providers are the components that you choose to tell OCSLogger what the tracing engine should collect logs from. The providers are the same components, and in many cases have the same name as the components in OCSLogger. If you are not familiar with OCSLogger, providers are server role specific components that the Centralized Logging Service can collect logs from. For details about the configuration of providers, see Configuring Providers for Centralized Logging Service.
- **Identity** The parameter –Identity sets the scope and name of the scenario. For example, you could set a scope of "global" and identify the scenario with "LyssServiceScenario". When you combine the two, you define the Identity (for example, "global/LyssServiceScenario").

  Optionally, you can use the –Name and –Parent parameters. You define the Name parameter to uniquely identify the scenario. If you use Name, you must also use Parent to add the scenario to either global or site.

  Important:

  If you use the Name and Parent parameters, you cannot use the **–Identity** parameter.

⊟To create a new scenario with the New-CsClsScenario cmdlet

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. To create a new scenario for a logging session, use New-CsClsProvider and define the name of the scenario (that is, how it will be uniquely identified). Choose a type of logging format from WPP (that is, Windows software tracing preprocessor and is the default), EventLog (that is, Windows event log format), or IISLog (that is, ASCII format file based on the IIS log file format). Next, define Level (as the defined under Logging Levels in this topic), and Flags (as defined under Flags in this topic).

   For this example scenario, we use LyssProvider as the example provider variable.

To create a scenario using the options defined, type:

```
New-CsClsScenario -Identity <scope>/<unique scenario name> -Provider <
```

For example:

```
New-CsClsScenario -Identity "site:Redmond/LyssServiceScenario" -Provid
```

The alternate format using –Name and –Parent:

```
New-CsClsScenario -Name "LyssServiceScenario" -Parent "site:Redmond" -
```

To create a new scenario with multiple providers with the New-CsClsScenario cmdlet

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. You are limited to two scenarios per scope. However, you are not limited to a set number of providers. In this example, assume that we have created three providers, and you want to assign all three to the scenario you are defining. The provider variable names are LyssProvider, ABServerProvider, and SIPStackProvider. To define and assign multiple providers to a scenario, type the following at a Lync Server Management Shell or Windows PowerShell command prompt:

```
New-CsClsScenario -Identity "site:Redmond/CollectDataScenario" -Provid
```

> **Note:**
> As it is known in Windows PowerShell, the convention for creating a hash table of values using `@{<variable>=<value1>, <value2>, <value>...}` is known as *splatting*. For details about splatting in Windows PowerShell, see http://go.microsoft.com/fwlink/p/?LinkId=267760.

To modify an existing scenario with the Set-CsClsScenario cmdlet

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. You are limited to two scenarios per scope. You can change which scenarios are running at any time, even when a logging capture session is in process. If you redefine the running scenarios, the current logging session will stop using the scenario that was removed and then begin using the new scenario. However, the logging information that was captured with the removed scenario remains in the captured logs. To define a new scenario, do the following (that is, assuming the addition of an already defined provider named "S4Provider"):

```
Set-CsClsScenario -Identity <name of scope and scenario defined by New
```

For example:

```
Set-CsClsScenario -Identity "site:Redmond/LyssServiceScenario" -Provid
```

If you want to replace providers, define a single provider or a comma separated list of providers to replace the current set. If you only want to replace one of many providers, add the current providers with the new providers to create a new set of providers that contains both new providers and existing providers. To replace all providers with a new set, type the following:

```
Set-CsClsScenario -Identity <name of scope and scenario defined by New
```

For example, to replace the current set of $LyssProvider, $ABServerProvider, and $SIPStackProvider with $LyssServiceProvider:

```
Set-CsClsScenario -Identity "site:Redmond/LyssServiceScenario" -Provid
```

To replace just the $LyssProvider provider from the current set of

$LyssProvider, $ABServerProvider, and $SIPStackProvider with $LyssServiceProvider, type the following:

```
Set-CsClsScenario -Identity "site:Redmond/LyssServiceScenario" -Provid
```

To remove an existing scenario with the Remove-CsClsScenario cmdlet

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. If you want to remove a scenario that has been previously defined, type the following:

   ```
   Remove-CsClsScenario -Identity <name of scope and scenario>
   ```

   For example, to remove the defined scenario site:Redmond/LyssServiceScenario:

   ```
   Remove-CsClsScenario -Identity "site:Redmond/LyssServiceScenario"
   ```

The **Remove-CsClsScenario** cmdlet removes the specified scenario, but the traces that have been captured are still available in the logs for you to search on.

To load and unload the Edit-CsClsScenario cmdlet using the ClsController.psm1 module

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

   Important:

   The ClsController.psm1 module is provided as a separate Web download. The module is part of the Lync Server 2013 Debugging tools. By default, the debugging tools are installed in the directory C:\Program Files\Lync Server 2013\Debugging Tools.

2. From the Windows PowerShell, type:

   ```
   Import-Module "C:\Program Files\Lync Server 2013\Debugging Tools\ClsCo
   ```

   Tip:

   Successful loading of the module returns you to the Windows PowerShell command prompt. To confirm that the module is loaded and that Edit-CsClsScenario is available, type `Get-Help Edit-CsClsScenario`. You should see the basic synopsis of the syntax for EditCsClsScenario.

3. To unload the modules, type:

   ```
   Remove-Module ClsController
   ```

   Tip:

   Successful unloading of the module returns you to the Windows PowerShell command prompt. To confirm that the module is unloaded, type `Get-Help Edit-CsClsScenario`. Windows PowerShell will attempt to locate the help for the cmdlet and fail.

To remove an existing provider from a scenario with the Edit-ClsController module

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. To remove a provider from the AlwaysOn scenario, type:

   ```
   Edit-CsClsScenario -ScenarioName <string of the scenario to edit> -Pro
   ```

For Example:

```
Edit-CsClsScenario -ScenarioName AlwaysOn -ProviderName ChatServer -Re
```

The parameters ScenarioName and ProviderName are positional (that is, they must be defined in the expected position in the command line) parameters. The parameter name does not have to be explicitly defined if the scenario name is in position two and the provider is in position three, relative to the name of the cmdlet as position one. Using this information, the previous command would be typed as:

```
Edit-CsClsScenario AlwaysOn ChatServer -Remove
```

The positional placing of the parameter values applies only to –Scenario and –Provider. All other parameters must be explicitly defined.

⊟To add a provider to a scenario with the Edit-ClsController module

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. To add a provider to the AlwaysOn scenario, type:

```
Edit-CsClsScenario -ScenarioName <string of the scenario to edit> -Pro
```

For Example:

```
Edit-CsClsScenario -ScenarioName AlwaysOn -ProviderName ChatServer -Le
```

-Loglevel can be of the type Fatal, Error, Warning, Info, Verbose, Debug, or All. –Flags can be any of the flags that the provider supports, such as TF_COMPONENT, TF_DIAG. –Flags can also be of value ALL

The previous example can also be typed using the positional feature of the cmdlet. For example, to add the provider ChatServer to the AlwaysOn scenario, type:

```
Edit-CsClsScenario AlwaysOn ChatServer -Level Info -Flags ALL
```

1.7.1.9.3 Understanding Centralized Logging Service Configuration Settings

Understanding Centralized Logging Service Configuration Settings

See Also

Operations > Lync Server Administrative Tools > Using the Centralized Logging Service >

***Topic Last Modified:** 2013-02-21*

The Centralized Logging Service is configured to define what the logging service is intended to collect, how it collects, where it will collect from, and what the log settings are. You define these settings globally (that is, for the entire deployment) or for a site (that is, a named site in your deployment). Any logging that you define will use the settings that are appropriate for the identity that you use for commands to start, stop, flush, and search logs.

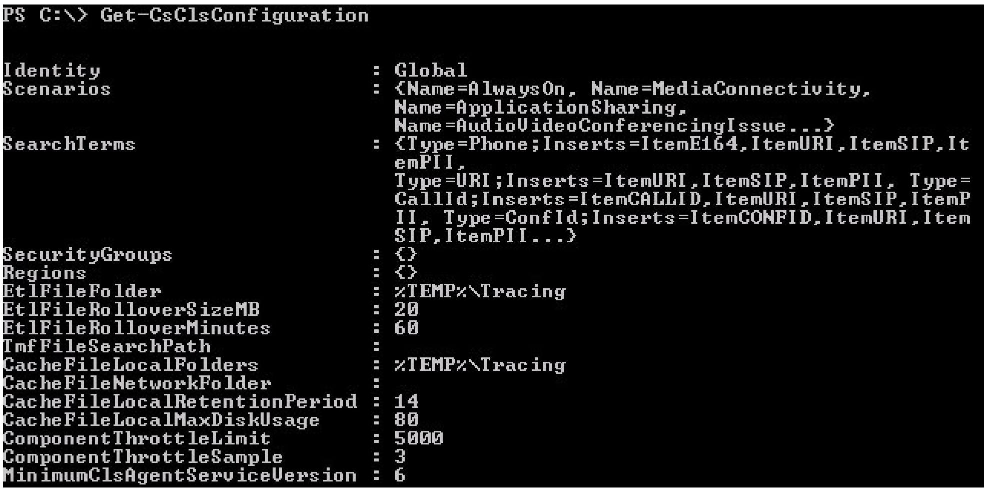
⊟To display the current Centralized Logging Service configuration

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Type the following at a command-line prompt:

```
Get-CsClsConfiguration
```

Tip:

You can narrow or expand the scope of the configuration settings that are returned by defining `-Identity` and a scope, such as "Site:Redmond" to return only the CsClsConfiguration for the site Redmond. If you want details about a given portion of the configuration, you can pipe the output into another Windows PowerShell cmdlet. For example, to get details about the scenarios defined in the configuration for site "Redmond", type: `Get-CsClsConfiguration -Identity "site:Redmond" | Select-Object -ExpandPropery Scenarios`



```
PS C:\> Get-CsClsConfiguration

Identity                         : Global
Scenarios                        : {Name=AlwaysOn, Name=MediaConnectivity,
                                   Name=ApplicationSharing,
                                   Name=AudioVideoConferencingIssue...}
SearchTerms                      : {Type=Phone;Inserts=ItemE164,ItemURI,ItemSIP,It
                                   emPII,
                                   Type=URI;Inserts=ItemURI,ItemSIP,ItemPII, Type=
                                   CallId;Inserts=ItemCALLID,ItemURI,ItemSIP,ItemP
                                   II, Type=ConfId;Inserts=ItemCONFID,ItemURI,Item
                                   SIP,ItemPII...}
SecurityGroups                   : {}
Regions                          : {}
EtlFileFolder                    : %TEMP%\Tracing
EtlFileRolloverSizeMB            : 20
EtlFileRolloverMinutes           : 60
TmfFileSearchPath                :
CacheFileLocalFolders            : %TEMP%\Tracing
CacheFileNetworkFolder           :
CacheFileLocalRetentionPeriod    : 14
CacheFileLocalMaxDiskUsage       : 80
ComponentThrottleLimit           : 5000
ComponentThrottleSample          : 3
MinimumClsAgentServiceVersion    : 6
```

The result from the cmdlet displays the current configuration of the Centralized Logging Service.

Configuration Setting	Description
Identity	Identifies the scope and name for this configuration. There is only one Global configuration, and one configuration per site.
Scenarios	Listing of all scenarios that are defined for this configuration.
SearchTerms	Defined search terms for the configuration. Office 365, not on-premises deployments.
SecurityGroups	Defined security groups that control who (that is, members of the security groups) can see computers based on the site they are located in. Site, in this context, is the site as defined in Topology Builder.
Regions	Defined regions are used to collect SecurityGroups into a region, for example EMEA.
EtlFileFolder	Defined path to the location where log files are written on computers. CLSAgent writes the log files and runs under the context of the Network Service. In this case, %TEMP% expands to %WINDIR%\ServiceProfiles\NetworkService\AppData\Local
EtlFileRolloverSizeMB	The parameter indicates the maximum

	size of the log file before a new event trace log (.etl) file is created. A new log file is created when the defined size is reached even if the maximum time set in EtlFileRolloverMinutes has not yet been reached.
EtlFileRolloverMinutes	Defined maximum amount of time, in minutes, that a log can elapse before a new .etl file is created. A new log file is created when the timer expires even if the maximum size set in EtlFileRolloverSizeMB has not yet been reached.
TmfFileSearchPath	Location to search for the trace message format files. The trace message format files are used to convert the binary files into a human readable format.
CacheFileLocalFolders	Defined path to the location where cache files are written on computers. CLSAgent writes the cache files and runs under the context of the Network Service. In this case, %TEMP% expands to %WINDIR%\ServiceProfiles\NetworkService\AppData\Local. By default, cache files and log files are written to the same directory.
CacheFileNetworkFolder	You can define a universal naming convention (UNC) path to receive the cache files during logging operations.
CacheFileLocalRetentionPeriod	Defined as the maximum time, in days, that cache files are retained.
CacheFileMaxDiskUsage	Defined as the percentage of disk space that can be used by the cache files.
ComponentThrottleLimit	Defined as the maximum number of traces per second that a component can produce before the automatic throttle limiter is triggered.
ComponentThrottleSample	Number of times in 60 seconds that the ComponentThrottleLimit can be exceeded.
MinimumClsAgentServiceVersion	The minimum version of the CLSAgent allowed to run. This element is intended for Office 365.

Concepts

Overview of the Centralized Logging Service

Other Resources

Set-CsClsConfiguration
Remove-CsClsConfiguration
New-CsClsConfiguration
Get-CsClsConfiguration

1.7.1.9.4 Using Start for the Centralized Logging Service to Capture Logs

Using Start for the Centralized Logging Service to Capture Logs

See Also

Operations > Lync Server Administrative Tools > Using the Centralized Logging Service >

Topic Last Modified: *2013-02-21*

To capture trace logs using the Centralized Logging Service, you issue a command to begin logging on one or more computers and pools. You also issue parameters that define which computers or pools, what scenarios to run (for example, AlwaysOn, another predefined scenario, or a scenario you have created), what Lync Server components (for example, S4, SipStack) to trace.

To capture the right information, you need to make sure you use the right scenario to collect information that is relevant to the problem. In the Centralized Logging Service, a scenario is the concept of turning logging on based on a collection of server components, logging levels, and flags, which is much more efficient and useful than having to define these elements on a per-server basis. You define and specify a scenario to run and the scenario is run consistently across all servers and pools in the scope of the infrastructure.

The default scenario is called **AlwaysOn**. The intended purpose for AlwaysOn is to run the scenario constantly, as the name of the scenario implies. The AlwaysOn scenario collects Info level information (note that Info logging level includes Fatal, Error, and Warning in addition to Info messages) for many of the most common server components. AlwaysOn collects information before, during, and after a problem occurs. This differs dramatically from the typical behavior of previous logging tools such as OCSLogger. You ran OCSLogger after the problem had already occurred, making your troubleshooting efforts more difficult because the data that you have is reactive, not proactive. If AlwaysOn does not contain the information that you are looking for in order to point to the problem component and indicate a course of action to fix it (which is not likely given the breadth and depth of providers in AlwaysOn), it will indicate a reasonable level of information to determine what else you need to do, such as creating a new scenario, gather other information, run a different search to collect more focused details, and so on.

The Centralized Logging Service provides two ways to issue commands. A number of topics have been focused squarely on using Windows PowerShell through the Lync Server Management Shell. The ability to use a number of complex configurations and commands favors Windows PowerShell for Centralized Logging Service use. Because Windows PowerShell through the Lync Server Management Shell is nearly ubiquitous for all functions in Lync Server, only the Windows PowerShell commands are discussed.

Note:

If you decide to use the limited command set available from the command line, you can get help with CLSController.exe by typing `ClsController.exe`. By default, **ClsController.exe** is installed in the directory C:\Program Files\Microsoft Lync Server 2013\ClsAgent.

To run Start-CsClsLogging with Windows PowerShell using basic commands

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Start a logging scenario with the Centralized Logging Service by typing the following:

```
Start-CsClsLogging -Scenario <name of scenario>
```

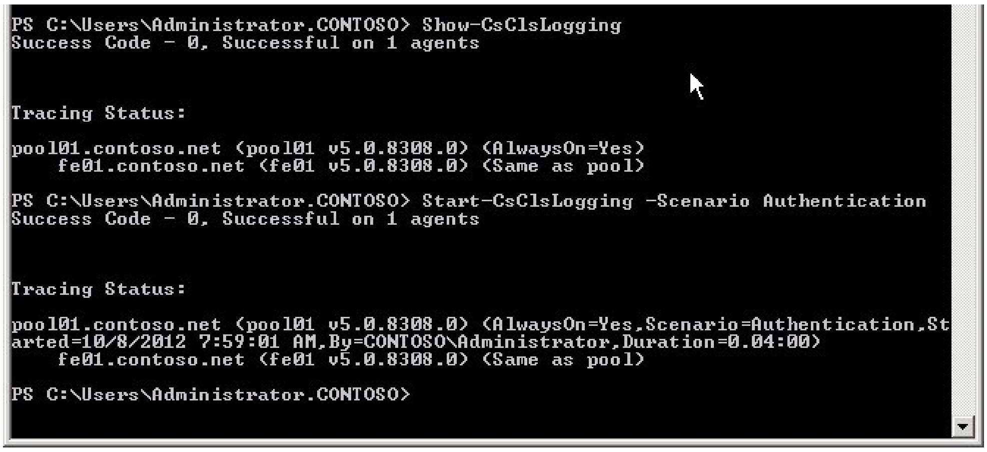
For example, to start the **AlwaysOn** scenario, type:

```
Start-CsClsLogging -Scenario AlwaysOn
```

Note:
The AlwaysOn scenario has no default duration. This scenario will run until you explicitly stop it with the **Stop-CsClsLogging** cmdlet. For details, see Stop-CsClsLogging. For all other scenarios, the default duration is 4 hours.

3. Press Enter to run the command.

Note:
It may take a short amount of time (30 to 60 seconds) for the commands to run and to receive the status back from the computers in your deployment.



```
PS C:\Users\Administrator.CONTOSO> Show-CsClsLogging
Success Code - 0, Successful on 1 agents


Tracing Status:

pool01.contoso.net (pool01 v5.0.8308.0) (AlwaysOn=Yes)
    fe01.contoso.net (fe01 v5.0.8308.0) (Same as pool)

PS C:\Users\Administrator.CONTOSO> Start-CsClsLogging -Scenario Authentication
Success Code - 0, Successful on 1 agents


Tracing Status:

pool01.contoso.net (pool01 v5.0.8308.0) (AlwaysOn=Yes,Scenario=Authentication,St
arted=10/8/2012 7:59:01 AM,By=CONTOSO\Administrator,Duration=0.04:00)
    fe01.contoso.net (fe01 v5.0.8308.0) (Same as pool)

PS C:\Users\Administrator.CONTOSO>
```

4. To start another scenario, use the **Start-CsClsLogging** cmdlet with the name of the additional scenario to run as follows (for example, the scenario **Authentication**):

```
Start-CsClsLogging -Scenario Authentication
```

Important:
You can have a total of two scenarios running on any given computer at any time. If the command is global in scope, all of the computers in your deployment will run the scenario or scenarios. To start a third scenario, you must stop logging on the computer, pool, site, or global scope that you want to run the new scenario on. If you have started a global scope, you can stop logging for one or both of the scenarios on one or more computers and pools. For details about managing which scenarios are running, see Using Stop for the Centralized Logging Service and Stop-CsClsLogging.

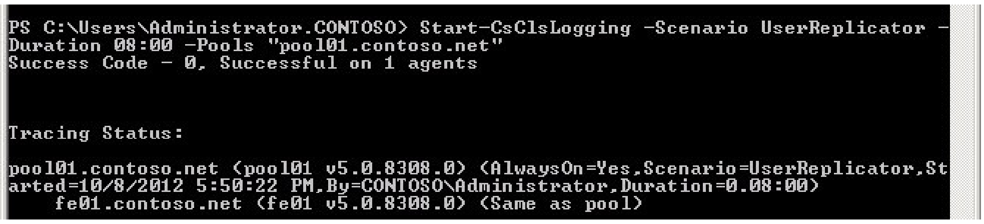
To run Start-CsClsLogging with Windows PowerShell using advanced commands

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Additional parameters are available to manage the logging commands. You can use -Duration to adjust the length of time for the scenario to run. You also can define -Computers, a list of computer fully qualified domain names (FQDNs) separated by a comma, or -Pools, a comma separated list of FQDNs for pools that you want to run logging on.

   You start a logging session for the *UserReplicator* scenario on the pool "pool01.contoso.net". You also define the duration of the logging session at 8 hours. To do this, type:

```
Start-CsClsLogging -Scenario UserReplicator -Duration 8:00 -Pools "poo
```

The successful execution of this scenario returns a result like the following:



```
PS C:\Users\Administrator.CONTOSO> Start-CsClsLogging -Scenario UserReplicator -
Duration 08:00 -Pools "pool01.contoso.net"
Success Code - 0, Successful on 1 agents


Tracing Status:

pool01.contoso.net (pool01 v5.0.8308.0) (AlwaysOn=Yes,Scenario=UserReplicator,St
arted=10/8/2012 5:50:22 PM,By=CONTOSO\Administrator,Duration=0.08:00)
    fe01.contoso.net (fe01 v5.0.8308.0) (Same as pool)
```

Note that in this example, the AlwaysOn scenario is running and the UserReplicator scenario is running.

Concepts

Overview of the Centralized Logging Service

1.7.1.9.5 Using Stop for the Centralized Logging Service

Using Stop for the Centralized Logging Service

See Also

Operations > Lync Server Administrative Tools > Using the Centralized Logging Service >

Topic Last Modified: *2012-11-01*

You can stop a currently running logging session with the Stop-CsClsLogging cmdlet. Generally, there aren't many situations in which you would need to stop a logging session. For example, you can search logs and change configurations without first needing to stop logging. If you have two scenarios running, for example AlwaysOn and UserReplicator, and you need to collect information related to Authentication, you will need to stop one of the other scenarios (at a global, site, pool or computer scope) before you can start running to Authentication scenario. For details, see Stop-CsClsLogging.

Note:

When determining what scenarios you can run on a given deployment, pool or computer, you need to remember that you are limited to running two scenarios **per computer**. If you are logging activity on a pool, you should treat a pool as a single entity. In most cases, it would not make sense to run different scenarios on each computer in a pool. It does make sense to look at the problem that you are collecting data about and think about what scenario makes the most sense on a given computer in the overall deployment. For example, if you consider the UserReplicator scenario, there would be very little value in running UserReplicator on an Edge Server or Edge pool.
After you understand the problem and the scope of the impact, you should make careful choices about what scenarios to run on which computers and pools. While the AlwaysOn scenario makes sense for a wide scope application because it collects information on a wide variety of providers, specific scenarios only have application value on specific computers or pools. Also, you should take caution when randomly starting up a logging session without first understanding the value of a given scenario. If you use the wrong scenario, or if you use a scenario that is appropriate for the task and you apply the scenario at the wrong scope (be it global, site, pool, or computer), you can get questionable data that is not very useful—as if you didn't run the scenario at all.

To control the Centralized Logging Service functions by using the Lync Server Management Shell, you must be a member of either the CsAdministrator or the CsServerAdministrator role-based access control (RBAC) security groups, or a custom RBAC role that contains either of these two groups. To return a list of all the RBAC roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Lync Server Management Shell or the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Lync Server 2013 cmdlet"}
```

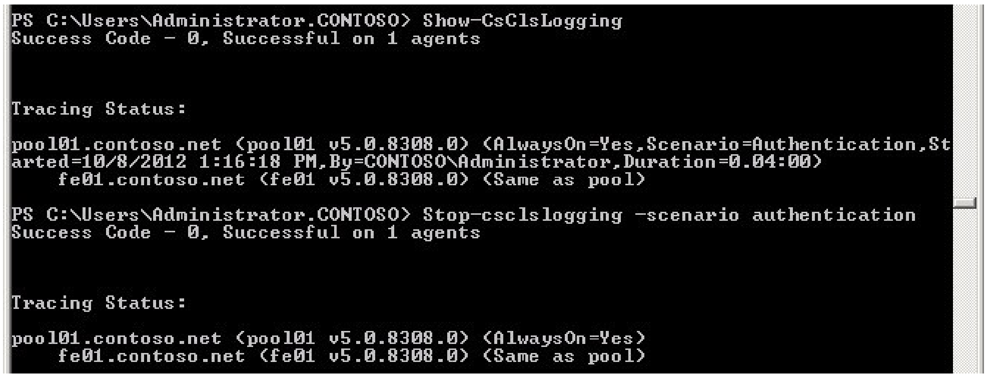
For example:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Set-CsClsConfiguration"}
```

To stop a currently running Centralized Logging Service session

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Query the Centralized Logging Service to find out what scenarios are currently running by typing the following:

   ```
   Show-CsClsLogging
   ```

   ```
   PS C:\Users\Administrator.CONTOSO> Show-CsClsLogging
   Success Code - 0, Successful on 1 agents


   Tracing Status:

   pool01.contoso.net (pool01 v5.0.8308.0) (AlwaysOn=Yes,Scenario=Authentication,St
   arted=10/8/2012 1:16:18 PM,By=CONTOSO\Administrator,Duration=0.04:00)
       fe01.contoso.net (fe01 v5.0.8308.0) (Same as pool)

   PS C:\Users\Administrator.CONTOSO> Stop-csclslogging -scenario authentication
   Success Code - 0, Successful on 1 agents


   Tracing Status:

   pool01.contoso.net (pool01 v5.0.8308.0) (AlwaysOn=Yes)
       fe01.contoso.net (fe01 v5.0.8308.0) (Same as pool)
   ```

   The result of Show-CsClsLogging is a summary of the scenarios that are running and what scope they are running in. For details, see Show-CsClsLogging.
3. To stop a currently running logging session with a specific scenario, type:

   ```
   Stop-CsClsLogging -Scenario <scenario name> -Computers <comma separate
   ```

   For example:

   ```
   Stop-CsClsLogging -Scenario UserReplicator -Pools pool01.contoso.net
   ```

   This command will stop logging with the UserReplicatior scenario on pool01.contoso.net.

   Note:

   Logs created during this logging session using the UserReplicator scenario are not deleted. The logging is still available for you to execute searches against using the Search-CsClsLogging command. For details, see Search-CsClsLogging.

Acting as the companion command to Start-CsClsLogging, the Stop-CsClsLogging cmdlet ends the logging session, defined by scenarios, and retains the logs created by the logging session. You can run two scenarios on a given computer at any time. The method of stopping one scenario to gather information using another scenario is a common task that you can perform during most workload troubleshooting.

Tasks

Using Start for the Centralized Logging Service to Capture Logs

Concepts

Overview of the Centralized Logging Service

Other Resources

Show-CsClsLogging
Start-CsClsLogging

Stop-CsClsLogging

1.7.1.9.6 Using Search on Capture Logs Created by the Centralized Logging Service

Using Search on Capture Logs Created by the Centralized Logging Service

Operations > Lync Server Administrative Tools > Using the Centralized Logging Service >

Topic Last Modified: *2013-02-21*

The search features in the Centralized Logging Service are useful and powerful for the following reasons:

- Your searches and the results are run on a single computer, a pool, a site, or a global scope, based on the criteria you define.
- Your searches can be initially broad and then narrowed down to more targeted criteria such as time, component, or computer. You search against the same logs and don't need to run a logging session again when the search criteria changes.
- The results of your search are gathered from all computers and pools in the scope, collected and aggregated into a single output file that represents all results of the search criteria (limited to the scenarios that have been running and the data captured by the scenarios). You use familiar tools such as **Snooper** or **Notepad** to read the output file and the trace messages from across your deployment.

The CLSAgent on each individual computer creates the logs based on the scenario or scenarios (two scenarios per computer can be running at any given time). The logs and their associated index and cache files are managed by the CLSAgent. When you define and execute a search, the search command instructs the CLSAgent on what information should be retrieved. The CLSAgent executes the query against the log files, cache files, and index files and returns the results of the search to the CLSContoller. The CLSController receives the search results from all computers and pools in the scope of the search. The CLSController then aggregates (combines) the logs and puts them into time delta order, oldest entry first, and proceeding in time to the most recent entry last.

After each search, the **Sync-CsClsLogging** cmdlet is run and it flushes the cache used by searches (not to be confused with the cache files maintained by the CLSAgent). Flushing the cache helps to ensure that there is a clean log and trace file capture buffer at the CLSController for the next search operation.

To get the most benefit from the Centralized Logging Service, you need a good understanding of how to configure search to return only trace messages from the computer and pool logs that are relevant to the issue that you are researching. issues

To run the Centralized Logging Service search functions by using the Lync Server Management Shell, you must be a member of either the CsAdministrator or the CsServerAdministrator role-based access control (RBAC) security groups, or a custom RBAC role that contains either of these two groups. To return a list of all the RBAC roles that this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Lync Server Management Shell or the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Lync Server 2013 cmdlet"}
```

For example:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Set-CsClsConfiguration"}
```

The remainder of this topic focuses on how to define a search to optimize your troubleshooting.

To run a basic search by using the Centralized Logging Service

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Make sure that you have the AlwaysOn scenario running in your deployment at the global scope and then type the following at a command prompt:

   ```
   Search-CsClsLogging -OutputFilePath <string value of path and file to
   ```

   > **Note:**
   > By default, Search-CsClsLogging sends the results of the search to the console. If you want to save the search results to a file, use –OutputFilePath *<string fully qualified file path>*. To define the –OutputFilePath parameter, supply a path and a filename as part of the parameter in a string format enclosed in quotation marks (for example; C:\LogFiles\SearchOutput.txt). In this example, you must ensure that the directory C:\LogFiles exists and that you have permissions to Read and Write (NTFS permission Modify) files in the folder. The output is appended to and is not overwritten. If you need separate files, define a distinct file name for each search.

   For example:

   ```
   Search-CsClsLogging -OutputFilePath "C:\LogFiles\logfile.txt"
   ```

To run a basic search on a pool or computer by using the Centralized Logging Service

1. To limit the search to a specific pool or computer, use the –Computers parameter with the computer defined by a computer fully qualified name, enclosed in quotation marks and separated by a comma as follows:

   ```
   Search-CsClsLogging -Computers <string value of computer names> -Outpu
   ```

   For example:

   ```
   Search-CsClsLogging -Computers "fe01.contoso.net" -OutputFilePath "C:\
   ```

2. To search more than one computer, type multiple computer names enclosed in quotation marks and separated by commas, such as the following:

   ```
   Search-CsClsLogging -Computers "fe01.contoso.net", "fe02.contoso.net",
   ```

3. If you need to search an entire pool instead of a single computer, change the –Computers parameter to –Pools, remove the computer name, and replace it with the pool or pools in quotation marks separated by commas.
   For example:

   ```
   Search-CsClsLogging -Pools "pool01.contoso.net" -OutputFilePath "C:\Lo
   ```

4. When using the search commands, pools can be any pool in your deployment, such as Front End pools, Edge pools, Persistent Chat Server pools, or others that are defined as a pool in your deployment.
   For example:

   ```
   Search-CsClsLogging -Pools "pool01.contoso.net", "pchatpool01.contoso.
   ```

To run a search by using time parameters

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. By default, the beginning time for a search's time-specific parameters is 30

minutes prior to the time you initiate the search. In other words, if you initiate your search at 4:00:00 PM, the search will search the logs for the computers and pools that you define from 3:30:00 PM until 4:00:00 PM. If you need to search 60 minutes or 3 hours prior to the current time, use the –StartTime parameter and set the date and time string to indicate the time you want the search to start.

For example, by using –StartTime and –EndTime to define a time and date range, you can define a search between 8 AM and 9 AM on 11/20/2012 on your pool. You can set the output path to write the results to a file named c:\logfile.txt as follows:

```
Search-CsClsLogging -Pools "pool01.contoso.net" -StartTime "11/20/2012
```

Note:

The time and date string that you specify can be "date time" or "time date. " The command will parse the string and use the appropriate values for date and time.

3. If you want to retrieve logs beginning at 11:00:00 AM on 11/20/2012, you define the –StartTime. The default time range for the search is 30 minutes unless you define a specific –EndTime. The resulting search will return logs from the defined computer or pools from 11:00:00 AM to 11:30:00 AM.

   For example:

   ```
   Search-CsClsLogging -Pools "pool01.contoso.net" -StartTime "11/20/2012
   ```

4. To conduct a search of logs within a specific period of time, define a –StartTime and an –EndTime. You need logs from 1 PM to 2:45 PM on the computer edge01.contoso.net.

   For example:

   ```
   Search-CsClsLogging -Computers "edge01.contoso.net" -StartTime "11/20/
   ```

To run an advanced search by using other criteria and matching options

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. To run a command to collect traces for specific components, type the following:

   ```
   Search-CsClsLogging -Components <components to search on> -OutputFileP
   ```

   For example:

   ```
   Search-CsClsLogging -Components "SIPStack","S4","UserServices" -Output
   ```

   The resulting search returns all log entries that have trace components for SIPStack, S4, and UserServices on all computers and pools in your deployment for the past 30 minutes.
3. To limit the search with the same components to just your Front End pool named pool01.contoso.net, type:

   ```
   Search-CsClsLogging -Components "SIPStack","S4","UserServices" -Output
   ```

4. The default search logic for commands with multiple parameters is to use the logical OR with each of the defined parameters. You can change this behavior by specifying the **–MatchAll** parameter. To do this, type the following:

   ```
   Search-CsClsLogging -CallId "d0af828e49fa4dcb99f5f80223a634bc" -Compon
   ```

5. If your scenarios are set to run constantly, such as AlwaysOn, or you have defined a long-running scenario logs may roll off of the local machine onto the file share. You define the file share by using the CacheFileNetworkFolder parameter by using New-CsClsConfiguration to create a new configuration or modifying an existing configuration with Set-CsClsConfiguration. If you do not want the search to include the file share in the collection of logs to search, use the SkipNetworkLogs parameter as follows:

```
Search-CsClsLogging -Components "SIPStack","S4","UserServices" -StartT
```

1.7.1.9.7 Reading Capture Logs From the Centralized Logging Service

Reading Capture Logs From the Centralized Logging Service

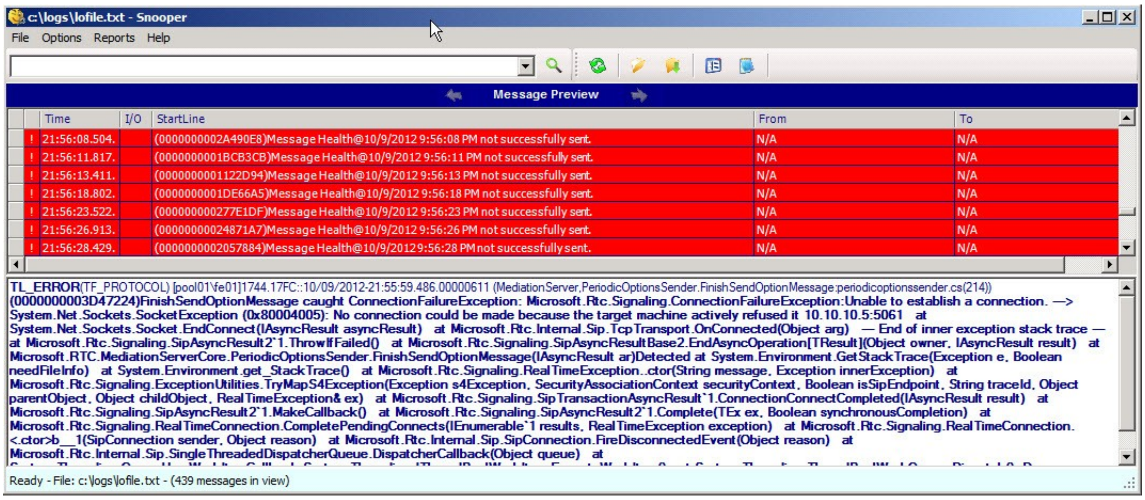
Operations > Lync Server Administrative Tools > Using the Centralized Logging Service >

Topic Last Modified: *2013-02-22*

You realize the real benefit of the Centralized Logging Service after you run the search and you have a file that you can use to track down a reported problem. There are a number of ways that you can read the file. The output file is in a standard text format and you can use Notepad.exe or any other programs that will allow you to open and read a text file. For larger files and more complex issues, you could use a tool like Snooper.exe that is designed to read and parse the logging output from the Centralized Logging Service. Snooper is included with the Lync Server 2013 Debug Tools that are available as a separate download. You can download the Lync Server 2013 Debug Tools here: http://go.microsoft.com/fwlink/?LinkId=285257. When you install the Lync Server 2013 Debug Tools, short cuts and menu items are not created. After you install the Lync Server 2013 Debug Tools, open Windows Explorer, a command-line window, or Lync Server Management Shell and go to the directory (default location) C:\Program Files\Microsoft Lync Server 2013\Debugging Tools. Double-click Snooper.exe or type Snooper.exe, and then press ENTER if you are using the command line or Lync Server Management Shell.

> ◆**Important:**
>
> The intent of this topic is not to detail and discuss troubleshooting techniques. Troubleshooting and the processes around it is a complex subject. For details about troubleshooting basics and troubleshooting specific workloads, see the Microsoft Lync Server 2010 Resource Kit book at http://go.microsoft.com/fwlink/p/?linkId=211003. The processes and procedures still apply to Lync Server 2013.

Lync Server 2013 introduces an updated version of Snooper that includes some new features. The following screen shot shows the version of Snooper from Office Communications Server 2007.

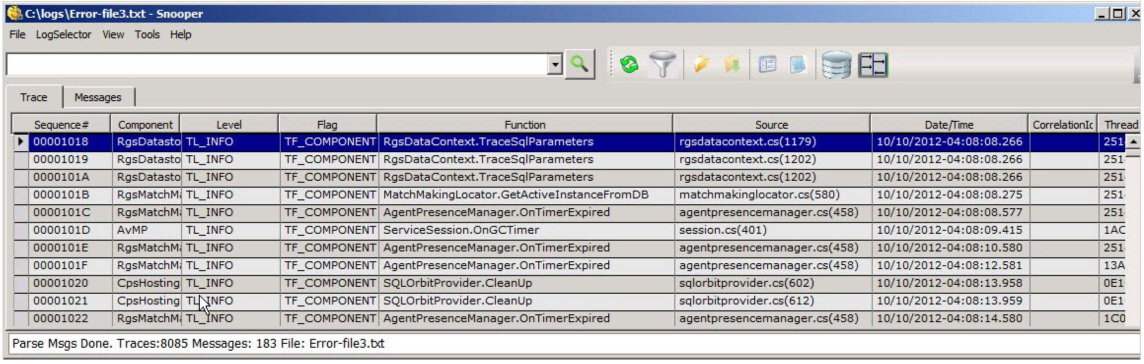


	Time	I/O	StartLine	From	To
!	21:56:08.504.		(0000000002A490E8)Message Health@10/9/2012 9:56:08 PM not successfully sent.	N/A	N/A
!	21:56:11.817.		(000000001BCB3CB)Message Health@10/9/2012 9:56:11 PM not successfully sent.	N/A	N/A
!	21:56:13.411.		(0000000001122D94)Message Health@10/9/2012 9:56:13 PM not successfully sent.	N/A	N/A
!	21:56:18.802.		(000000001DE66A5)Message Health@10/9/2012 9:56:18 PM not successfully sent.	N/A	N/A
!	21:56:23.522.		(000000000277E1DF)Message Health@10/9/2012 9:56:23 PM not successfully sent.	N/A	N/A
!	21:56:26.913.		(00000000024871A7)Message Health@10/9/2012 9:56:26 PM not successfully sent.	N/A	N/A
!	21:56:28.429.		(0000000002057884)Message Health@10/9/2012 9:56:28 PM not successfully sent.	N/A	N/A

```
TL_ERROR(TF_PROTOCOL) [pool01\fe01]1744.17FC::10/09/2012-21:55:59.486.00000611 (MediationServer,PeriodicOptionsSender.FinishSendOptionMessage:periodicoptionssender.cs(214))
(000000003D47224)FinishSendOptionMessage caught ConnectionFailureException: Microsoft.Rtc.Signaling.ConnectionFailureException:Unable to establish a connection. —>
System.Net.Sockets.SocketException (0x80004005): No connection could be made because the target machine actively refused it 10.10.10.5:5061   at
System.Net.Sockets.Socket.EndConnect(IAsyncResult asyncResult)   at Microsoft.Rtc.Internal.Sip.TcpTransport.OnConnected(Object arg)   — End of inner exception stack trace —
at Microsoft.Rtc.Signaling.SipAsyncResult2`1.ThrowIfFailed()   at Microsoft.Rtc.Signaling.SipAsyncResultBase2.EndAsyncOperation[TResult](Object owner, IAsyncResult result)   at
Microsoft.RTC.MediationServerCore.PeriodicOptionsSender.FinishSendOptionMessage(IAsyncResult ar)Detected at System.Environment.GetStackTrace(Exception e, Boolean
needFileInfo)   at System.Environment.get_StackTrace()   at Microsoft.Rtc.Signaling.RealTimeException..ctor(String message, Exception innerException)   at
Microsoft.Rtc.Signaling.ExceptionUtilities.TryMapS4Exception(Exception s4Exception, SecurityAssociationContext securityContext, Boolean isSipEndpoint, String traceId, Object
parentObject, Object childObject, RealTimeException& ex)   at Microsoft.Rtc.Signaling.SipTransactionAsyncResult`1.ConnectionConnectCompleted(IAsyncResult result)   at
Microsoft.Rtc.Signaling.SipAsyncResult2`1.MakeCallback()   at Microsoft.Rtc.Signaling.SipAsyncResult2`1.Complete(TEx ex, Boolean synchronousCompletion)   at
Microsoft.Rtc.Signaling.RealTimeConnection.CompletePendingConnects(IEnumerable`1 results, RealTimeException exception)   at Microsoft.Rtc.Signaling.RealTimeConnection.
<.ctor>b__1(SipConnection sender, Object reason)   at Microsoft.Rtc.Internal.Sip.SipConnection.FireDisconnectedEvent(Object reason)   at
Microsoft.Rtc.Internal.Sip.SingleThreadedDispatcherQueue.DispatcherCallback(Object queue)   at
```

Ready - File: c:\logs\lofile.txt - (439 messages in view)

The following screen shot shows the new version of Snooper included in the Lync Server 2013 Debug Tools.

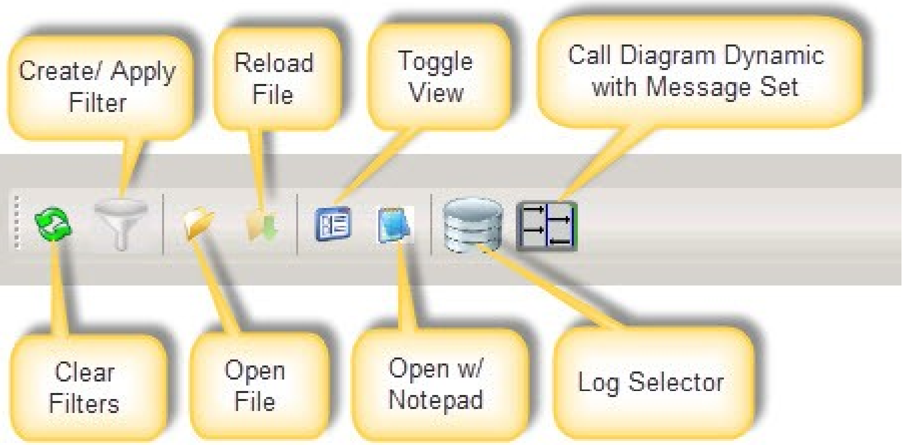


C:\logs\Error-file3.txt - Snooper
File LogSelector View Tools Help
Trace
Messages

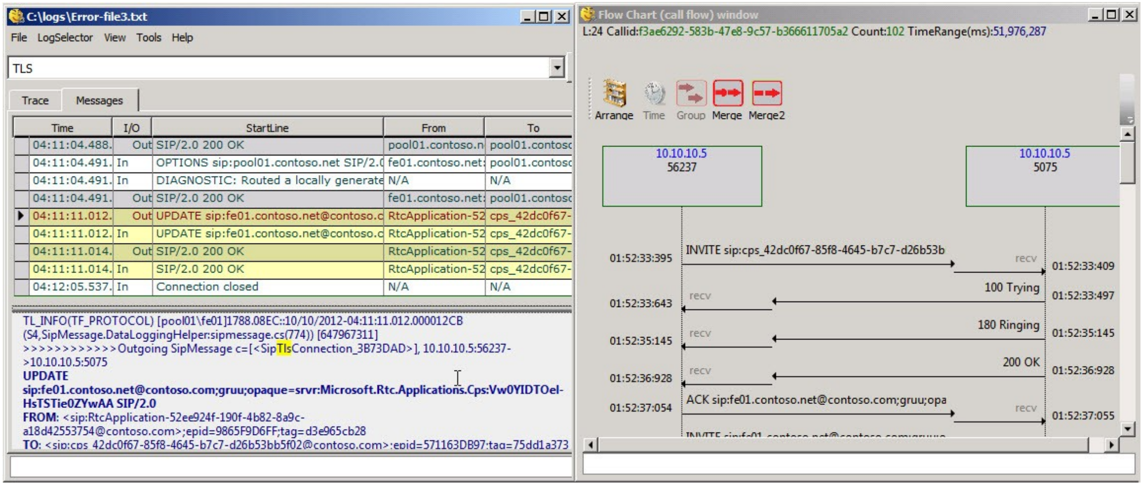
Sequence#	Component	Level	Flag	Function	Source	Date/Time	CorrelationIc	Thread
00001018	RgsDatasto	TL_INFO	TF_COMPONENT	RgsDataContext.TraceSqlParameters	rgsdatacontext.cs(1179)	10/10/2012-04:08:08.266		251
00001019	RgsDatasto	TL_INFO	TF_COMPONENT	RgsDataContext.TraceSqlParameters	rgsdatacontext.cs(1202)	10/10/2012-04:08:08.266		251
0000101A	RgsDatasto	TL_INFO	TF_COMPONENT	RgsDataContext.TraceSqlParameters	rgsdatacontext.cs(1202)	10/10/2012-04:08:08.266		251
0000101B	RgsMatchM	TL_INFO	TF_COMPONENT	MatchMakingLocator.GetActiveInstanceFromDB	matchmakinglocator.cs(580)	10/10/2012-04:08:08.275		251
0000101C	RgsMatchM	TL_INFO	TF_COMPONENT	AgentPresenceManager.OnTimerExpired	agentpresencemanager.cs(458)	10/10/2012-04:08:08.577		251
0000101D	AvMP	TL_INFO	TF_COMPONENT	ServiceSession.OnGCTimer	session.cs(401)	10/10/2012-04:08:09.415		1AC
0000101E	RgsMatchM	TL_INFO	TF_COMPONENT	AgentPresenceManager.OnTimerExpired	agentpresencemanager.cs(458)	10/10/2012-04:08:10.580		251
0000101F	RgsMatchM	TL_INFO	TF_COMPONENT	AgentPresenceManager.OnTimerExpired	agentpresencemanager.cs(458)	10/10/2012-04:08:12.581		13A
00001020	CpsHosting	TL_INFO	TF_COMPONENT	SQLOrbitProvider.CleanUp	sqlorbitprovider.cs(602)	10/10/2012-04:08:13.958		0E1
00001021	CpsHosting	TL_INFO	TF_COMPONENT	SQLOrbitProvider.CleanUp	sqlorbitprovider.cs(612)	10/10/2012-04:08:13.959		0E1
00001022	RgsMatchM	TL_INFO	TF_COMPONENT	AgentPresenceManager.OnTimerExpired	agentpresencemanager.cs(458)	10/10/2012-04:08:14.580		1C0

Parse Msgs Done. Traces:8085 Messages: 183 File: Error-file3.txt

The following screen shot shows the toolbar with frequently used functions.



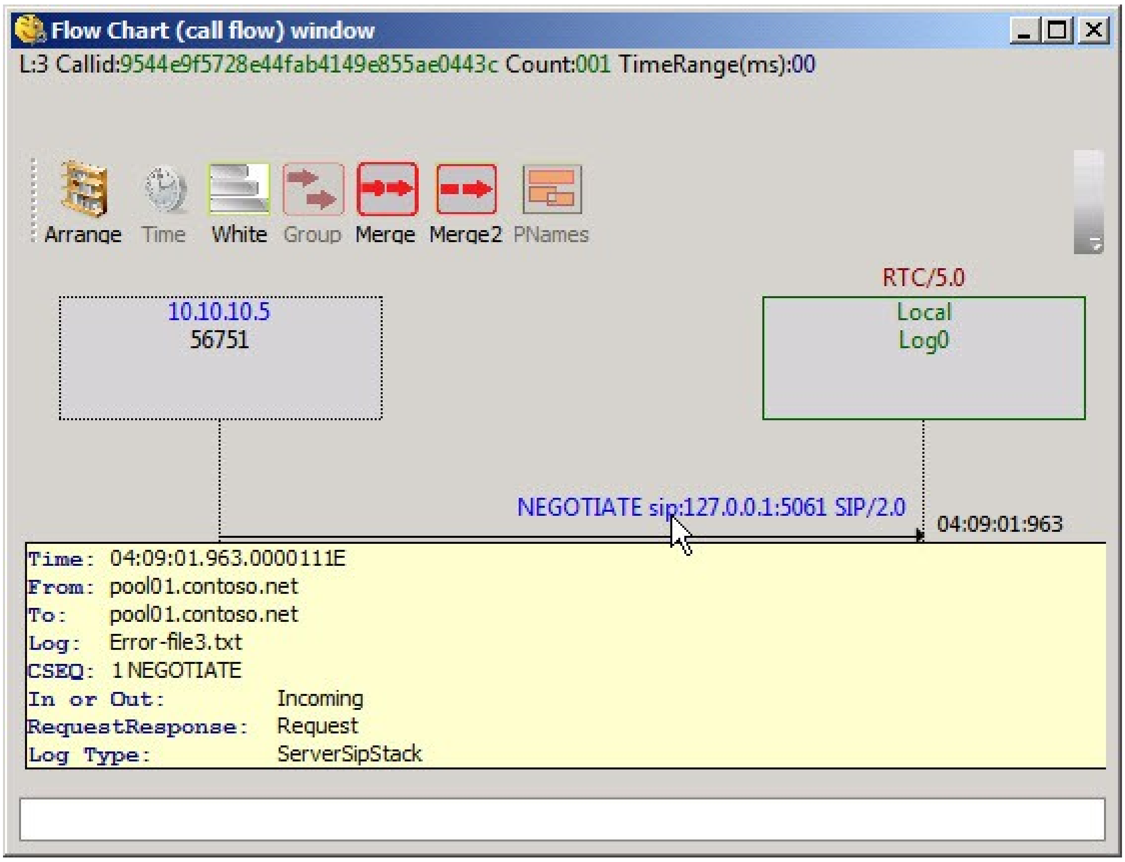
And, the newest feature that adds value is the Flow Chart (call flow) diagram view. You select a message flow in the **Message** tab and click the **Call Flow** button. As you proceed through the messages, the call flow diagram updates with new data.



Time	I/O	StartLine	From	To
04:11:04.488.	Out	SIP/2.0 200 OK	pool01.contoso.n	pool01.contoso
04:11:04.491.	In	OPTIONS sip:pool01.contoso.net SIP/2.0	fe01.contoso.net:	pool01.contoso
04:11:04.491.	In	DIAGNOSTIC: Routed a locally generate	N/A	N/A
04:11:04.491.	Out	SIP/2.0 200 OK	fe01.contoso.net:	pool01.contoso
04:11:11.012.	Out	UPDATE sip:fe01.contoso.net@contoso.c	RtcApplication-52	cps_42dc0f67-
04:11:11.012.	In	UPDATE sip:fe01.contoso.net@contoso.c	RtcApplication-52	cps_42dc0f67-
04:11:11.014.	Out	SIP/2.0 200 OK	RtcApplication-52	cps_42dc0f67-
04:11:11.014.	In	SIP/2.0 200 OK	RtcApplication-52	cps_42dc0f67-
04:12:05.537.	In	Connection closed	N/A	N/A

```
TL_INFO(TF_PROTOCOL) [pool01\fe01]1788.08EC::10/10/2012-04:11:11.012.000012CB
(S4,SipMessage.DataLoggingHelper:sipmessage.cs(774)) [647967311]
>>>>>>>>>>>>Outgoing SipMessage c=[<SipTlsConnection_3B73DAD>], 10.10.10.5:56237-
>10.10.10.5:5075
UPDATE
sip:fe01.contoso.net@contoso.com;gruu;opaque=srvr:Microsoft.Rtc.Applications.Cps:Vw0YIDTOel-
HsTSTie0ZYwAA SIP/2.0
FROM: <sip:RtcApplication-52ee924f-190f-4b82-8a9c-
a18d42553754@contoso.com>;epid=9865F9D6FF;tag=d3e965cb28
TO: <sip:cps_42dc0f67-85f8-4645-b7c7-d26b53bb5f02@contoso.com>;epid=571163DB97;tag=75dd1a373
```

You can hover over the diagram view and get details about the messages and content of the flows and messages as well as the server elements. Click on any call flow arrow to go to the message in the Messages view.



L:3 Callid:9544e9f5728e44fab4149e855ae0443c Count:001 TimeRange(ms):00

```
Time:  04:09:01.963.0000111E
From:  pool01.contoso.net
To:    pool01.contoso.net
Log:   Error-file3.txt
CSEQ:  1 NEGOTIATE
In or Out:          Incoming
RequestResponse:    Request
Log Type:           ServerSipStack
```

⊟To open a log file in Snooper

1. To use Snooper and open log files, you need read access to the log files. To use Snooper and access the log files you must be a member of the CsAdministrator or the CsServerAdministrator role-based access control (RBAC) security groups, or a custom RBAC role that contains either of these two groups.
2. After the installation of the Lync Server Debugging Tools (LyncDebugTools.msi), change directory to the location of Snooper.exe using Windows Explorer or from the command line. By default, the debugging tools are located in C:\Program Files\Microsoft Lync Server 2013\Debugging Tools. Double-click or run Snooper.exe.
3. After Snooper is open, right-click **File**, click **OpenFile**, find your log files, select a file in the **Open** dialog box, and then click **Open**.
4. The log file's **Trace** messages are displayed on the **Trace** tab. Click the **Messages** tab to view the message contents of the collected traces.

⊟To display a call flow diagram

1. To use Snooper and open log files, you need read access to the log files. To use Snooper and access the log files, you need to be a member of the CsAdministrator or the CsServerAdministrator role-based access control (RBAC) security groups, or a custom RBAC role that contains either of these two groups.
2. Open a log file and click the **Messages** tab, select a conversation in the messages view or select a trace component on the **Trace** tab.
3. Click **Call Flow**.

Note:

If you click on a message or trace that is not part of a call flow, the diagram will not appear and a status message appears at the bottom of Snooper stating "This message is not eligible for callfow". Choose another message or trace and the call flow will appear if the message or trace is part of a call flow.

4. Move through the Messages or the Trace lines and note whether the call flow diagram updates or changes to display a new diagram.
5. Hover over elements to get information about call messages, endpoints, and other components.

1.7.2 Managing Users in Lync Server 2013

Managing Users in Lync Server 2013

See Also

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-10-17*

You can use the Lync Server 2013 Control Panel and Lync Server 2013 Management Shell to manage user accounts in Lync Server 2013. The procedures in this section guide you through how to view account information and configure setting for user accounts.

- User Accounts Enabled for Lync Server 2013

⊟See Also

Concepts

Operations

1.7.2.1 User Accounts Enabled for Lync Server 2013

User Accounts Enabled for Lync Server 2013

See Also

Microsoft Lync Server 2013 > Operations > Managing Users in Lync Server 2013 >

Topic Last Modified: *2012-11-01*

Topics in this section provide step-by-step procedures for configuring user settings that you can perform using the Lync Server 2013 Control Panel.

Important:

You cannot use Lync Server Control Panel to manage users who are members of the Active Directory Domain Admins group. For Domain Admins users, you can use Lync Server Control Panel only to perform read-only search operations. To perform write operations on Domain Admins users (for example, enable or disable for Lync Server Control Panel, change pool or policy assignments, telephony settings, SIP address), you must use Windows PowerShell cmdlets while logged on as a Domain Admins user. For details about using Windows PowerShell cmdlets to manage users, see Lync Server Management Shell.

When you perform any Lync Server 2013 administrative task that involves searching for a user or filtering user search results, there are some user properties that exist as attributes in Active Directory Domain Services (AD DS) but are not replicated to the global catalog until Microsoft Exchange Server is deployed. Microsoft Exchange, not Lync Server, marks the following attributes for replication to the global catalog when it is installed:

User Information	Address and Phone	Organization

Initials	Street address Country/region Pager Fax Mobile	Title Company Department Office

- Viewing Information about User Accounts Enabled for Lync Server 2013
- Enabling and Disabling Users for Lync Server 2013
- Managing Enterprise Voice for Users
- Modifying User Account Properties
- Manage External Access Policy for Your Organization
- Assigning Per-User Policies

See Also

Concepts

User Management Cmdlets

Other Resources

Managing Users in Lync Server 2013

1.7.2.1.1 Viewing Information about User Accounts Enabled for Lync Server 2013

Viewing Information about User Accounts Enabled for Lync Server 2013

Operations > Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 >

Topic Last Modified: *2012-10-18*

Follow the procedures in this section to view settings and policy information for Lync Server 2013 user accounts.

- Search for Lync Server Users

Related Sections

Assigning Per-User Policies

1.7.2.1.1.1 Search for Lync Server Users

Search for Lync Server Users

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Viewing Information about User Accounts Enabled for Lync Server 2013 >

Topic Last Modified: *2012-11-01*

You can use the results of a search query to configure users for Lync Server 2013. You can search for users by display name, first name, last name, Security Accounts Manager

(SAM) account name, SIP address, or line Uniform Resource Identifier (URI).

You can search for users by using the Lync Server Control Panel or the Active Directory Users and Computers snap-in. The following procedure describes how to use Lync Server Control Panel to search for users.

Note:

In an environment with a central forest topology, search results might not be accurate when you search for a user by the user's email address. Instead, you can search for users by specifying a SIP address prefix, for example, sip:name, add a search filter and select a SIP address that contains a partial email address, or use the **Get-CSUser** cmdlet.

To search for one or more users

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, SAM account name, SIP address, or line URI of the user account that you want to search for, and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - 5.a. Click the expand arrow button in the upper-right corner of the screen above **Search results**, and then click **Add Filter**.
   - 5.b. Enter the user property by typing it or clicking the arrow in the drop-down list to select a user property.
   - 5.c. In the **Equal to** list, click **Equal to** or **Not equal to**.
   - 5.d. In the text box, type the search criteria you want to use to filter search results, and then click **Find**.
6. The search results appear under **Search Results**. You can select any or all of the users in the list and perform configuration tasks on the users you select.

Other Resources

Viewing Information about User Accounts Enabled for Lync Server 2013
Enabling and Disabling Users for Lync Server 2013

1.7.2.1.2 Enabling and Disabling Users for Lync Server 2013

Enabling and Disabling Users for Lync Server 2013

See Also

Operations > Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 >

Topic Last Modified: *2012-11-01*

You can enable, temporarily disable, or remove Active Directory users from Lync Server 2013.

- Add and Enable User Account for Lync Server
- Disable or Re-Enable User Account for Lync Server
- Remove a User Account from Lync Server

See Also

Other Resources

Managing Users in Lync Server 2013

Enable-CsUser
Disable-CsUser

1.7.2.1.2.1 Add and Enable User Account for Lync Server

Add and Enable User Account for Lync Server

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Enabling and Disabling Users for Lync Server 2013 >

Topic Last Modified: *2012-11-02*

After enabling a user account in Active Directory Users and Computers, you can use Lync Server Control Panel to create and enable new Lync Server 2013 user accounts by adding an Active Directory user to Lync Server.

⊟To add and enable a new Lync Server user

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Click **Enable users**.
5. On the **New Lync Server User** dialog, click **Add**.
6. In the **Search users** box, type all or the first portion of the name, display name, first name, last name, Security Accounts Manager (SAM) account name, email address, User Principal Name (UPN), or phone number of the Active Directory user account that you want, and then click **Find**.
7. In the table, select the account you want to add to Lync Server, and then click **OK**.
8. Assign the user to a pool, specify any additional details, and assign the policies to the user you want, and then click **Enable**.

Tasks

Disable or Re-Enable User Account for Lync Server
Remove a User Account from Lync Server

Other Resources

Enabling and Disabling Users for Lync Server 2013

1.7.2.1.2.2 Disable or Re-Enable User Account for Lync Server

Disable or Re-Enable User Account for Lync Server

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Enabling and Disabling Users for Lync Server 2013 >

Topic Last Modified: *2013-02-22*

You can use the following procedure to disable a previously enabled user account in Lync Server 2013 without losing the Lync Server settings that you configured for the user account. Because you do not lose the Lync Server user account settings, you can re-enable a previously enabled user account again without having to reconfigure the user account.

⊟To disable or re-enable a previously enabled user account for Lync Server

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to disable or re-enable, and then click **Find**.
5. In the table, click the user account that you want to disable or re-enable.
6. On the **Action** menu, do one of the following:
   - To temporarily disable the user account for Lync Server 2013, click **Temporarily disable for Lync Server**.
   - To enable the user account for Lync Server 2013, click **Re-enable for Lync Server**.

Using Windows PowerShell to Disable or Re-enable User Accounts

User accounts can be temporarily disabled, and then later re-enabled, by using the **Set-CsUser** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To disable a user account

- To temporarily disable a user account, set the value of the Enabled property to False ($False). For example:

```
Set-CsUser -Identity "Ken Myer" -Enabled $False
```

⊟To re-enable a user account

- To re-enable a disabled user account, set the value of the Enabled property to True ($True). For example:

```
Set-CsUser -Identity "Ken Myer" -Enabled $True
```

For more information, see the help topic for the Set-CsUser cmdlet.

⊟See Also

Tasks

Add and Enable User Account for Lync Server

Other Resources

Enabling and Disabling Users for Lync Server 2013

1.7.2.1.2.3 Remove a User Account from Lync Server

Remove a User Account from Lync Server

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Enabling

and Disabling Users for Lync Server 2013 >

Topic Last Modified: *2013-02-22*

You can use the following procedure to remove a previously added user account in Lync Server 2013.

Note:

Removing a user will cause you to lose any settings you configured for the user account. If you would like to temporarily disable a user account instead, see the topic Disable or Re-Enable User Account for Lync Server.

To remove a user account by using Lync Server Management Shell

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to disable or re-enable, and then click **Find**.
5. In the table, click the user account that you want to remove.
6. On the **Action** menu, select **Remove from Lync Server**, and a dialog box appears.
7. From the dialog box, select **OK** to remove the user.

Removing User Accounts by Using Windows PowerShell Cmdlets

You can remove user accounts by using the Disable-CsUser cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a user account

- To remove a user account, use the Disable-CsUser cmdlet. For example:

  ```
  Disable-CsUser -Identity "Ken Myer"
  ```

  After this command has run there is no way to re-enable the account and its previous settings. Instead, you will need to use the Enable-CsUser cmdlet to create a brand-new account for Ken Myer.

For more information, see the help topic for the Disable-CsUser cmdlet.

See Also

Tasks

Disable or Re-Enable User Account for Lync Server

Other Resources

Enabling and Disabling Users for Lync Server 2013

1.7.2.1.3 Managing Enterprise Voice for Users

Managing Enterprise Voice for Users

Operations > Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 >

Topic Last Modified: *2012-10-11*

You can enable Enterprise Voice on a per-user basis. Use the procedures in this section to manage Enterprise Voice using Lync Server 2013 Control Panel and Lync Server 2013 Management Shell.

- Enable Users for Enterprise Voice
- Disable a User for Enterprise Voice

⊟Related Sections

Managing Voice Routing

1.7.2.1.3.1 Enable Users for Enterprise Voice

Enable Users for Enterprise Voice

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-11-01*

After you install files for one or more Mediation Servers, configure outbound call routing, and optionally deploy one or more advanced Enterprise Voice features, you can use the following procedures to enable a user to make calls by using Enterprise Voice:

Note:
Of the following procedures, only the first can be performed by using Lync Server Control Panel. For the remaining procedures, you can use only Lync Server Management Shell.

- Enable the user account for Enterprise Voice.
- (Optional) Assign the user account a user-specific voice policy.
- (Optional) Assign the user account a user-specific dial plan.

⊟To enable a user account for Enterprise Voice

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to enable, and then click **Find**.
5. In the table, click the user account that you want to enable for Enterprise Voice.
6. On the **Edit** menu, click **Show details**.
7. On the **Edit Lync Server User** page, under **Telephony**, click **Enterprise Voice**.

8. Click **Line URI**, and then type a unique, normalized phone number (for example, tel:+14255550200).
9. Click **Commit**.

To finish enabling a user for Enterprise Voice, be sure that the user is assigned a voice policy and a dial plan, whether global (assigned by default) or user-specific.

By default, all users are assigned a global voice policy and dial plan. If a voice policy or dial plan exists at the site level for the site on which the user account is homed, those site policies will automatically apply to the user. To apply a per-user voice policy or dial plan to a user, you must run the **Grant-CsVoicePolicy** and **Grant-CsDialPlan** cmdlets. For details, see the Lync Server Management Shell documentation.

Voice Policy Assignment

Global and site-level voice policies are automatically assigned to all user accounts that are enabled for Enterprise Voice. You can also create voice policies that apply to specific users or groups. These per-user policies must be explicitly assigned to the users or groups. If you want to use the global or site voice policy for all users who are enabled for Enterprise Voice, you can skip this section and continue to Dial Plan Assignment section later in this topic.

To assign a user-specific voice policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. To assign an existing user voice policy to a user, run the following at the command prompt:

   ```
   Grant-CsVoicePolicy -Identity <UserIdParameter> -PolicyName <String>
   ```

   For example:

   ```
   Grant-CsVoicePolicy -Identity "Bob Kelly" -PolicyName VoicePolicyJapar
   ```

   In this example, the user with the display name Bob Kelly is assigned the voice policy with the name **VoicePolicyJapan**.

For details about assigning a user-specific voice policy or about running the **Grant-CsVoicePolicy** cmdlet, see the Lync Server Management Shell documentation.

Dial Plan Assignment

To complete user account configuration for either users of Enterprise Voice or users of dial-in conferencing, the user must be assigned a dial plan. User accounts will automatically use the global dial plan or, if one exists, the site-level dial plan, when you do not explicitly assign an existing per-user dial plan. If you want to use the global or site dial plan for all users who are enabled for Enterprise Voice, you can skip this section.

To assign a dial plan

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. To assign a user-specific dial plan, run the following at the command prompt:

   ```
   Grant-CsDialPlan -Identity <UserIdParameter> -PolicyName <String>
   ```

For example:

```
Grant-CsDialPlan -Identity "Bob Kelly" -PolicyName DialPlanJapan
```

In this example, the user with the display name Bob Kelly is assigned the user dial plan with the name **DialPlanJapan**.

For details about assigning a user dial plan or about running the **Grant-CsDialPlan** cmdlet, see the Lync Server Management Shell documentation.

See Also

Tasks

Disable a User for Enterprise Voice

1.7.2.1.3.2 Disable a User for Enterprise Voice

Disable a User for Enterprise Voice

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Managing Enterprise Voice for Users >

Topic Last Modified: *2012-09-21*

Use the following procedure to disable Enterprise Voice for a user account that is enabled for Lync Server 2013.

To disable a user account for Enterprise Voice

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to enable, and then click **Find**.
5. In the table, click the user account that you want to enable for Enterprise Voice.
6. On the **Edit** menu, click **Show details**.
7. On the **Edit Lync Server User** page, under **Telephony**, click any option except **Enterprise Voice**.

   > **Note:**
   >
   > To restrict a user from making audio or video calls by using Lync, under **Telephony**, click **Audio/video disabled**.

8. Click **Commit**.

The user is now unable to use the Enterprise Voice feature.

Tasks

Enable Users for Enterprise Voice

Other Resources

Managing Enterprise Voice for Users

Lync Server Management Shell

1.7.2.1.4 Modifying User Account Properties

Modifying User Account Properties

See Also

Operations > Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 >

Topic Last Modified: *2012-11-01*

You can use the procedures in this section to modify individual user account properties.

- Configure Telephony for a User
- Move Users to Another Pool

⊟See Also

Other Resources

User Accounts Enabled for Lync Server 2013
Assigning Per-User Policies

1.7.2.1.4.1 Configure Telephony for a User

Configure Telephony for a User

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Modifying User Account Properties >

Topic Last Modified: *2012-11-01*

Telephony settings are some of the individual settings of a user account that can be configured in Lync Server Control Panel for the user (that is, if the individual user has been enabled for Lync Server 2013 and the organization supports telephony).

Lync Server user telephony options include the following:

- **Audio/video disabled** The user cannot make calls with audio and video.
- **PC-to-PC only** The user can make only PC-to-PC audio or video calls.
- **Enterprise Voice** The user can use the Lync Server 2013 infrastructure to route all incoming and outgoing calls. The user can also make PC-to-PC calls.
- **Remote call control** The user can use Lync Server 2013 to control the desktop phone, and can also make PC-to-PC calls.

For details about configuring telephony for an organization, see Configure Telephony for a User and Deploying Enterprise Voice in the Deployment documentation.

⊟To configure telephony for a specific user account

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want, and then click **Find**.
5. In the table, click the user account that you want to modify.
6. On the **Edit** menu, click **Modify**.
7. In **Telephony**, do the following:

- To disable audio and video calls for the user, click **Audio/video disabled**.
- To enable PC-to-PC audio communications for the user, but not remote call control or Enterprise Voice, click **PC-to-PC only**. Specify a value for **Line URI** for the telephone that the user uses for PC-to-PC audio communications.
- To route the user's phone calls by using the Lync Server 2010 infrastructure in accordance with the class of service policy, including PC-to-PC audio communication, click **Enterprise Voice**. In **Line URI**, specify the telephone number for Enterprise Voice. In **Dial plan policy** and **Voice policy**, specify the appropriate policies for the user. To specify the normalization rules for translating phone numbers dialed by the user to the E.164 format, select the appropriate location profile in **Location policy**.
- To enable remote call control, which enables users to control their desktop phone line from Lync Server 2013 to make PC-to-PC calls and PC-to-phone calls, click **Remote call control**. In **Line URI**, specify the telephone number for remote call control. The user must have a desktop phone and private branch exchange (PBX) connection for call routing.

Other Resources

Modifying User Account Properties

1.7.2.1.4.2 Move Users to Another Pool

Move Users to Another Pool

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Modifying User Account Properties >

Topic Last Modified: *2013-03-11*

You can use Lync Server Control Panel to assign users to a specific server or pool.

Tip:

Moving all existing users from a source pool that is running Lync Server 2010 or earlier to a Lync Server 2013 destination pool in a complex Active Directory environment might result in slower Active Directory replication. To avoid this, you can use search filters to move users from pools that are running Lync Server 2010 or earlier separately, or you can use Lync Server Management Shell to move users with cmdlets. Also, the filter functionality works with Lync Server 2013 users.

⊟To move selected users to a different server or pool

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want, and then click **Find**.
5. In the table, select a specific user or users in the list.
6. On the **Action** menu, click **Move selected users to pool**.
7. In **Move Users**, select the pool that you want to move the users to in **Destination registrar pool**.
8. (Optional) If the destination server or pool is unavailable, select the **Force** check box.

> **Caution:**
> If you select **Force**, the user account is moved, but any associated user data is deleted (for example, conferences that the user has scheduled). If you do not select it, both the account and the associated data are moved.

⊟To move all users from one server or pool to a different server or pool

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. On the **Action** menu, click **Move all users to pool**.
5. In **Move Users**, select the pool that contains the user accounts that you want to move in **Source registrar pool**.
6. In **Destination registrar pool**, select the pool that you want to move the users to.
7. (Optional) If the destination server or pool is unavailable, select the **Force** check box.

> **Caution:**
> If you select **Force**, the user account is moved, but any associated user data is deleted (for example, conferences that the user has scheduled). If you do not select it, both the account and the associated data are moved.

⊟To move users from one pool to a different pool by using a filter

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In **User Search**, click **Search**, and then click **Add Filter**.
5. In the Search criteria, select **Registrar Pool**, select **Equal to**, select **Current Pool FQDN**, and then click **Find**.
6. On the **Action** menu, click **Move all users to pool**.

> **Note:**
> When a filter is applied to an existing set of users, the option **Move all users to pool** is in the context of the filtered subset of users, not ***all*** possible users.

7. In **Move Users**, select the pool that contains the user accounts that you want to move in **Source registrar pool**.
8. In **Destination registrar pool**, select the pool where you want to move the users.
9. (Optional) If the destination server or pool is unavailable, select the **Force** check box.

> **Caution:**
> If you select **Force**, the user account is moved, but any associated user data is deleted (for example, conferences that the user has scheduled and contacts). If you do not select it, both the account and the associated data are moved.

⊟To move users from one pool to another using Windows PowerShell cmdlets

1. Depending on how you run Windows PowerShell commands (that is, locally or remotely), you need to log on as a member of the correct Lync Server 2013

administrative roles as follows:

1.a. If you are running the commands on the local machine (for example, you log on directly to a Front End Server): Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.

1.b. If you are running the commands remotely on another computer (for example, you log on to your computer and run the commands remotely on a Standard Edition Front End Server): From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.

2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. To move single users, use the Move-CsUser cmdlet as follows:

```
Move-CsUser -Identity "Pilar Ackerman" -Target "pool01.contoso.net"
```

   Where the user to move is the user Pilar Ackerman, and the user will be moved from their currently assigned home pool to the pool pool01.contoso.net
4. To move a large number of users, use filters with the **Get-CsUser** cmdlet and pass the resulting set of users to **Move-CsUser**:

```
Get-CsUser -Filter {RegistrarPool -eq "CurrentPoolFqdn"} | Move-CsUser
```

   The combined commands of the **Get-CsUser** and **Move-CsUser** might result in this:

```
Get-CsUser -Filter {RegistrarPool -eq "pool02.contoso.net"} | Move-CsU
```

Other Resources

Modifying User Account Properties

1.7.2.1.5 Manage External Access Policy for Your Organization

Manage External Access Policy for Your Organization

Operations > Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 >

Topic Last Modified: *2013-02-22*

After deploying one or more Edge Servers, you must enable the types of external access that will be supported for your organization.

By default, there are no policies configured to support external user access, including remote user access, federated user access, even if you have already enabled external user access support for your organization. To control the use of external user access, you must configure one or more policies, specifying the type of external user access supported for each policy. The following policy scopes are available for creation and configuration. By default, the Global policy is created, but cannot be deleted.

- **Global policy** The global policy is created when you deploy your Edge Servers. By default, no external user access options are enabled in the global policy. To support external user access at the global level, you configure the global policy to support one or more types of external user access options. The global policy applies to all users in your organization, but site policies and user policies override the global policy. If you delete the global policy, you do not remove it. Instead, you reset it to the default setting.
- **Site policy** You can create and configure one or more site policies to limit support for external user access to specific sites. The configuration in the site policy overrides the global policy, but only for the specific site covered by the

site policy. For example, if you enable remote user access in the global policy, you might specify a site policy that disables remote user access for a specific site. By default, a site policy is applied to all users of that site, but you can assign a user policy to a user to override the site policy setting.

- **User policy** You can create and configure one or more user policies to limit support for remote user access to specific users. The configuration in the user policy overrides the global and site policy, but only for the specific users to whom the user policy is assigned. For example, if you enable remote user access in the global policy and site policy, you might specify a user policy that disables remote user access and then assign that user policy to specific users. If you create a user policy, you must apply it to one or more users before it takes effect.

> **Important:**
>
> Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

These options include the following types of external access:

- **Enable communications with federated users** Enable this if you want to support user access to federated partner domains. This setting configures the ability for users to communicate with other SIP federated domains, as well as Hosted providers like Microsoft Office 365. Selecting this setting allows you to select the option to allow communication with XMPP federated domains.
  As an option, you can select **Enable communications with XMPP federated partners** if you first select **Enable communications with federated users**. XMPP federation is a federation with organizations that use extensible messaging and presence protocol (XMPP).

  > **Note:**
  >
  > If you enable XMPP federation, you must also select to deploy **XMPP federation** in the Edge pools configuration section of Topology Builder. Configuring for XMPP federation deploys an XMPP Proxy on the Edge Server and an XMPP gateway on the Front End Server.

- **Enable communications with remote users** Enable this option if you want users in your organization who are outside your firewall, such as telecommuters and users who are traveling, to be able to connect to Lync Server over the Internet.
- **Enable communications with public users** Enable this option if you want internal users to be able to communicate with public IM provider contacts, such as those provided by Windows Live, Yahoo!, and America Online (AOL).

  > **Important:**
  >
  > - As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License (“PIC USL”) is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
  > - The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft’s ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
  > - More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be

added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

Note:
In addition to enabling external user access support, you must also configure policies to control the use of external user access in your organization before any type of external user access is available to users. For details about creating, configuring, and applying policies for external user access see Enable or Disable Remote User Access.

To view external access policies by using Windows PowerShell cmdlets

- You can view external access policies by using Lync Server Management Shell and the **Get-CsExternalAccessPolicy** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

  To view information about all your external access policies, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsExternalAccessPolicy
  ```

  This command returns information similar to the following:

  ```
  Identity                          : Global
  Description                       :
  EnableFederationAccess            : False
  EnableXmppAccess                  : False
  EnablePublicCloudAccess           : False
  EnablePublicCloudAudioVideoAccess : False
  EnableOutsideAccess               : False
  ```

- Configure Policies to Control Federated User Access
- Configure Policies to Control XMPP Federated User Access
- Configure Policies to Control Remote User Access
- Configure Policies to Control Public User Access
- Assign an External User Access Policy to a Lync Enabled User
- Resetting or Deleting External User Access Policies

1.7.2.1.5.1 Configure Policies to Control Federated User Access

Configure Policies to Control Federated User Access

See Also

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up Lync Federation >

Topic Last Modified: *2012-11-01*

When you configure policies to support communications with federated partners, the policies apply to users of federated domains. You can configure one or more external user access policies to control whether users of federated domains can collaborate with your Lync Server 2013 users. To control federated user access, you can configure policies at the global, site, and user level. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

Note:
You can configure policies to control federated user access, even if you have not enabled federation for your organization. However, the policies that you configure are in effect

only when you have federation enabled for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation. Additionally, if you specify a user policy to control federated user access, the policy applies only to users that are enabled for Lync Server 2013 and configured to use the policy. For details about specifying federated users that can sign in to Lync Server 2013, see Assign an External User Access Policy to a Lync Enabled User in the Deployment documentation or the Operations documentation.

⊟To configure a policy to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do one of the following:
   - To configure the global policy to support federated user access, click the global policy, click **Edit**, and then click **Show details**.
   - To create a new site policy, click **New**, and then click **Site policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
   - To create a new user policy, click **New**, and then click **User policy**. In **New External Access Policy**, create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnableFederatedUsers** for a user policy that enables communications for federated domain users).
   - To change an existing policy, click the appropriate policy listed in the table, click **Edit**, and then click **Show details**.
5. (Optional) If you want to add or edit a description, specify the information for the policy in **Description**.
6. Do one of the following:
   - To enable federated user access for the policy, select the **Enable communications with federated users** check box.
   - To disable federated user access for the policy, clear the **Enable communications with federated users** check box.
7. Click **Commit**.

To enable federated user access, you must also enable support for federation in your organization. For details, see Enable or Disable Federation and Public IM Connectivity.

If this is a user policy, you must also apply the policy to users that you want to be able to collaborate with federated users. For details, see Assign an External User Access Policy to a Lync Enabled User.

⊟To configure an existing policy using Windows PowerShell to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   Set-CsExternalAccessPolicy -Identity <name of global, site or user pol
   ```

   An example command that will set the global policy for Federated user access to enabled, XMPP domain access to enabled, Remote user access to enabled, Public provider access to enabled, and grant the ability to use audio and video for public providers that support it:

```
Set-CsExternalAccessPolicy -Identity global -EnableFederationAccess $t
```

Tip:

The parameter "EnablePublicCloudAudioVideoAccess" does not have a corresponding selection in the Lync Server Control Panel

To create a new policy using Windows PowerShell to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

```
New-CsExtenalAccessPolicy -Identity <name of site or user policy - you
```

An example of creating a new site policy:

```
New-CsExternalAccessPolicy -Identity site:Redmond -EnableFederationAcc
```

To delete or reset a policy using Windows PowerShell to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Type the following in the Lync Server Management Shell

```
Remove-CsExternalAccessPolicy -Identity <name of global, site or user
```

An example of resetting the global policy (The global policy can only have its setting removed. The policy cannot be deleted):

```
Remove-CsExternalAccessPolicy -Identity global
```

To remove a site policy, type:

```
Remove-CsExternalAccessPolicy -Identity site:Redmond
```

Deletes the site policy Redmond. To delete a user policy named UserEAPPolicy, type:

```
Remove-CsExternalAccessPolicy -Identity UserEAPPolicy
```

Tasks

Enable or Disable Federation and Public IM Connectivity
Assign an External User Access Policy to a Lync Enabled User

Other Resources

Manage SIP Federated Domains for Your Organization
Manage SIP Federated Providers for Your Organization
Set-CsExternalAccessPolicy
New-CsExternalAccessPolicy
Get-CsExternalAccessPolicy
Remove-CsExternalAccessPolicy
Grant-CsExternalAccessPolicy

1.7.2.1.5.2 Configure Policies to Control XMPP Federated User Access

Configure Policies to Control XMPP Federated User Access

See Also

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up XMPP Federation >

Topic Last Modified: *2012-11-01*

This is preliminary documentation and is subject to change. Blank topics are included as placeholders.

When you configure policies for support of extensible messaging and presence protocol (XMPP) federated partners, the policies apply to users of XMPP federated domains, but not to users of session initiation protocol (SIP) instant messaging (IM) service providers (for example, Windows Live), or SIP federated domains. You configure an **XMPP Federated Partner** for each XMPP federated domain that you want to allow your users to add contacts and communicate with. XMPP federated partners policies are only available in a single scope, though it is not defined as a global policy, acts as a global policy. To define a global, site or user policy for XMPP Federation Partners, you configure the policy scope by first creating and configuring the External Access Policy for the scope you require. For details about the types of policies that you can configure for external access and federation, see Managing Federation and External Access to Lync Server 2013 in the Operations documentation.

Note:

All **Federation and External Access** policies are applied through in-band provisioning. The policies that apply to the user, belong to a site, or are global in scope are communicated to the client during login. You can configure policies to control XMPP federated partner access, even if you have not enabled XMPP federation for your organization. However, the policies that you configure take effect only when you have XMPP partner federation deployed, enabled and configured for your organization. For details about deploying and configuring XMPP partner federation, see Configuring SIP Federation, XMPP Federation and Public Instant Messaging in the Deployment documentation. Additionally, if you specify a user policy in External Access Policy to control XMPP federated partners, the policy applies only to users that are enabled for Lync Server 2013 and configured to use the policy.

⊟To edit a global policy for XMPP federated partners

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do the following for the global policy:
5. Click the global policy, click **Edit**, and then click Show details.
6. Provide a description for the Global policy (optional).
7. Select **Enable communications with federated users**.
8. Select **Enable communications with XMPP federated users**.
9. Click **Commit** to save your changes to the Global policy.

⊟To create a site or user policy for XMPP federated partners

1. Click **New**, and then click **Site policy** or **User policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
2. Provide a description for the Site policy (optional).
3. In the site or user policy, select **Enable communications with federated users**.
4. Select **Enable communications with XMPP federated users**.
5. Click **Commit** to save your changes to the site or user policy.

To edit an existing policy for XMPP federated partners

1. To change an existing policy, select the appropriate policy in the list, click **Edit**, and then click **Show details**.
2. Change or update the description for the policy (optional).
3. Select or unselect **Enable communications with federated users**.
4. Select or unselect **Enable communications with XMPP federated users**.
5. Click **Commit** to save your changes to the policy.

To edit an existing policy for XMPP federated partners by using Windows PowerShell

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   Set-CsExternalAccessPolicy -Identity <name of global, site or user pol
   ```

   An example command that will set the global policy for Federated user access to True (enabled) and XMPP domain access to True (enabled):

   ```
   Set-CsExternalAccessPolicy -Identity global -EnableFederationAccess $t
   ```

To create a site or user policy for XMPP federated partners using Windows PowerShell

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   New-CsExternalAccessPolicy -Identity <name of global, site or user pol
   ```

   An example command that will set a site policy for the Redmond site for Federated user access to enabled and XMPP domain access to enabled:

   ```
   New-CsExternalAccessPolicy -Identity site:Redmond -EnableFederationAcc
   ```

To delete an existing policy for XMPP federated partners by using Windows PowerShell

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   Remove-CsExternalAccessPolicy -Identity <name of global, site or user
   ```

   An example command that will delete a user policy:

   ```
   Remove-CsExternalAccessPolicy -Identity EAPUserPolicySetXMPP
   ```

4. An example command that will reset the global policy to defaults:

   ```
   Remove-CsExternalAccessPolicy -Identity global
   ```

Tasks

Assign an External User Access Policy to a Lync Enabled User
Enable or Disable Federation and Public IM Connectivity

Other Resources

Manage XMPP Federated Partners for Your Organization
Set-CsExternalAccessPolicy
New-CsExternalAccessPolicy
Get-CsExternalAccessPolicy
Remove-CsExternalAccessPolicy
Grant-CsExternalAccessPolicy

1.7.2.1.5.3 Configure Policies to Control Remote User Access

Configure Policies to Control Remote User Access

Deployment > Deploying External User Access > Configuring Support for External User Access >

Topic Last Modified: *2012-10-18*

You configure one or more external user access policies to control whether remote users can collaborate with internal Lync Server users. To control remote user access, you can configure policies at the global, site, and user level. Site policies override the global policy, and user policies override site and global policies. For details about the types of policies that you can configure, see Managing Federation and External Access to Lync Server 2013. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

Note:

You can configure policies to control remote user access, even if you have not enabled remote user access for your organization. However, the policies that you configure are in effect only when you have remote user access enabled for your organization. For details about enabling remote user access, see Enable or Disable Federation and Public IM Connectivity. Additionally, if you specify a user policy to control remote user access, the policy applies only to users that are enabled for Lync Server and configured to use the policy. For details about specifying users that can sign in to Lync Server from remote locations, see Assign an External User Access Policy to a Lync Enabled User.

Use the following procedure to configure each external access policy that you want to use to control remote user access.

Note:

This procedure describes how to configure a policy only to enable communications with remote users, but each policy that you configure to support remote user access can also configure federated user access and public user access. For details about configuring policies to support federated users, see Configure Policies to Control Federated User Access. For details about configuring policies to support public users, see Create or Edit Public SIP Federated Providers.

⊟To configure an external access policy to support remote user access

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External**

Access Policy.

4. On the **External Access Policy** page, do one of the following:
   - To configure the global policy to support remote user access, click the global policy, click **Edit**, and then click **Show details**.
   - To create a new site policy, click **New**, and then click **Site policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
   - To create a new user policy, click **New**, and then click **User policy**. In **New External Access Policy**, create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnableRemoteUsers** for a user policy that enables communications for remote users).
   - To change an existing policy, click the appropriate policy listed in the table, click **Edit**, and then click **Show details**.
5. (Optional) If you want to add or edit a description, specify the information for the policy in **Description**.
6. Do one of the following:
   - To enable remote user access for the policy, select the **Enable communications with remote users** check box.
   - To disable remote user access for the policy, clear the **Enable communications with remote users** check box.
7. Click **Commit**.

To enable remote user access, you must also enable support for remote user access in your organization. For details, see Enable or Disable Federation and Public IM Connectivity in the Deployment documentation or the Operations documentation.

If this is a user policy, you must also apply the policy to users that you want to be able to connect remotely. For details, see Assign an External User Access Policy to a Lync Enabled User in the Deployment documentation or the Operations documentation.

1.7.2.1.5.4 Configure Policies to Control Public User Access

Configure Policies to Control Public User Access

See Also

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up Public Instant Messaging Connectivity >

Topic Last Modified: *2013-01-11*

Public instant messaging (IM) connectivity enables users in your organization to use IM to communicate with users of IM services provided by public IM service providers, including the Windows Live network of Internet services, Yahoo!, and AOL. You configure one or more external user access policies to control whether public users can collaborate with internal Lync Server users. Public instant messaging connectivity is an added feature that relies on configuration of your deployment and users. It also depends on the provisioning of the service at the public IM provider. For information on how to provision your deployment to use the public providers, see the “Public IM Connectivity Provisioning Guide for Microsoft Lync Server, Office Communications Server, and Live Communications Server” guide: http://go.microsoft.com/fwlink/?LinkId=269821

Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License (“PIC USL”) is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo!

Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.

- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

To access the Microsoft Lync Server Public IM Connectivity Provisioning site, use the following link: http://go.microsoft.com/fwlink/p/?linkId=212638

To control public user access, you can configure policies at the global, site, and user level. For details about the types of policies that you can configure, see Configuring Support for External User Access in the Deployment documentation or the Planning documentation. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

In the case of IM invitations, the response depends on the client software. The request is accepted unless external senders are explicitly blocked by a user-configured rule (that is, the settings in the user's client **Allow** and **Block** lists). Additionally, IM invitations can be blocked if a user elects to block all IM from users who are not on his or her **Allow** list.

Note:

You can configure policies to control public user access, even if you have not enabled federation for your organization. However, the policies that you configure are in effect only when you have federation enabled for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation. Additionally, if you specify a user policy to control public user access, the policy applies only to users that are enabled for Lync Server and configured to use the policy. For details about specifying public users that can sign in to Lync Server, see Assign an External User Access Policy to a Lync Enabled User in the Deployment documentation or the Operations documentation.

Use the following procedure to configure a policy to support access by users of one or more public IM providers.

To configure an external access policy to support public user access

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do one of the following:
   - To configure the global policy to support public user access, click the global policy, click **Edit**, and then click **Show details**.
   - To create a new site policy, click **New**, and then click **Site policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
   - To create a new user policy, click **New**, and then click **User policy**. In **New External Access Policy**, create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnablePublicUsers** for a user policy that enables communications for public users).
   - To change an existing policy, click the appropriate policy listed in the table,

click **Edit**, and then click **Show details**.

5. (Optional) If you want to add or edit a description, specify the information for the policy in **Description**.
6. Do one of the following:
   - To enable public user access for the policy, select the **Enable communications with public users** check box.
   - To disable public user access for the policy, clear the **Enable communications with public users** check box.
7. Click **Commit**.

To enable public user access, you must also enable support for federation in your organization. For details, see Configure Policies to Control Federated User Access.

If this is a user policy, you must also apply the policy to public users that you want to be able to collaborate with public users. For details, see Assigning Per-User Policies.

Tasks

Create or Edit Public SIP Federated Providers

Other Resources

Manage SIP Federated Providers for Your Organization

1.7.2.1.5.5 Assign an External User Access Policy to a Lync Enabled User

Assign an External User Access Policy to a Lync Enabled User

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Manage External Access Policy for Your Organization >

Topic Last Modified: *2013-02-22*

If a user has been enabled for Lync Server, you can configure SIP federation, XMPP federation, remote user access, and public instant messaging (IM) connectivity in the Lync Server Control Panel by applying the appropriate policies to specific users. For example, if you created a policy to support remote user access, you must apply it to the user before the user can connect to Lync Server from a remote location and collaborate with internal users from the remote location.

Note:

To support external user access, you must enable support for each type of external user access you want to support, and configure the appropriate policies and other options to control its use. For details, see Configuring Support for External User Access in the Deployment documentation or Managing Federation and External Access to Lync Server 2013 in the Operations documentation.

Use the procedure in this topic to apply a previously created external user access policy to one or more user accounts.

⊟To apply an external user policy to a user account

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**, and then search on the user account that you want to configure.
4. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
5. In **Edit Lync Server User** under **External access policy**, select the user

policy that you want to apply.

Note:
The **<Automatic>** settings apply the default server or global policy settings.

Assigning Per-User External Access Policies by Using Windows PowerShell Cmdlets

Per-user external access policies can be assigned by using Windows PowerShell and the Grant-CsExternalAccessPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user external access policy to a single user

- This command assigns the per-user external access policy RedmondExternalAccessPolicy to the user Ken Myer.

```
Grant-CsExternalAccessPolicy -Identity "Ken Myer" -PolicyName "RedmondE
```

To assign a per-user external access policy to multiple users

- This command assigns the per-user external access policy USAExternalAccessPolicy to all the users who have accounts in the UnitedStates OU in Active Directory. For more information on the OU parameter used in this command, see the documentation for the Get-CsUser cmdlet.

```
Get-CsUser -OU "ou=UnitedStates,dc=litwareinc,dc=com" | Grant-CsExterna
```

To unassign a per-user external access policy

- This command unassigns any per-user external access policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsExternalAccessPolicy -Identity "Ken Myer" -PolicyName $Null
```

For more information, see the help topic for the Grant-CsExternalAccessPolicy cmdlet.

1.7.2.1.5.6 Resetting or Deleting External User Access Policies

Resetting or Deleting External User Access Policies

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Manage External Access Policy for Your Organization >

Topic Last Modified: *2012-09-08*

If you have created or configured external user access policies that you no longer want to use, you can do the following:

- Delete any site or user policy that you created.
- Reset the global policy to the default settings. The default global policy settings deny any external user access. The global policy cannot be deleted.
- Delete a Site or User Policy for External User Access

- Reset the Global Policy for External User Access

Delete a Site or User Policy for External User Access

User Accounts Enabled for Lync Server 2013 > Manage External Access Policy for Your Organization > Resetting or Deleting External User Access Policies >

Topic Last Modified: *2013-02-22*

You can delete any site or user policy that is listed in Lync Server Control Panel on the **External Access Policy** page. Deleting the global policy does not actually delete it, but only resets it to the default settings, which do not include support for any external user access options. For details about resetting the global policy, see Reset the Global Policy for External User Access.

To delete a site or user policy for external user access

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. Click **External User Access**, click **External Access Policy**.
4. On the **External Access Policy** tab, click the site or user policy you want to delete, click **Edit**, and then click **Delete**.
5. When prompted to confirm the deletion, click **OK**.

Removing PIN Policies by Using Windows PowerShell Cmdlets

External access policies can be deleted by using Windows PowerShell and the Remove-CsExternalAccessPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specific external access policy

- This command removes the external access policy applied to the Redmond site:

```
Remove-CsExternalAccessPolicy -Identity "site:Redmond"
```

To remove all the external access policies applied to the per-user scope

- This command removes all the external access policies configured at the per-user scope:

```
Get-CsExternalAccessPolicy -Filter "tag:*" | Remove-CsExternalAccessPol
```

To remove all the external access policies where outside user access is disabled

- This command deletes all the external access policies where outside user access has been disabled:

```
Get-CsExternalAccessPolicy | Where-Object {$_.EnableOutsideAccess -eq $
```

For more information, see the help topic for the Remove-CsExternalAccessPolicy cmdlet.

Reset the Global Policy for External User Access

User Accounts Enabled for Lync Server 2013 > Manage External Access Policy for Your Organization > Resetting or Deleting External User Access Policies >

Topic Last Modified: *2013-02-22*

You cannot completely delete a global policy. Using the **Delete** option on the global policy only resets the global policy to the default settings, which do not include support for any external user access options.

To reset the global policy to the default settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, click **External Access Policy**.
4. On the **External Access Policy** tab, click the global policy, click **Edit**, and then click **Delete**.
5. When prompted to confirm the deletion, click **OK**. A message appears at the top of the page informing you that the global policy has been reset.

Resetting the Global External Access Policy by Using Windows PowerShell Cmdlets

The global external access policy can be reset by using Windows PowerShell and the Remove-CsExternalAccessPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To reset the global external access policy

- This command resets the global external access policy:

```
Remove-CsExternalAccessPolicy -Identity "global"
```

For more information, see the help topic for the Remove-CsExternalAccessPolicy cmdlet.

1.7.2.1.6 Assigning Per-User Policies

Assigning Per-User Policies

See Also

Operations > Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 >

Topic Last Modified: *2012-10-14*

You can assign certain policies to a user or a group of users in order to specify particular settings that deviate from the settings defined in policies assigned to other users, such as global policies. These policies are called per-user policies.

- Assign a Per-User Conferencing Policy
- Assign a Per-User Client Version Policy
- Assign a Per-User PIN Policy
- Assign an External User Access Policy to a Lync Enabled User
- Assign a Per-User Archiving Policy
- Assign a Per-User Location Policy
- Assign a Per-User Mobility Policy
- Assign a Per-User Persistent Chat Policy
- Assign a Per-User Dial Plan Policy
- Assign a Per-User Voice Policy

⊟See Also

Other Resources

Managing Users in Lync Server 2013

1.7.2.1.6.1 Assign a Per-User Conferencing Policy

Assign a Per-User Conferencing Policy

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

The conferencing policy is one of the individual settings of a user account that you can configure in Lync Server Control Panel.

Deploying one or more per-user conferencing policies is optional. You can also deploy only a global-level conferencing policy or site-level conferencing policy. If you do deploy per-user policies, you must explicitly assign them to users, groups, or contact objects. Conferencing user rights and permissions automatically default to those defined in the global-level conferencing policy when no specific site-level or per-user policy is assigned.

After creating at least one per-user conferencing policy, use the procedures in this topic to assign the policy that specifies the user rights and permissions that you want the server to grant to the meetings organized by a particular user.

For a list of all available conferencing policy settings, see Conferencing Policy Settings Reference.

For details about creating conferencing policies, see Create or Modify a Conferencing Policy.

⊟To assign a per-user conferencing policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.

4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

     Tip:
     To add additional search clauses to your query, click **Add Filter**.

   - Click **Find**.
6. Click a user in the search results, click **Action**, and then click **Assign policies**.

   Tip:
   If you want the same per-user conferencing policy to apply to multiple users, select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **Conferencing policy**, do one of the following:

   Note:
   Because there are multiple policies that you can configure in **Assign Policies**, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

   - Select **<Automatic>** to allow Lync Server 2013 to automatically choose either the global-level policy or, if defined, the site-level policy.
   - Click the name of a per-user conferencing policy you previously defined on the **Conferencing Policy** page.

     Tip:
     To help you decide the policy you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

Assigning a Per-User Conferencing Policy by Using Windows PowerShell Cmdlets

Per-user conferencing policies can be assigned by using Windows PowerShell and the Grant-CsConferencingPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To assign a per-user conferencing policy to a single user

- The following command assigns the per-user conferencing policy RedmondConferencingPolicy to the user Ken Myer.

```
Grant-CsConferencingPolicy -Identity "Ken Myer" -PolicyName "RedmondCon
```

To assign a per-user conferencing policy to multiple users

- This command assigns the per-user conferencing policy HRConferencingPolicy to all the users who work for the Human Resources department. For more information on the LdapFilter parameter used in this command, see the documentation for the Get-CsUser cmdlet.

  ```
  Get-CsUser -LdapFilter "Department=Human Resources" | Grant-CsConferenc
  ```

To unassign a per-user conferencing policy

- The following command unassigns any per-user conferencing policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

  ```
  Grant-CsConferencingPolicy -Identity "Ken Myer" -PolicyName $Null
  ```

For more information, see the help topic for the Grant-CsConferencingPolicy cmdlet.

See Also

Tasks

Create or Modify a Conferencing Policy

Other Resources

Assigning Per-User Policies

1.7.2.1.6.2 Assign a Per-User Client Version Policy

Assign a Per-User Client Version Policy

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

The client version policy is one of the individual settings of a user account that you can configure in the Lync Server Control Panel.

Deploying one or more per-user client version policies is optional. You can also deploy only a global-level client version policy, or site-level or pool-level client version policies. If you do deploy per-user policies, you must explicitly assign them to users, groups, or contact object. When no specific site-level, pool-level, or per-user policy is assigned, the default clients that are allowed to register with Lync Server 2013 are those defined in the global-level client version policy.

After creating at least one per-user client version policy, use the procedures in this topic to assign the policy that specifies the client versions that you want to allow to register with Lync Server.

For details about creating per-user client version policies, see Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013.

To assign a per-user client version policy

1. From a user account that is assigned to the CsUserAdministrator role or the

CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

     Tip:
     To add additional search clauses to your query, click **Add Filter**.

   - Click **Find**.
6. Click a user in the search results, click **Action**, and then click **Assign policies**.

   Tip:
   If you want the same per-user client version policy to apply to multiple users, select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **Client version policy**, do one of the following:

   Note:
   Because there are multiple policies that you can configure by using the **Assign Policies** dialog box, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

   - Allow Lync Server to automatically choose either the global-level policy or, if defined, the site-level policy or pool-level policy.
   - Click the name of a per-user client version policy you previously defined on the **Client Version Policy** page.

     Tip:
     To help you decide the policy you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

Assigning a Per-User Client Version Policy by Using Windows PowerShell Cmdlets

You can assign per-user client version policies by using the Grant-CsClientVersionPolicy cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user client version policy to a single user

- The following command assigns the per-user client version policy RedmondClientVersionPolicy to the user Ken Myer.

```
Grant-CsClientVersionPolicy -Identity "Ken Myer" -PolicyName "RedmondCl
```

To assign a per-user client version policy to multiple users

- This command assigns the per-user client version policy RedmondClientVersionPolicy to all the users who are currently assigned the voice policy RedmondVoicePolicy. For more information on the Filter parameter used in this command, see the documentation for the Get-CsUser cmdlet.

```
Get-CsUser -Filter {VoicePolicy -eq "RedmondVoicePolicy"} | Grant-CsCli
```

To unassign a per-user client version policy

- The following command unassigns any per-user client version policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy, his local site policy (if one exists), or the service-scope policy assigned to his Registrar. A service scope policy takes precedence over any site policy, and a site policy takes precedence over the global policy.

```
Grant-CsClientVersionPolicy -Identity "Ken Myer" -PolicyName $Null
```

For more information, see the help topic for the Grant-CsClientVersionPolicy cmdlet.

See Also

Other Resources

Assigning Per-User Policies
Managing Devices, Phones, and Client Applications

1.7.2.1.6.3 Assign a Per-User PIN Policy

Assign a Per-User PIN Policy

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

The dial-in conferencing personal identification number (PIN) policy is one of the individual settings of a user account that can be configured in the Lync Server 2013 Control Panel.

Deploying one or more per-user PIN policies is optional. You can also deploy only a global-level PIN policy or site-level PIN policy. If you do deploy per-user policies, you must explicitly assign them to users, groups, or contact object. User rights and permissions regarding the use of PINs for dial-in conferencing automatically default to those defined in the global-level PIN policy when no specific site-level or per-user policy is assigned.

After creating at least one per-user PIN policy, use the procedures in this topic to assign the policy that specifies the constraints you want the server to impose on the PINs created by and used by a particular user.

For details about creating per-user dial-in conferencing PIN policies, see Create or Modify Dial-in Conferencing PIN Settings for a Site or Group of Users.

To assign a per-user PIN policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

     Tip:
     To add additional search clauses to your query, click **Add Filter**.

   - Click **Find**.
6. Click a user in the search results, click **Action**, and then click **Assign policies**.

   Tip:
   If you want the same per-user PIN policy to apply to multiple users, select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **PIN policy**, do one of the following:

   Note:
   Because there are multiple policies that you can configure by using the **Assign Policies** dialog box, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

   - Allow Lync Server 2013 to automatically choose either the global-level policy or, if defined, the site-level policy.
   - Click the name of a per-user PIN policy you previously defined on the **PIN Policy** page.

     Tip:
     To help you decide the policy you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

Assigning a Per-User PIN Policy by Using Windows PowerShell Cmdlets

You can assign per-user PIN policies by using Windows PowerShell and the **Grant-CsPinPolicy** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote

Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To assign a per-user PIN policy to a single user

- The following command assigns the per-user PIN policy RedmondPinPolicy to the user Ken Myer.

```
Grant-CsPinPolicy -Identity "Ken Myer" -PolicyName "RedmondPinPolicy"
```

⊟To assign a per-user PIN policy to multiple users

- The following command assigns the per-user PIN policy RedmondUsersPinPolicy to all the users who work in the city of Redmond. For details about the LdapFilter parameter used in this command, see Get-CsUser.

```
Get-CsUser -LdapFilter "l=Redmond" | Grant-CsPinPolicy -PolicyName "Red
```

⊟To unassign a per-user PIN policy

- The following command unassigns any per-user PIN policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsPinPolicy -Identity "Ken Myer" -PolicyName $Null
```

For details, see Grant-CsPinPolicy.

⊟See Also

Tasks

Create a New PIN Policy

Other Resources

Assigning Per-User Policies

1.7.2.1.6.4 Assign an External User Access Policy to a Lync Enabled User

Assign an External User Access Policy to a Lync Enabled User

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Manage External Access Policy for Your Organization >

Topic Last Modified: *2013-02-22*

If a user has been enabled for Lync Server, you can configure SIP federation, XMPP federation, remote user access, and public instant messaging (IM) connectivity in the Lync Server Control Panel by applying the appropriate policies to specific users. For example, if you created a policy to support remote user access, you must apply it to the user before the user can connect to Lync Server from a remote location and collaborate with internal users from the remote location.

Note:

To support external user access, you must enable support for each type of external user access you want to support, and configure the appropriate policies and other options to control its use. For details, see Configuring Support for External User Access in the Deployment documentation or Managing Federation and External Access to Lync Server 2013 in the Operations documentation.

Use the procedure in this topic to apply a previously created external user access policy to one or more user accounts.

To apply an external user policy to a user account

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**, and then search on the user account that you want to configure.
4. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
5. In **Edit Lync Server User** under **External access policy**, select the user policy that you want to apply.

   Note:
   The **<Automatic>** settings apply the default server or global policy settings.

Assigning Per-User External Access Policies by Using Windows PowerShell Cmdlets

Per-user external access policies can be assigned by using Windows PowerShell and the Grant-CsExternalAccessPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user external access policy to a single user

- This command assigns the per-user external access policy RedmondExternalAccessPolicy to the user Ken Myer.

```
Grant-CsExternalAccessPolicy -Identity "Ken Myer" -PolicyName "RedmondE
```

To assign a per-user external access policy to multiple users

- This command assigns the per-user external access policy USAExternalAccessPolicy to all the users who have accounts in the UnitedStates OU in Active Directory. For more information on the OU parameter used in this command, see the documentation for the Get-CsUser cmdlet.

```
Get-CsUser -OU "ou=UnitedStates,dc=litwareinc,dc=com" | Grant-CsExterna
```

To unassign a per-user external access policy

- This command unassigns any per-user external access policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsExternalAccessPolicy -Identity "Ken Myer" -PolicyName $Null
```

For more information, see the help topic for the Grant-CsExternalAccessPolicy cmdlet.

Assign a Per-User Archiving Policy

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

The archiving policy is one of the individual settings of a user account that you can configure in the Lync Server 2013 Control Panel.

Deploying one or more per-user archiving policies is optional. You can also deploy only a global-level archiving policy or site-level archiving policy. If you do deploy per-user policies, you must explicitly assign them to users, groups, or contact object. Archiving requirements automatically default to those defined in the global-level conferencing policy when no specific site-level or per-user policy is assigned.

After creating at least one per-user archiving policy, use the procedures in this topic to assign the policy that appropriately specifies whether a particular user’s internal communications, external communications, or both, will be archived by the server.

For details about creating per-user archiving policies, see Creating an Archiving Policy to Enable or Disable Archiving of Internal or External Communications for Specific Sites or Users.

⊟To assign a per-user archiving policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

Tip:
To add additional search clauses to your query, click **Add Filter**.

   - Click **Find**.
6. Click a user in the search results, click **Action**, and then click **Assign policies**.

Tip:
If you want the same per-user archiving policy to apply to multiple users,

> select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **Archiving policy**, do one of the following:

> **Note:**
>
> Because there are multiple policies that you can configure by using the **Assign Policies** dialog box, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

- Allow Lync Server 2013 to automatically choose either the global-level policy or, if defined, the site-level policy.
- Click the name of a per-user archiving policy you previously defined on the **Archiving Policy** page.

> **Tip:**
>
> To help you decide the policy that you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

Assigning a Per-User Archiving Policy by Using Windows PowerShell Cmdlets

You can assign per-user archiving policies by using Windows PowerShell and the **Grant-CsArchivingPolicy** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user archiving policy to a single user

- The following command assigns the per-user archiving policy RedmondArchivingPolicy to the user Ken Myer.

```
Grant-CsArchivingPolicy -Identity "Ken Myer" -PolicyName "RedmondArchiv
```

To assign a per-user archiving policy to multiple users

- This command assigns the per-user archiving policy RedmondArchivingPolicy to all the users who have accounts homed on the Registrar pool atl-cs-001.litwareinc.com. For more information on the Filter parameter used in this command, see the documentation for the Get-CsUser cmdlet.

```
Get-CsUser -Filter {RegistrarPool -eq "atl-cs-001.litwareinc.com"} | Gr
```

To unassign a per-user archiving policy

- The following command unassigns any per-user archiving policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsArchivingPolicy -Identity "Ken Myer" -PolicyName $Null
```

For more information, see the help topic for the Grant-CsArchivingPolicy cmdlet.

See Also

Tasks

Creating an Archiving Policy to Enable or Disable Archiving of Internal or External Communications for Specific Sites or Users

Other Resources

Assigning Per-User Policies

1.7.2.1.6.6 Assign a Per-User Location Policy

Assign a Per-User Location Policy

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

The location policy is one of the individual settings of a user account that you can configure in the Lync Server Control Panel.

Deploying one or more per-user location policies is optional. You can also deploy only a global-level location policy or subnet-level location policy. If you do deploy per-user policies, you must explicitly assign them to users, groups, or contact object. Enhanced 9-1-1 (E9-1-1) settings automatically default to those defined in the global-level location policy when no specific subnet-level or per-user policy is assigned.

After creating at least one per-user location policy, use the procedures in this topic to assign to the policy that specifies the settings that you want the server to apply for emergency calls placed by a particular user.

For a list of all available location policy settings, see Defining the Location Policy.

For details about creating location policies, see Create Location Policies.

⊟To assign a per-user location policy with the Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

Tip:
To add additional search clauses to your query, click **Add Filter**.

- Click **Find**.

6. Click a user in the search results, click **Action**, and then click **Assign policies**.

   > **Tip:**
   > If you want the same per-user location policy to apply to multiple users, select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **Location policy**, do one of the following:

   > **Note:**
   > Because there are multiple policies that you can configure by using the **Assign Policies** dialog box, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

   - Allow Lync Server 2013 to automatically choose either the global-level policy or, if defined, the subnet-level policy.
   - Click the name of a per-user location policy you previously defined by running the **New-CsLocationPolicy** cmdlet.

     > **Tip:**
     > To help you decide the policy that you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

Assigning a Per-User Location Policy by Using Lync Server Management Shell Cmdlets

You can assign per-user location policies by using the Grant-CsLocationPolicy cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user location policy to a single user

- The following command assigns the per-user location policy RedmondLocationPolicy to the user Ken Myer.

```
Grant-CsLocationPolicy -Identity "Ken Myer" -PolicyName "RedmondLocatio
```

To assign a per-user location policy to multiple users

- This command assigns the per-user location policy AccountingDepartmentLocationPolicy to all the users who work for the Accounting department. For more information on the LdapFilter parameter used in this command, see the documentation for the Get-CsUser cmdlet.

```
Get-CsUser -LdapFilter "Department=Accounting" | Grant-CsLocationPolicy
```

To unassign a per-user location policy

- The following command unassigns any per-user location policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsLocationPolicy -Identity "Ken Myer" -PolicyName $Null
```

For more information, see the help topic for the Grant-CsLocationPolicy cmdlet.

1.7.2.1.6.7 Assign a Per-User Mobility Policy

Assign a Per-User Mobility Policy

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

The mobility policy is one of the individual settings of a user account that you can configure in Lync Server Control Panel or Lync Server Management Shell.

⊟To assign a per-user mobility policy with Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

     > **Tip:**
     > To add additional search clauses to your query, click **Add Filter**.

   - Click **Find**.
6. Click a user in the search results, click **Action**, and then click **Assign policies**.

   > **Tip:**
   > If you want the same per-user mobility policy to apply to multiple users, select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **Mobility policy**, do one of the following:

   > **Note:**
   > Because there are multiple policies that you can configure in **Assign Policies**, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

   - Select **<Automatic>** to allow Lync Server 2013 to automatically choose either the global-level policy or, if defined, the site-level policy.

- Click the name of a per-user mobility policy you previously defined on the **Mobility Policy** page.

Tip:
To help you decide the policy you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

Assigning a Per-User Mobility Policy by Using Windows PowerShell Cmdlets

You can assign per-user mobility policies by using Windows PowerShell and the **Grant-CsMobilityPolicy** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To assign a per-user mobility policy to a single user

- The following command assigns the per-user mobility policy RedmondMobilityPolicy to the user Ken Myer.

```
Grant-CsMobilityPolicy -Identity "Ken Myer" -PolicyName "RedmondMobilit
```

⊟To assign a per-user mobility policy to multiple users

- The following command assigns the per-user mobility policy RedmondMobilityPolicy to all the users who are currently assigned the policy NorthAmericaMobilityPolicy. For details about the Filter parameter used in this command, see Get-CsUser.

```
Get-CsUser -Filter {MobilityPolicy -eq "NorthAmericaMobilityPolicy"} |
```

⊟To unassign a per-user mobility policy

- The following command unassigns any per-user mobility policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsMobilityPolicy -Identity "Ken Myer" -PolicyName $Null
```

For details, see Grant-CsMobilityPolicy.

⊟See Also

Tasks

Configuring Mobility Policy

1.7.2.1.6.8 Assign a Per-User Persistent Chat Policy

Assign a Per-User Persistent Chat Policy

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

You can assign a per-user persistent chat policy with either Lync Server 2013 Control Panel or Lync Server 2013 Management Shell. For details on creating user policies for Persistent Chat Server, see Create a User Policy for Persistent Chat.

To assign a per-user persistent chat policy with Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

     > **Tip:**
     > To add additional search clauses to your query, click **Add Filter**.

   - Click **Find**.
6. Click a user in the search results, click **Action**, and then click **Assign policies**.

   > **Tip:**
   > If you want the same per-user persistent Chat policy to apply to multiple users, select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **Persistent Chat policy**, do one of the following:

   > **Note:**
   > Because there are multiple policies that you can configure by using the **Assign Policies** dialog box, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

   - Select **<Automatic>** to allow Lync Server 2013 to automatically choose either the global-level policy or, if defined, the site-level policy.
   - Click the name of a per-user Persistent Chat policy you previously defined on the **Persistent Chat Policy** page.

     > **Tip:**
     > To help you decide the policy you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

Assigning a Per-User Persistent Chat Policy by Using Windows PowerShell Cmdlets

You can also assign per-user persistent chat policies by using the **Grant-CsPersistentChatPolicy** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To assign a per-user persistent chat policy to a single user

- The following command assigns the per-user Persistent Chat policy RedmondPersistentChatPolicy to the user Ken Myer.

```
Grant-CsPersistentChatPolicy -Identity "Ken Myer" -PolicyName "RedmondP
```

⊟To assign a per-user persistent chat policy to multiple users

- This command assigns the per-user Persistent Chat policy RedmondUsersPersistentChatPolicy to all the users who work for the IT department. For more information on the LdapFilter parameter used in this command, see the documentation for the Get-CsUser cmdlet.

```
Get-CsUser -LdapFilter "Department=IT" | Grant-CsPersistentChatPolicy -
```

⊟To unassign a per-user persistent chat policy

- The following command unassigns any per-user Persistent Chat policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsPersistentChatPolicy -Identity "Ken Myer" -PolicyName $Null
```

For more information, see the help topic for the Grant-CsPersistentChatPolicy cmdlet.

⊟See Also

Concepts

Create a User Policy for Persistent Chat

1.7.2.1.6.9 Assign a Per-User Dial Plan Policy

Assign a Per-User Dial Plan Policy

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

To complete user account configuration for either users of Enterprise Voice or users of dial-in conferencing, the user must be assigned a dial plan. User accounts will automatically use the global dial plan or, if one exists, the site-level dial plan when you do not explicitly assign an existing per-user dial plan. If you want to use the global or site dial plan for all users that are enabled for Enterprise Voice, you can skip this section.

To assign a dial plan by using the Lync Server 2013 Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account that you want to enable, and then click **Find**.
5. In the table, click the user account that you want to assign a dial plan.
6. On the **Edit** menu, click **Show details**.
7. On the **Edit Lync Server User** page, under **Telephony**, click **Enterprise Voice**.
8. Click **Dial plan policy**, and then choose the desired dial plan.
9. Click **Commit**.

For details about configuring dial plans, see the Configuring Dial Plans topic.

Assign a Per-User Dial Plan by Using Windows PowerShell Cmdlets

You can assign per-user dial plans with Windows PowerShell and the **Grant-CsdialPlan** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user dial plan to a single user

- The following command assigns the per-user dial plan RedmondDialPlan to the user Ken Myer.

```
Grant-CsDialPlan -Identity "Ken Myer" -PolicyName "RedmondDialPlan"
```

To assign a per-user dial plan to multiple users

- This command assigns the per-user dial plan RedmondDialPlan to all the users who work in the city of Redmond. For more information on the LdapFilter parameter used in this command, see the documentation for the Get-CsUser cmdlet.

```
Get-CsUser -LdapFilter "l=Redmond" | Grant-CsDialPlan -PolicyName "Redm
```

To unassign a per-user dial plan

- The following command unassigns any per-user dial plan previously assigned to Ken Myer. After the per-user dial plan is unassigned, Ken Myer will automatically be managed by using the global dial plan, his local site dial plan (if one exists), or the service-scope dial plan assigned to his Registrar or PSTN gateway. A service scope dial plan takes precedence over any site dial plan, and a site dial plan takes precedence over the global dial plan.

```
Grant-CsDialPlan -Identity "Ken Myer" -PolicyName $Null
```

For more information, see the help topic for the Grant-CsDialPlan cmdlet.

See Also

Other Resources

Configuring Dial Plans
User Accounts Enabled for Lync Server 2013

1.7.2.1.6.10 Assign a Per-User Voice Policy

Assign a Per-User Voice Policy

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

Global and site-level voice policies are automatically assigned to all Lync Server 2013 user accounts that are enabled for Enterprise Voice. You can also assign voice policies to specific users by using either the Lync Server 2013 Control Panel or the Lync Server 2013 Management Shell. Use the procedures in this topic to explicitly assign per-user policies to Lync Server users.

To assign a user-specific voice policy using the Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**, and then search on the user account that you want to configure.
4. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
5. In **Edit Lync Server User** under **Voice policy**, select the user policy that you want to apply.

Note:
The **<Automatic>** settings apply the default server or global policy settings.

Assigning a Per-User Voice Policy by using Windows PowerShell Cmdlets

You can assign per-user voice policies by using Windows PowerShell and the **Grant-CsVoicePolicy** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user voice policy to a single user

- The following command assigns the per-user voice policy RedmondVoicePolicy to the user Ken Myer.

```
Grant-CsVoicePolicy -Identity "Ken Myer" -PolicyName "RedmondVoicePolic
```

⊟To assign a per-user voice policy to multiple users

- This command assigns the per-user voice policy FinanceVoicePolicy to all the users who have accounts in the Finance OU in Active Directory. For more information on the OU parameter used in this command, see the documentation for the Get-CsUser cmdlet.

```
Get-CsUser -OU "ou=Finance,ou=North America,dc=litwareinc,dc=com" | Gra
```

⊟To unassign a per-user voice policy

- The following command unassigns any per-user voice policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsVoicePolicy -Identity "Ken Myer" -PolicyName $Null
```

For more information, see the help topic for the Grant-CsVoicePolicy cmdlet.

⊟See Also

Tasks

Disable a User for Enterprise Voice

Other Resources

Lync Server Management Shell

1.7.3 Managing the Lync Server 2013 Topology

Managing the Lync Server 2013 Topology

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-10-11*

Topics in this section provide step-by-step procedures for tasks you can perform using the **Topology** page in Lync Server 2013 Control Panel.

- View a List of Computers Running Lync Server 2013
- View the Status of Services Running on a Computer
- View Details about a Service
- Start or Stop Lync Server 2013 Services
- Prevent Sessions for Services
- Upgrade or Update Front End Servers
- Add or Remove a Front End Server
- Upgrade or Update a Back End Server or Standard Edition Server
- Managing Microsoft SIP Processing Language (MSPL) Applications
- Managing Simple URLs

1.7.3.1 View a List of Computers Running Lync Server 2013

View a List of Computers Running Lync Server 2013

See Also

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2012-11-01*

You can use Lync Server 2013 Control Panel to view a list of all the computers that are running Lync Server 2013 in your topology and see the service status of each. You can sort the list by computer, pool, or site.

⊟To view a list of computers running Lync Server

1. From a user account that is assigned to any of the predefined administrative roles for Lync Server 2013, log on to any computer in your internal deployment. For details about the predefined administrative roles available in Lync Server 2013, see Planning for Role-Based Access Control.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, do any of the following as needed:
   - Sort the list by clicking the **Computer**, **Pool**, or **Site** column heading, and then clicking the up arrow or the down arrow.
   - Click **Refresh** to view the most up-to-date list.
   - Search for a specific computer by typing the computer name in the search field.

Other Resources

Managing the Lync Server 2013 Topology

1.7.3.2 View the Status of Services Running on a Computer

View the Status of Services Running on a Computer

See Also

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2013-02-22*

You can use Lync Server 2013 Control Panel to view all the services that are running on a specific computer in your Lync Server topology and see the status of each service.

⊟To view the status of services running on a computer

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology**.
4. On the **Status** page, sort or search the list, as required, to find the computer you're interested in, and then click the computer name.
5. Do any of the following:
   - To see the latest status of services running on the computer, click **Get service status**.
   - To see a list of specific services running on the computer and the status of each service, click **Properties**, and then click **Close** to return to the list.

Viewing Service Status by Using Windows PowerShell Cmdlets

You can also view service status by using Windows PowerShell and the **Get-CsWindowsService** cmdlet. You can run this cmdlet from the Lync Server 2013

Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view service status

- To view service status on a computer, type a command similar to the following in the Lync Server Management Shell and then press Enter:

```
Get-CsWindowsService -ComputerName atl-cs-001.litwareinc.com | Select-O
```

This command returns information similar to the following:

```
RoleName                                    Status
--------                                    ------
{W3SVC}                                     Running
{CentralManagement}                         Running
{ClsAgent}                                  Running
{Registrar, UserServer, EdgeServer}         Running
{ApplicationServer}                         Running
{ConferencingServer}                        Running
{MediationServer}                           Running
```

For details, see Get-CsWindowsService.

See Also

Other Resources

Managing Devices, Phones, and Client Applications

1.7.3.3 View Details about a Service

View Details about a Service

See Also

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2012-09-21*

You can use Lync Server Control Panel to view details about each service that is running on a specific computer in your topology. You can view the status of each service and details such as the associated databases, ports, and dependent services.

To view details for a service

1. From a user account that is assigned to any of the predefined administrative roles for Lync Server 2013, log on to any computer in your internal deployment. For details about the predefined administrative roles available in Lync Server 2013, see Planning for Role-Based Access Control.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. In the **Status** page, sort or search through the list and then click the computer that you want to view.
5. Click **Properties**.
6. In the **View Computer Detail** window, sort the list of services, if necessary, and click the service you want to view.
7. Do any of the following as needed:
   - To see the latest status of that specific service, click **Get service status**.
   - To see the details for that specific service, click **Properties** and then click **Close**.

- To return to the list of all computers in your topology, click **Close**.

Other Resources

Managing the Lync Server 2013 Topology

1.7.3.4 Start or Stop Lync Server 2013 Services

Start or Stop Lync Server 2013 Services

See Also

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2012-11-01*

You can use Lync Server Control Panel to start or stop all the Lync Server 2013 services running on a specific computer or to start or stop a specific service.

⊟To start or stop all Lync Server services on a computer

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the services you want to start or stop, and then click it.
5. Click **Action**.
6. Click **Start All services** or **Stop All services**.

⊟To start or stop a specific service

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the service you want to start or stop, and then click it.
5. Click **Properties**.
6. Sort the list of services, if necessary, and click the service you want to start or stop.
7. Click **Action**.
8. Click **Start service** or **Stop service**.
9. Click **Close**.

Tasks

Prevent Sessions for Services

Other Resources

Managing the Lync Server 2013 Topology

1.7.3.5 Prevent Sessions for Services

Prevent Sessions for Services

See Also

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2012-11-01*

You can use Lync Server Control Panel to prevent new sessions for all the Lync Server 2013 services running on a specific computer or to prevent new sessions for a specific Lync Server 2013 service.

⊟To prevent new sessions for all Lync Server services on a computer

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the services for which you want to prevent new sessions, and then click it.
5. Click **Action**.
6. Click **Prevent new sessions for all services**.

⊟To prevent new sessions for a specific service

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and then click **Status**.
4. On the **Status** page, sort or search through the list as needed to find the computer that is running the service you want to start or stop, and then click it.
5. Click **Properties**.
6. Sort the list of services, if necessary, and click the service for which you want to prevent new sessions.
7. Click **Action**.
8. Click **Prevent new sessions for service**.
9. Click **Close**.

Other Resources

Managing the Lync Server 2013 Topology

1.7.3.6 Upgrade or Update Front End Servers

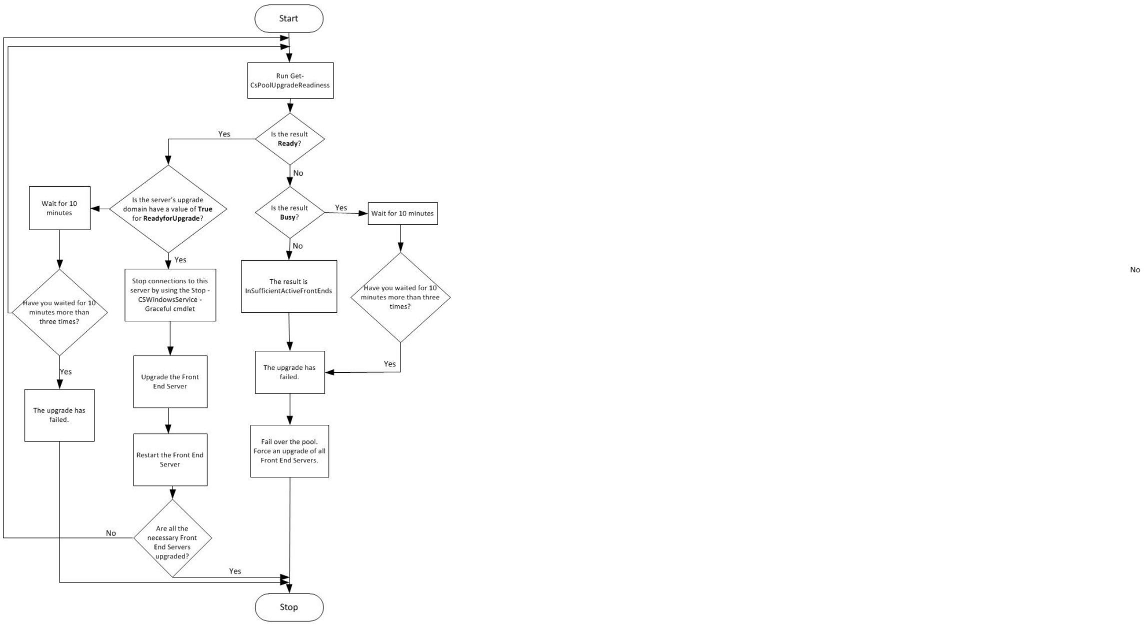
Upgrade or Update Front End Servers

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2013-02-22*

The Front End Servers in an Enterprise Edition pool are organized into *upgrade domains*. These are subsets of Front End Servers in the pool. Upgrade domains are created automatically by Topology Builder.

We recommend that when you upgrade Front End Servers, you perform the upgrades one server at a time. Bring one server down, upgrade it, and then restart it before you upgrade another server. Be sure to keep track of which servers you have upgraded so far.


Start
Run Get-CsPoolUpgradeReadiness
Is the result **Ready**?
Yes
No
Is the server's upgrade domain have a value of **True** for **ReadyforUpgrade**?
Wait for 10 minutes
Is the result **Busy**?
Yes
Wait for 10 minutes
No
Yes
Stop connections to this server by using the Stop -CSWindowsService -Graceful cmdlet
The result is InSufficientActiveFrontEnds
Have you waited for 10 minutes more than three times?
Have you waited for 10 minutes more than three times?
No
Yes
Yes
The upgrade has failed.
Upgrade the Front End Server
The upgrade has failed.
Restart the Front End Server
Fail over the pool. Force an upgrade of all Front End Servers.
No
Are all the necessary Front End Servers upgraded?
Yes
Stop

⊟To apply an upgrade to a Front End server in a pool

1. On a Front End Server in the pool, run the following cmdlet:

   Get-CsPoolUpgradeReadiness

   If the value of *PoolUpgradeState* is **Busy**, wait for 10 minutes, and then try **Get-CsPoolUpgradeReadiness** again. If you see **Busy** for at least three consecutive times, after waiting 10 minutes in between each attempt, or if you see any result of **InsufficientActiveFrontEnds** for **PoolUpgradeState,** then there is an issue with the pool. If this pool is paired with another Front End pool in a disaster recovery topology, you should fail the pool over to the backup pool, and then update the servers in this pool. For details, see Failing Over a Pool.

   If the value of *PoolUpgradeState* is **Ready**, go to step 2.
2. The **Get-CsPoolUpgradeReadiness** cmdlet also returns information about each upgrade domain in the pool, and about which Front End Servers are in each upgrade domain. If the **ReadyforUpgrade** value is **True** for the upgrade domain that contains the server you want to upgrade, you can safely upgrade that server now. To do so, do the following:

   2.a.Stop new connections to the Front End Server by using the `Stop -CsWindowsServices -Graceful` cmdlet.

   2.b.Restart the server, and make sure it is accepting new connections.

1.7.3.7 Add or Remove a Front End Server

Add or Remove a Front End Server

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2012-11-01*

When you add a Front End Server to a pool, or remove a Front End Server from a pool, you then need to restart the pool. To prevent any interruption of service to users, use the following procedure when adding or removing a Front End Server.

To add or remove Front End servers

1. If you are removing any Front End Servers, first stop new connections to those servers. To do so, you can use the following cmdlet:

   ```
   Stop -CsWindowsServices -Graceful
   ```

2. When the servers being removed have no current sessions, stop Lync Server services on them.
3. Open Topology Builder, and add or remove the necessary servers.
4. Publish the topology.
5. If the pool has gone from having two Front End Servers to more than two, or gone from more than two servers to exactly two, you need to type the following cmdlet:

   ```
   Reset-CsPoolRegistrarState-ResetType FullReset -PoolFqdn <PoolFqdn>
   ```

   If the pool has three or more servers, then at least three of those servers must be running when you type this cmdlet.
6. Restart all Front End Servers in the pool, one at a time.

1.7.3.8 Upgrade or Update a Back End Server or Standard Edition Server

Upgrade or Update a Back End Server or Standard Edition Server

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2012-11-01*

This topic explains how to install an update on an Enterprise Edition Back End Server or a Standard Edition server.

If a Back End Server is down for at least 30 minutes while you are upgrading it, users may then go into resiliency mode. When the upgrade is finished and the Back End Servers has again connected with the Front End Servers in the pool, users are returned to full functionality. If the upgrade takes less than 30 minutes, users will not be affected.

To update a back end server or Standard Edition server

1. Log on to the server you are upgrading as a member of the CsAdministrator role.
2. Download the update and extract it to the local hard disk.
3. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
4. Stop Lync Server services. At the command line, type:

   ```
   Stop-CsWindowsService
   ```

5. Stop the World Wide Web service. At the command line, type:

   ```
   net stop w3svc
   ```

6. Close all Lync Server Management Shell windows.
7. Install the update.
8. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
9. Stop Lync Server services again to catch Global Assembly Cache (GAC) –d assemblies. At the command line, type:

   ```
   Stop-CsWindowsService
   ```

10. Restart the World Wide Web service. At the command line, type:

    ```
    net start w3svc
    ```

11. Apply the changes made by LyncServerUpdateInstaller.exe to the SQL Server databases by doing one of the following:
    - If this is an Enterprise Edition Back End Server and there are no collocated databases on this server, such as Archiving or Monitoring databases, then type the following at a command line:

      ```
      Install-CsDatabase -Update -ConfiguredDatabases -SqlServerF
      ```

    - If this is an Enterprise Edition Back End Server and there are collocated databases on this server, then type the following at a command line:

      ```
      Install-CsDatabase -Update -ConfiguredDatabases -SqlServerF
      ```

    - If this is an Standard Edition server, type the following at a command line:

      ```
      Install-CsDatabase -Update -LocalDatabases
      ```

1.7.3.9 Managing Microsoft SIP Processing Language (MSPL) Applications

Managing Microsoft SIP Processing Language (MSPL) Applications

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2012-10-14*

You can use the procedures in this section to manage Microsoft SIP Processing Language (MSPL) Applications.

- View Microsoft SIP Processing Language (MSPL) Server Applications
- Mark a Microsoft SIP Processing Language (MSPL) Application as Critical or Not Critical
- Enable or Disable a Microsoft SIP Processing Language (MSPL) Server Application

1.7.3.9.1 View Microsoft SIP Processing Language (MSPL) Server Applications

View Microsoft SIP Processing Language (MSPL) Server Applications

See Also

Operations > Managing the Lync Server 2013 Topology > Managing Microsoft SIP Processing Language (MSPL) Applications >

Topic Last Modified: *2012-11-01*

A Microsoft SIP Processing Language (MSPL) server application is a script-only application that uses a scripting language instead of the Microsoft Lync 2010 API. MSPL provides more granular control over filtering and proxy behaviors, in addition to a facility for dispatching specific messages to transaction-based SIP applications. MSPL is used specifically for filtering and routing SIP messages. MSPL applications run in the same process as the UserServices module, while a program that is based on the Lync 2010 API runs in a separate process.

You can use the **Server Application** page in the **Topology** group of Lync Server Control Panel to see a list of MSPL server applications that run on Front End Servers in your Lync Server 2013 environment. The list shows the scripts that are available for each pool, as well as whether they are enabled or critical. The scripts run in the order they are listed.

These scripts include the following:

- ClientVersionFilter provides the administrator with a way to specify the version of clients that are supported by a pool. The client version filter checks the client version and can either prevent the client from logging on or present the user with a message that indicates he or she is using a client that is not supported. The client version filter can also be configured to display a message to the user that contains the URL of the latest downloadable version of the client.
- TranslationService translates a number that a user dials to an E.164 number according to the normalization rules defined by the administrator. For details, see Translation Rules.
- IncomingFederation enforces tenant-level federation validation for inter-tenant and incoming messages from external deployments.
- UserServices is the SIP Registrar, presence, and conferencing component of a Front End Server. It provides closely integrated IM, presence, and conferencing features built on top of the SIP Proxy.
- InterClusterRouting is responsible for routing calls to the callee’s primary Registrar pool. For details, see Front End Server VoIP Components.
- IIMFilter (Intelligent IM Filter) blocks messages that contain clickable URLs or that attempt to initiate file transfers. IIMFilter also checks the client version on behalf of the server. IIMFilter affects file transfers that are initiated by using either Lync Server, Communicator, or the Live Meeting 2007 client. By default, clickable links are disabled by adding an underscore character before the first character of the link. An administrator can change this behavior so that the link is blocked, in which case messages that contain clickable URLs or that attempt to initiate a file transfer are blocked by the server from reaching their intended destinations. IIMFilter is installed on all servers running Lync Server except Proxy Servers and Archiving Servers.
- UserPinService is used to verify user personal identification numbers (PINs) for dial-in conferencing.
- DefaultRouting is the default routing application for servers running Lync Server. It is enabled by default. The routing application is installed on all Standard Edition and Enterprise Edition servers.
- ExumRouting routes calls to Exchange Server Unified Messaging (UM). ExumRouting determines the appropriate Exchange UM server to route the call to when there is a new voice mail message to deposit. ExumRouting also handles some other Exchange UM integration aspects, including routing to Auto Attendant and Subscriber Access.
- OutboundRouting determines the gateway that routes a call to a phone number according to the dialed number and the user’s dialing authorization. OutboundRouting also handles rerouting of calls if a gateway cannot process a call.
- QoEAgent receives Quality of Experience (QoE) data reports from endpoints through SIP SERVICE requests, and sends the data to the destination queue on the Monitoring Server or to third-party consumers using HTTP POST. For details, see Deploying Monitoring.

- OutgoingFederation enforces tenant-level federation validation for messages going to a targeted external deployment.
- AcpRouting proxies INVITE requests destined for the audio conferencing provider to the audio conferencing provider gateway.

Scripts that run on Edge Servers include the following:

- IIMFilter
- OptionsHandler responds to incoming OPTIONS requests with **200 OK** if the request is destined for the current server. This is used for topology validation.

Tasks

Enable or Disable a Microsoft SIP Processing Language (MSPL) Server Application
Mark a Microsoft SIP Processing Language (MSPL) Application as Critical or Not Critical

1.7.3.9.2 Mark a Microsoft SIP Processing Language (MSPL) Application as Critical or Not Critical

Mark a Microsoft SIP Processing Language (MSPL) Application as Critical or Not Critical

See Also

Operations > Managing the Lync Server 2013 Topology > Managing Microsoft SIP Processing Language (MSPL) Applications >

Topic Last Modified: *2012-11-01*

Microsoft SIP Processing Language (MSPL) server applications are script-only applications that use the MSPL scripting language instead of the Microsoft Lync 2010 API. Some MSPL server applications are specified as critical. If a script is critical, the script must start during system startup in order for Lync Server 2013 to start. If the script fails while Lync Server is running, the server does not shut down, but it stops sending traffic to the script, and it writes errors in the event log.

You can use Lync Server Control Panel to mark Microsoft SIP Processing Language (MSPL) server applications as critical or unmark them.

Not all scripts support this option. For example, the DefaultRouting script is marked as critical, and this option cannot be changed for DefaultRouting.

⊟To mark or unmark an MSPL server application as critical

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and then click **Server Application**.
4. On the **Server Application** page, click a column heading to sort the applications, if needed, and then click the server application that you want to modify.
5. Click **Action**.
6. Click **Mark as critical** or **Unselect as critical** (that is, if the script supports this option).

Tasks

Enable or Disable a Microsoft SIP Processing Language (MSPL) Server Application

Concepts

View Microsoft SIP Processing Language (MSPL) Server Applications

Other Resources

Managing the Lync Server 2013 Topology

1.7.3.9.3 Enable or Disable a Microsoft SIP Processing Language (MSPL) Server Application

Enable or Disable a Microsoft SIP Processing Language (MSPL) Server Application

See Also

Operations > Managing the Lync Server 2013 Topology > Managing Microsoft SIP Processing Language (MSPL) Applications >

Topic Last Modified: *2012-09-21*

You can use Lync Server Control Panel to enable or disable Microsoft SIP Processing Language (MSPL) server applications that run in your Lync Server 2013 environment. These applications are script-only applications that use a scripting language instead of the Microsoft Lync 2013 Preview API.

Not all scripts can be enabled or disabled. For instance, the DefaultRouting script is enabled and this option cannot be changed for DefaultRouting.

⊟To enable or disable an MSPL server application

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and then click **Server Application**.
4. On the **Server Application** page, click a column heading to sort the applications, if needed, and then click the server application that you want to modify.
5. Click **Action**.
6. Click **Enable application** or **Disable application** (that is, if the script supports this option).

Tasks

Mark a Microsoft SIP Processing Language (MSPL) Application as Critical or Not Critical

Concepts

View Microsoft SIP Processing Language (MSPL) Server Applications

Other Resources

Managing the Lync Server 2013 Topology

1.7.3.10 Managing Simple URLs

Managing Simple URLs

See Also

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2012-10-11*

Use the procedures in this section to manage simple URLs from the **Topology** page in Lync

Server 2013 Control Panel.
View Simple URL Details

⊟See Also

Concepts

Planning for Simple URLs

1.7.3.10.1 View Simple URL Details

View Simple URL Details

See Also

Operations > Managing the Lync Server 2013 Topology > Managing Simple URLs >

Topic Last Modified: *2012-10-11*

You can use Lync Server 2013 Control Panel to view simple URL details for your Lync Server 2013 environment. Simple URLs make it easier for users to join meetings, and they make it easier for administrators to get to administrative tools. For details, see Planning for Simple URLs.

⊟To view Simple URL details

1. From a user account that is assigned to the CsServerAdministrator, CsAdministrator, CsHelpDesk, or CsViewOnlyAdministrator role, log on to any computer in your internal deployment. For details about the predefined administrative roles available in Lync Server 2013, see Planning for Role-Based Access Control.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and then click **Simple URL**.
4. On the **Simple URL** page, click a column heading to sort the list, if needed.
5. Select the name for which you want to see simple URL details, and then click **Properties**.
6. When you are finished viewing details, click **Close**.

Other Resources

Managing the Lync Server 2013 Topology

1.7.4 Delegating Administrative Control of Lync Server 2013

Delegating Administrative Control of Lync Server 2013

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2013-02-22*

In Lync Server 2013, administrative tasks are delegated to users by using the new role-based access control (RBAC) feature. When you install Lync Server, a number of RBAC roles are created for you. These roles correspond to universal security groups in Active Directory Domain Services (AD DS). For example, the RBAC role CsHelpDesk corresponds to the CsHelpDesk group found in the Users container in Active Directory Domain Services. In addition, each RBAC role is associated with a set of Lync Server Windows PowerShell cmdlets. These cmdlets represent the tasks that can be carried out by users who have been assigned the given RBAC role. For example, the CsHelpDesk role has been assigned the Lock-CsClientPin and UnlockCsClientPin cmdlets. That means users who have been assigned the CsHelpDesk role can lock and unlock user PIN numbers. However, the CsHelpDesk role has not been assigned the New-CsVoicePolicy cmdlet. That means that users who have been assigned the CsHelpDesk role cannot create new voice policies.

Viewing Information about RBAC Roles

You can retrieve basic information about your RBAC roles by running the following command from within the Lync Server Management Shell:

```
Get-CsAdminRole
```

Keep in mind that the Identity of the RBAC role (for example, CsVoiceAdministrator) has a direct mapping to a security group found in the Users container in Active Directory Domain Services.

To view a list of the cmdlets that have been assigned to a role, use a command similar to this:

```
Get-CsAdminRole -Identity "CsHelpDesk" | Select-Object -ExpandProperty Cmdlets
```

Assigning an RBAC Role to a User

To assign an RBAC role to a user, you must add that user to the appropriate Active Directory security group. For example, to assign the CsLocationAdministrator role to a user, you must add that user to the CsLocationAdministrator group. That can be done by carrying out the following procedure:

To assign a user to a security group

1. Using an account that has permission to modify the membership of an Active Directory group, log on to a computer where Active Directory Users and Computers has been installed.
2. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In Active Directory Users and Computers, expand the name of your domain and click the **Users** container.
4. Right-click the security group **CsLocationAdministrator**, and then click **Properties**.
5. In the **Properties** dialog box, on the **Members** tab, click **Add**.
6. In the **Select Users, Computers, Contacts, or Groups** dialog box, type the user name or display name of the user to be added to the group (for example, **Ken Myer**) in the **Enter the object names to select** box and then click **OK**.
7. In the **Properties** dialog box, click **OK**.

To verify that the RBAC role has been assigned, use the Get-CsAdminRoleAssignment cmdlet, passing the cmdlet the SamAccountName (Active Directory logon name) of the user. For example, run this command from within the Lync Server Management Shell:

```
Get-CsAdminRoleAssignment  -Identity "kenmyer"
```

1.7.5 Managing IM and Presence Settings

Managing IM and Presence Settings

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-10-14*

Topics in this section provide step-by-step procedures for tasks that you can perform using the **IM and Presence** group in Lync Server 2013 Control Panel.

- Configuring File Transfer and URL Filtering for Instant Messaging (IM)
- Assigning Per-User Presence Policies

1.7.5.1 Configuring File Transfer and URL Filtering for Instant Messaging (IM)

Configuring File Transfer and URL Filtering for Instant Messaging (IM)

See Also

Microsoft Lync Server 2013 > Operations > Managing IM and Presence Settings >

Topic Last Modified: *2012-11-01*

The Intelligent IM Filter tool helps protect your Lync Server 2013 deployment against the spread of the most common forms of viruses with minimal degradation to the user experience. Use Intelligent IM Filter to configure filters to block unsolicited or potentially harmful instant messages from unknown endpoints outside the corporate firewall. You configure filters by specifying the criteria to be used to determine what should be blocked, such as instant messages containing hyperlinks with specific prefixes and files with specific extensions.

Intelligent IM Filter provides the following:

- Enhanced URL filtering.
- Enhanced file transfer filtering.

Configuring Intelligent IM Filter includes the following:

- Configuring URL filtering.
- Configuring file transfer filtering.

How Filtering Options Are Applied to Instant Messages

Before you deploy the Intelligent IM Message Filter tool, you need to understand how filtering options are applied as messages are routed from one Lync Server 2013 server to another. The way these filtering options are applied is consistent, regardless of whether the servers are located in a single organization or across organizational boundaries. This consistency applies to the way that the customized notice and warning texts are inserted into messages and sent across servers.

Note:

The instant message filter increases the amount of CPU resources required to process URLs in a message. This increase in CPU demand also affects the performance of Lync Server.

By using the **URL Filter** page in the **IM and Presence** group in Lync Server Control Panel, you can block some or all hyperlinks or configure a warning. The warning is inserted at the beginning of an instant message that contains a hyperlink when you choose the **Hyperlink prefix** option **Send warning message**.

When an instant message travels from one server to another, the following general guidelines apply:

- If a server blocks an instant message (because you selected the **Block URLs with file extension** check box on the **URL Filter** page or because you chose

the **Hyperlink prefix** option **Block hyperlinks**), an error message is returned to the client. Subsequent servers do not receive this instant message.
- If a server (Server1) adds a warning to an instant message that contains an active hyperlink, a subsequent server (Server2) that receives this instant message can still take a different action based on this active hyperlink present in the instant message and block the instant message or add a warning. If Server2 is configured only to add a warning for this URL, the earlier warning added by Server1 is removed, and the warning configured on Server2 is added to the beginning of the instant message.

Note:

If you are running Lync Server 2013 in a mixed environment, Live Communications Server 2005 with SP1 is the minimum version required to use the Intelligent IM Filter application. The Intelligent IM Filter is not supported on Live Communications Server 2005 without SP1.

URL Filtering

URLs are filtered according to their hyperlink prefix. The following examples are valid prefixes:

- www*.
- ftp.
- http:

If you do not configure the instant message filter to perform any URL filtering, all URLs contained in instant messages are passed unmodified through the server. If you configure the instant message filter to perform URL filtering, URLs in instant messages are filtered according to the options that you select in the **Edit URL Filter** or **New URL Filter** dialog box.

- **Enable URL filter** This option enables URL filtering for the global deployment or for the site that you select.
- **Block URLs with file extension** The instant message filter blocks any active intranet or Internet URL that contains a file with an extension listed under **File type extensions to block** in the **Edit File Filter** dialog box. When a URL is blocked, an error message is displayed to the sender. When selected, this option takes precedence over all other filtering options for any file extensions defined under **File type extensions to block**.

  Important:

  Filtering of file extensions is limited to standard file names. Filtering may not work with file extensions embedded in other names.

To configure how hyperlinks are handled in instant message conversations, select one of the following options under **Hyperlink prefix**:

- **Do not filter** URLs in messages are sent through the server. When you choose this option, the **Allow message** box appears. In the **Allow message** box, specify the notice that you want to insert at the beginning of each instant message containing hyperlinks. This notice can consist of no more than 65535 characters.
- **Block hyperlinks** Delivery of instant messages containing active hyperlinks is blocked by Lync Server, and an error message is displayed to the sender.
- **Send warning message** Lync Server permits active hyperlinks in instant messages, but it includes a warning. When you choose this option, the **Warning message** box appears. In the **Warning message** box, you must type the warning that you want to include with instant messages containing valid hyperlinks. For example, this warning might state the potential dangers of clicking an unknown link, or it might refer to your organization’s relevant policies and requirements. The warning can be no more than 65535 characters.

If you select **Block hyperlinks** or **Send warning message**, the following options are available:

- **Exclude local intranet hyperlinks** The instant message filter blocks only Internet URLs. URLs for locations within your intranet are passed unmodified through the server. However, the intranet URLs that individual servers running Lync Server pass depend on which types of local websites are considered part of their intranet zone. To check a server's intranet zone settings, see the "To configure your intranet settings in Internet Explorer" procedure in Modify the Default URL Filter.
- **Filter these hyperlink prefixes** To choose which prefixes you want to block, click **Select**, and then, in **Select Hyperlink Prefix**, add the prefixes to the **Hyperlink prefixes** list.
  All prefixes except **href** must end with a period or a colon, or an asterisk followed by a period. Valid prefixes can contain any characters in the set of valid URL characters except the asterisk (*). The set of valid URL characters is:
  #*+/0123456789=@ABCDEFGHIJKLMNOPQRSTUVWXYZ^_`
  abcdefghijklmnopqrstuvwxyz|~

File Transfer Filtering

Filter transfer filtering affects both instant messages and conferences. For conferences, these settings affect the handout feature in the Office Live Meeting 2007 client and multimedia playback features.

Note:

Lync Server also offers file transfer setting options. This server-side option is offered in addition to the client-side controls available in Lync Server.

You can filter file transfers during instant message conversations, when you are using the handout feature in the Office Live Meeting 2007 client, and for multimedia playback features for all file types. You can set the following options to control file transfers:

- **Enable file filter** This option enables file filtering for the global deployment or for the site that you select.
  When you enable the file filter, you can choose one of the following options in **File transfer**:
  - **Block specific file types** You specify which file transfer requests are filtered by the server by specifying a list of file extensions to block. Entries in the list can contain all standard characters, but not the wildcard character (*). In the Office Live Meeting 2007 client the handout feature is enabled, but any file with this extension cannot be uploaded or downloaded. If you select the **Block URLs with file extension** check box on the settings for a URL filter listed on the **URL Filter** tab, the URL filter uses this same list to block active hyperlinks that contain any of these file extensions. To choose which file types you want to block, click **Select**, and then, in **Select File Type**, add the file type extensions to the **Selected file type extensions** list.
  - **Block All** The server drops all instant messages that contain file transfer requests and returns an error message to the sender of the request. The handout feature in the Office Live Meeting 2007 client is disabled.

Important:

Filtering of file extensions is limited to standard file names. Filtering may not work with file extensions embedded in other names.

In This Section

- Modify the Default File Transfer Filter
- Create a New File Transfer Filter for a Specific Site
- Modify the Default URL Filter
- Create a New URL Filter to Handle Hyperlinks in IM Conversations

⊟See Also

Other Resources

Managing IM and Presence Settings

1.7.5.1.1 Modify the Default File Transfer Filter

Modify the Default File Transfer Filter

See Also

Operations > Managing IM and Presence Settings > Configuring File Transfer and URL Filtering for Instant Messaging (IM) >

Topic Last Modified: *2012-11-01*

Lync Server 2013 provides a global file transfer filter that blocks specific types of files during the following file-related activities within your Lync Server 2013 deployment:

- File transfer requests during instant messaging (IM) conversations
- File uploads and downloads while using the handout feature in the Office Live Meeting 2007 client
- Multimedia playback during conferences

Depending on the types of files you want to block or allow, you can use Lync Server Control Panel to modify the global filter. For details about file transfer filtering, see Configuring File Transfer and URL Filtering for Instant Messaging (IM).

⊟To modify the default file transfer filter

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **IM and Presence** and then click **File Filter**.
4. On the **File Filter** page, double-click the **Global** filter.
5. In **Edit File Filter**, select the **Enable file filter** check box.
6. In the **File transfer** drop-down list box, click **Block All** or **Block specific file types**.
7. If you clicked **Block All**, skip to step 9.
8. If you clicked **Block specific file types**, do the following:
   - 8.a. Click **Select** to modify the default list of file type extensions that you want to block.
   - 8.b. In **Select File Type**, select the file types that you want to block or allow by adding or removing their extensions from the categories under **File type extensions**.
   - 8.c. If you do not see the extension for a file type that you want to block, type the extension in the text box under **Add file type extensions to the list**, and then click **Add**.
   - 8.d. Click **OK**.
9. Click **Commit**.

Tasks

Configuring File Transfer and URL Filtering for Instant Messaging (IM)
Create a New File Transfer Filter for a Specific Site
Create a New URL Filter to Handle Hyperlinks in IM Conversations

Concepts

Modify the Default URL Filter

1.7.5.1.2 Create a New File Transfer Filter for a Specific Site

Create a New File Transfer Filter for a Specific Site

See Also

Operations > Managing IM and Presence Settings > Configuring File Transfer and URL Filtering for Instant Messaging (IM) >

Topic Last Modified: *2012-10-18*

In addition to modifying the global file transfer filter, you can configure custom file transfer filters for specific sites within your Lync Server 2013 deployment. For details about file transfer filtering, see Configuring File Transfer and URL Filtering for Instant Messaging (IM).

⊟To create a file transfer filter for a specific site

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **IM and Presence** and then click **File Filter**.
4. On the **File Filter** page, click **New**.
5. In the **Select a Site** dialog box, click the site for which you want to create the file transfer filter, and then click **OK**.
6. In **New File Filter**, click the **Enable file filter** check box.
7. In **File transfer** drop-down list box, click **Block All** or **Block specific file types**.
8. If you clicked **Block All**, skip to step 10.
9. If you clicked **Block specific file types**, do the following:
   - 9.a.Click **Select** to modify the default list of file type extensions that you want to block.
   - 9.b.In the **Select File Type** dialog box, select the file types that you want to block or allow by adding or removing their extensions from the categories under **File type extensions**.
   - 9.c.If you do not see the extension for a file type that you want to block, type the extension in the text box under **Add file type extensions to the list**, and then click **Add**.
   - 9.d.Click **OK**.
10. Click **Commit**.

Tasks

Configuring File Transfer and URL Filtering for Instant Messaging (IM)
Create a New URL Filter to Handle Hyperlinks in IM Conversations
Modify the Default File Transfer Filter

Concepts

Modify the Default URL Filter

1.7.5.1.3 Modify the Default URL Filter

Modify the Default URL Filter

See Also

Operations > Managing IM and Presence Settings > Configuring File Transfer and URL Filtering for Instant Messaging (IM) >

Topic Last Modified: *2012-06-26*

By using the instant messaging (IM) filter, Lync Server 2013 provides a global URL filter that blocks specific URLs contained in IM conversations among users throughout your Lync Server 2013 deployment. By using Lync Server Control Panel, you can do the following:

- Block all or a subset of URLs in instant message conversations.
- Allow all URLs. As an option, you can create a notice that is inserted at the beginning of each instant message that contains a URL.
- Allow specific URLs and include a warning with each instant message that contains a URL.

In addition, you can choose to block URLs that contain specific file types, or block only Internet URLs by allowing URLs that are within the server's local intranet zone — intranet URLs — to pass through the server. For details about URL filtering, see Configuring File Transfer and URL Filtering for Instant Messaging (IM).

Tasks

Configuring File Transfer and URL Filtering for Instant Messaging (IM)
Create a New File Transfer Filter for a Specific Site
Create a New URL Filter to Handle Hyperlinks in IM Conversations
Modify the Default File Transfer Filter

1.7.5.1.4 Create a New URL Filter to Handle Hyperlinks in IM Conversations

Create a New URL Filter to Handle Hyperlinks in IM Conversations

See Also

Operations > Managing IM and Presence Settings > Configuring File Transfer and URL Filtering for Instant Messaging (IM) >

Topic Last Modified: *2012-09-26*

In addition to modifying the global URL filter, you can configure custom URL filters for individual sites within your Lync Server 2013 deployment. For details about URL filtering, see Configuring File Transfer and URL Filtering for Instant Messaging (IM).

⊟To create a new URL filter

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **IM and Presence**, and then click **URL Filter**.
4. On the **URL Filter** page, click **New**.
5. In **Select a Site**, click the site for which you want to create the URL filter, and then click **OK**.
6. In the **New URL Filter** dialog box, select the **Enable URL Filter** check box to enable URL filtering for the site.
7. To block any active URL that contains a file with an extension listed under **File type extensions to block** in **Edit File Filter**, select the **Block URLs with file extension** check box.
8. In the **Hyperlink prefix** drop-down list box, click the option that corresponds to how you want to handle URLs in instant message conversations.

   The **Allow message** box enables a warning message to be sent to the user when sending hyperlinks that are allowed to be sent.
9. Click **Commit**.

Tasks

Configuring File Transfer and URL Filtering for Instant Messaging (IM)
Create a New File Transfer Filter for a Specific Site
Modify the Default File Transfer Filter

Concepts

Modify the Default URL Filter

1.7.5.2 Assigning Per-User Presence Policies

Assigning Per-User Presence Policies

Microsoft Lync Server 2013 > Operations > Managing IM and Presence Settings >

Topic Last Modified: *2012-10-11*

A presence policy is a set of limits and restrictions that affect presence. The following table describes the presence policy settings available in Lync Server 2013.

Presence Policy Settings

XML name	Display name	Description	Type	Value
CategorySubscriptions	Maximum Number of Subscriber Category Subscriptions	Limits the number of subscriber category subscriptions. For example, when Communicator subscribes to a user’s presence, it obtains a category subscription for each of the contact card, calendar data, notes, services, and state categories. A setting of 0 means that the user or contact object cannot be subscribed to by others. **Note:** This setting can have a significant impact on performance if it is set to a high number, and the average user has a large number of users subscribing to his or her presence.	Integer	0-3000
PromptedSubscribers	Maximum Number of	Limits the number of entries in the prompted	Integer or Token	0-500

	Queued Presence Subscription Alerts	subscribers table. This setting determines the maximum number of prompts that can be queued for a given user. For example, when user A subscribes to user B's presence, user B receives a prompt that user A is now subscribed to user B, and an acknowledgement prompt is created in user B's prompted subscribers table. After user B accepts, or acknowledges, the subscription, the acknowledgement prompt is removed from user B's prompted subscribers table. A setting of 0 means that the user is not prompted when someone subscribes to his or her presence.		

By default, the **Default Policy** and **Service: Medium** presence policies are installed when you deploy Lync Server. The following table describes the specific settings of the two presence policies.

Presence Policies

Policy name	Description	CategorySubscriptions	PromptedSubscribers
Default Policy	Policy for typical users. This is the default presence policy.	1000	200
Service: Medium	Policy for applications that require more users to subscribe to the object's presence.	1000	0

1.7.6 Managing Lync Server 2013, Persistent Chat Server

Managing Lync Server 2013, Persistent Chat Server

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-10-11*

You can use Lync Server 2013, Persistent Chat Server to enable multiple users to participate in conversations in which they post and access content about specific topics, including text, links, and files. Although users can communicate in real time during a session, the content of each session is persistent, which means that it continues to be available after a session ends.

The content of Persistent Chat rooms consists primarily of short text messages, although it can include longer messages, referred to as *stories*, and also hyperlinks, emoticons, and uploaded documents.

Note:

File upload and download is not supported by the Lync 2013 client; however, it is still supported by Lync Server 2013, Persistent Chat Server. The legacy Group Chat client can post and view files, but if the same chat room is accessed via the Lync 2013 client, it will not be able to access the files.

Access to a chat room is controlled by a membership list. The entire chat room history is available to any member for chronological review or full-text search. For details about using the Persistent Chat client, see Planning for Clients in the Planning documentation, and Deploying Clients and Devices in the Deployment documentation.

When you set up Persistent Chat Server for your organization, you specify the initial configuration during deployment. However, there may be times when you want to change how you implement Persistent Chat Server support. For example, you may need to set up Persistent Chat Server support and controls differently for a specific team or group within your organization. This section provides information and procedures to help you customize your Persistent Chat Server deployment. For details about the features and functionality that you can configure for Persistent Chat Server, see Defining Your Organization's Requirements for Persistent Chat Server in the Planning documentation, and How Persistent Chat Server Works in the Planning documentation, Deployment documentation, or Operations documentation. For details about deploying Persistent Chat Server for Lync Server 2013, see Deploying Persistent Chat Server in the Deployment documentation.

- How Persistent Chat Server Works
- Using Categories to Administer Persistent Chat Server
- Understanding Persistent Chat Membership
- Persistent Chat Server Best Practices
- Managing Categories, Rooms, and Add-Ins
- Managing Persistent Chat User Access
- Operating and Maintaining the Persistent Chat System

1.7.6.1 How Persistent Chat Server Works

How Persistent Chat Server Works

Microsoft Lync Server 2013 > Planning > Planning for Persistent Chat Server >

Topic Last Modified: *2012-11-21*

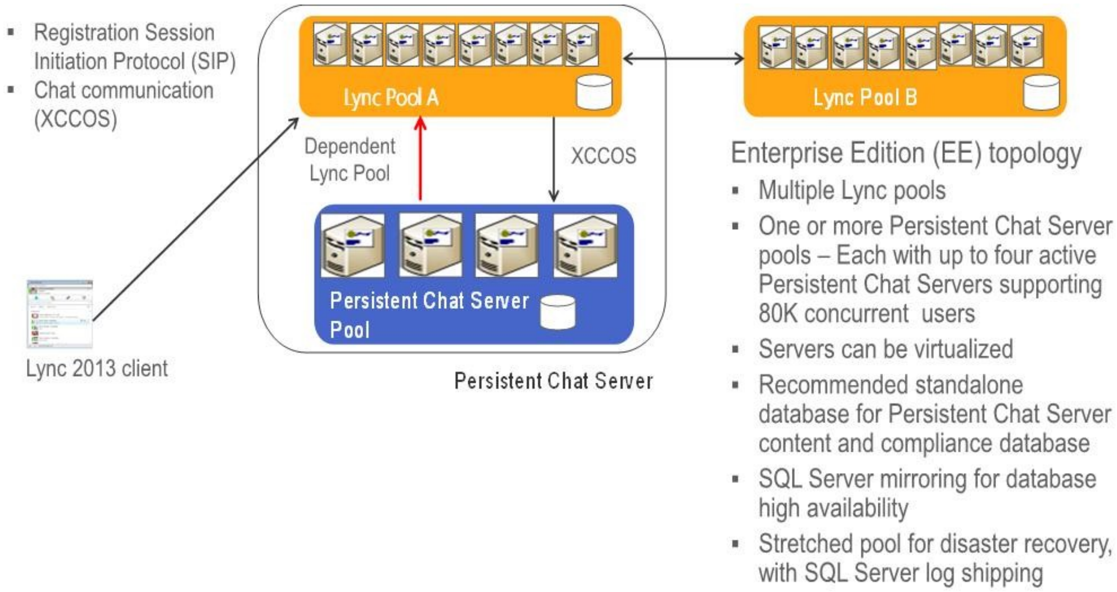
Lync Server 2013, Persistent Chat Server enables you to participate in multiparty, topic-based conversations that persist over time. Persistent Chat Server can help your organization do the following:

- Improve communication between geographically dispersed and cross-functional teams
- Broaden information awareness and participation
- Improve communication with your extended organization
- Reduce information overload
- Improve information awareness
- Increase dispersion of important knowledge and information

You can deploy Persistent Chat Server as an optional role with Lync Server 2013. Persistent Chat services run on a dedicated pool, and a Persistent Chat Server pool depends on a Lync Server pool to route messages to it. Clients use eXtensible Chat Communication Over SIP (XCCOS). The Lync Server Front End Servers are configured to route the traffic to a Persistent Chat Server pool.

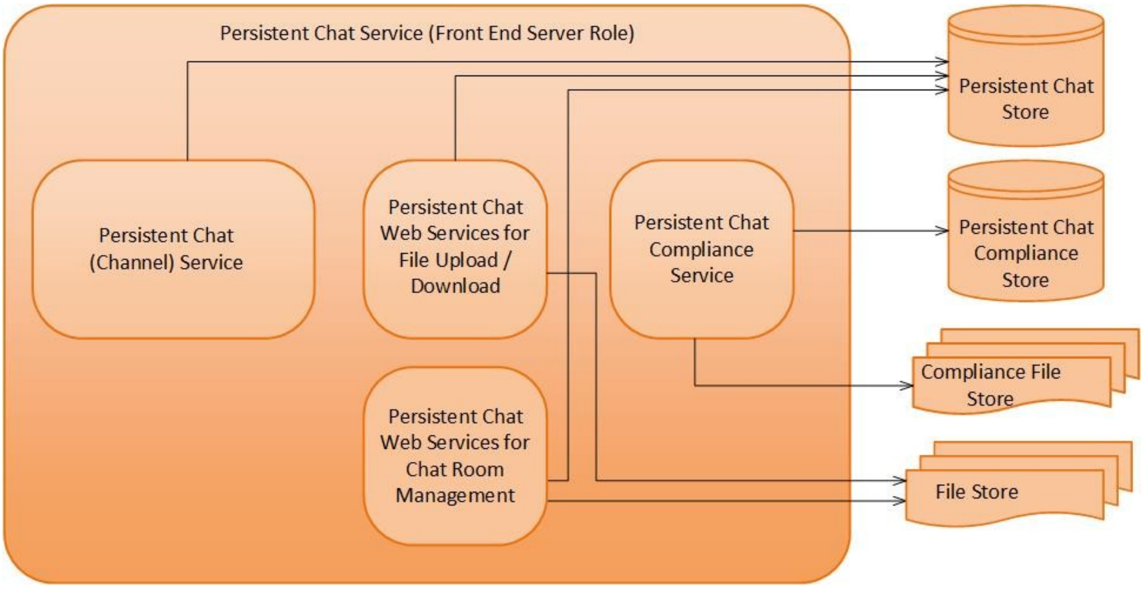
High-Level Architecture

The following diagrams provide high-level perspectives of the Persistent Chat Server architecture and services.


Registration Session Initiation Protocol (SIP)
Chat communication (XCCOS)
Lync Pool A
Lync Pool B
Dependent Lync Pool
XCCOS
Persistent Chat Server Pool
Lync 2013 client
Persistent Chat Server

Enterprise Edition (EE) topology

- Multiple Lync pools
- One or more Persistent Chat Server pools – Each with up to four active Persistent Chat Servers supporting 80K concurrent users
- Servers can be virtualized
- Recommended standalone database for Persistent Chat Server content and compliance database
- SQL Server mirroring for database high availability
- Stretched pool for disaster recovery, with SQL Server log shipping


Persistent Chat Service (Front End Server Role)
Persistent Chat (Channel) Service
Persistent Chat Web Services for File Upload / Download
Persistent Chat Compliance Service
Persistent Chat Web Services for Chat Room Management
Persistent Chat Store
Persistent Chat Compliance Store
Compliance File Store
File Store

Two services run on the Persistent Chat Server Front End Servers:

- Persistent Chat (Channel)
- Compliance

Persistent Chat (Channel) Service

The Persistent Chat (Channel) service is the core service responsible for Persistent Chat Server. This service provides the following functions:

- Accepts incoming messages
- Registers and lists online participants within a Persistent Chat room
- Retransmits messages to other channel subscribers
- Implements logic for channel management, chat room invitation, search, and new content notifications

The Persistent Chat (Channel) service stores and accesses chat room content and other system metadata (authorization rules, and so on) by using the Persistent Chat Store. This service stores files that are uploaded into chat rooms in the Persistent Chat File Store.

Compliance Service

The Compliance service is an optional component of Persistent Chat Server and is responsible for archiving chat content and events to the Persistent Chat Compliance Store. If your organization has regulations that require Persistent Chat activity to be archived, you can deploy the optional Persistent Chat Compliance service. The Compliance service is installed on each Persistent Chat Server in a Persistent Chat pool. When configured, Persistent Chat Server compliance records user activity such as joining and leaving rooms, and posting and reading of messages. The Compliance service stores files that need to be archived in the Persistent Chat Compliance File Store.

Persistent Chat Web Services

On the Lync Server Front End Servers, two services run that depend on Internet Information Services (IIS), and are implemented as web components:

- **Persistent Chat Web Services for File Upload/Download** Responsible for posting and retrieving files from chat rooms.
- **Persistent Chat Web Services for Chat Room Management** Responsible for providing users the ability to manage their chat rooms, and create new chat rooms.

How Do I Start Using Persistent Chat Server?

Persistent Chat Server is an optional server role within the Lync Server 2013 infrastructure. If you install the Persistent Chat Server role, any users who have been enabled through policy by an administrator can use Persistent Chat with the Lync 2013 client.

For details about how to deploy Persistent Chat Server and enable users to leverage the capabilities by policy, see Deploying Persistent Chat Server.

For details about how to configure settings on your Persistent Chat Server deployment, see Deploying Persistent Chat Server and Managing Lync Server 2013, Persistent Chat Server.

For details about how to enable users by policy such that they can leverage Persistent Chat functionality in Lync 2013 client, see Deploying Persistent Chat Server and Managing Lync Server 2013, Persistent Chat Server.

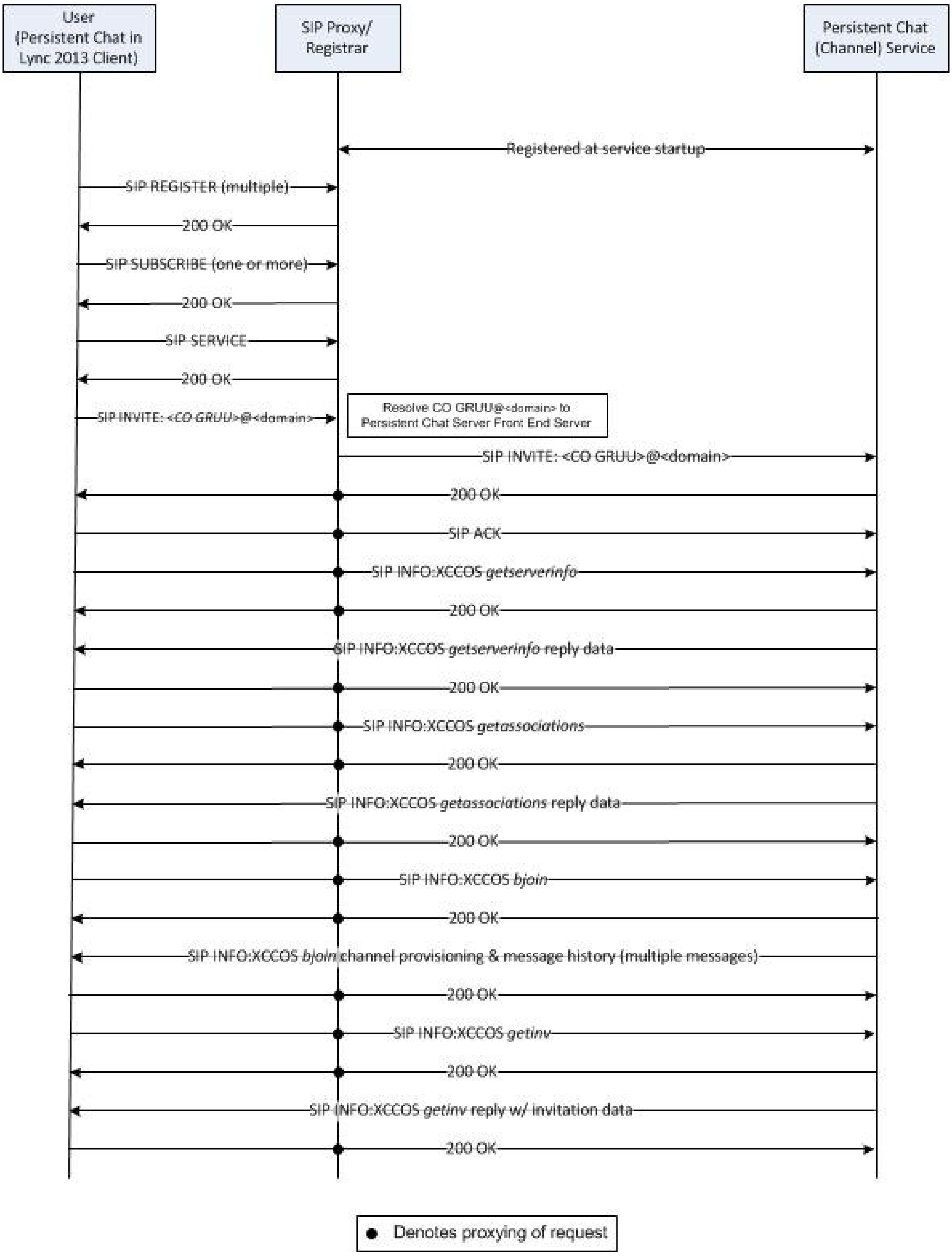
If you deployed Persistent Chat compliance, see Managing Lync Server 2013, Persistent Chat Server for details about how to configure settings for compliance.

Persistent Chat Call Flows

The Persistent Chat client communicates with the Persistent Chat service by using XCCOS. The following sequences describe the sign-in process and a typical room subscription and message post scenario.

Sign-in

The following call flow diagram and steps describe the sign-in process.


User (Persistent Chat in Lync 2013 Client)
SIP Proxy/ Registrar
Persistent Chat (Channel) Service
Registered at service startup
SIP REGISTER (multiple)
200 OK
SIP SUBSCRIBE (one or more)
200 OK
SIP SERVICE
200 OK
SIP INVITE: <CO GRUU>@<domain>
Resolve CO GRUU@<domain> to Persistent Chat Server Front End Server
SIP INVITE: <CO GRUU>@<domain>
200 OK
SIP ACK
SIP INFO:XCCOS getserverinfo
200 OK
SIP INFO:XCCOS getserverinfo reply data
200 OK
SIP INFO:XCCOS getassociations
200 OK
SIP INFO:XCCOS getassociations reply data
200 OK
SIP INFO:XCCOS bjoin
200 OK
SIP INFO:XCCOS bjoin channel provisioning & message history (multiple messages)
200 OK
SIP INFO:XCCOS getinv
200 OK
SIP INFO:XCCOS getinv reply w/ invitation data
200 OK
● Denotes proxying of request

1. The Persistent Chat client first sends a SIP SUBSCRIBE to retrieve the in-band provisioning document from the server. This document indicates if Persistent Chat is enabled or disabled for the user and the list of SIP URIs for the Persistent Chat Server pool.
2. The Persistent Chat client sends a SIP INVITE message to the SIP URI of the Persistent Chat Server that it obtained in the previous step. The INVITE sequence is followed by 200 OK and ACK, and the Persistent Chat client has

now opened a SIP session with a Persistent Chat Server endpoint. Consequently, the Persistent Chat client communicates with Persistent Chat Server by sending SIP INFO messages that contain either chat messages or commands requesting the server to take an action. All of these messages are acknowledged with either 200 OK or 503 Service Unavailable (that is, in the event of heavy server load). If the client receives a 503 response, it will retry the message. (This example does not include a 503 response.) If the server accepts the message or command and sends 200 OK, it provides a response to the client in the form of a separate SIP INFO message. This response includes a reference to the originating command.

3. The Persistent Chat client sends a SIP INFO message that contains the XCCOS **getserverinfo** command. Persistent Chat Server replies with a new SIP INFO message that contains information about the Persistent Chat service configuration.
4. The Persistent Chat client sends a SIP INFO message that contains the XCCOS **getassociations** command. Persistent Chat Server replies with a new SIP INFO message that contains the list of rooms of which the user is a member. The Persistent Chat client repeats the command to retrieve the list of rooms of which the user is a manager.
5. The Persistent Chat client gets the list of followed rooms from the "presence" document, where each followed room is represented by a "roomSetting" category. All followed rooms are joined by a single SIP INFO message that contains the XCCOS **bjoin** command that contains the list of room URIs. Because the list of followed rooms is kept on the server, any client on any computer has the same list of followed rooms for the specified user URI. The Persistent Chat client also keeps the list of opened rooms (if this option is enabled by the user) in the local computer registry, and joins each of these rooms at sign-in by sending a SIP INFO message that contains the XCCOS **join** command for each opened room. Because this list is kept in the registry, it can be different on two Persistent Chat clients running on different computers.
6. For each room joined, the Persistent Chat client sends a SIP INFO message that contains the XCCOS **bccontext** command. Persistent Chat Server replies with a new SIP INFO message that contains the most recent chat message in the room.
7. The Persistent Chat client sends a SIP INFO message that contains a XCCOS **getinv** (that is, get invitation) command to request any new room invitations that the client has not yet seen. In a separate SIP INFO message, Persistent Chat Server returns a list of those rooms.

Subscribe to a Room and Post a Message

The following call flow diagram and steps describe a typical room subscription and message post scenario.

1. From the Persistent Chat client, User1 clicks **Join a Chat Room**, clicks **Search**, and then enters some search criteria. The Persistent Chat client sends a SIP INFO message that contains the XCCOS **chansrch** (room search) command, along with the search criteria. Persistent Chat Server queries the back-end database and replies in a new SIP INFO message that contains a list of available rooms that meet the search criteria.
2. User1 selects the chat room that he or she wants to join, and then clicks **Follow this room**. The Persistent Chat client sends Persistent Chat Server a SIP INFO message that contains the XCCOS **join** command and the room ID of the chat room that the user selected. Persistent Chat Server replies with a SIP INFO message that contains the provisioning data.
3. The Persistent Chat client sends Persistent Chat Server a SIP INFO message that contains the XCCOS **bccontext** (backchat context) command. Persistent Chat Server retrieves the chat history, and returns it to the Persistent Chat client in a separate SIP INFO message. At this point, the user enters the chat

room and is ready to participate.

4. User1 enters a new message, and then clicks **Send**. The Persistent Chat client posts the message to the chat room in a SIP INFO XCCOS **grpchat** command. Persistent Chat Server stores a copy of this new message in the Persistent Chat back-end database.
5. Persistent Chat Server sends a separate copy of the SIP INFO XCCOS **grpchat** message to User2, who has already entered the chat room.

Persistent Chat Compliance Call Flows

Persistent Chat Server uses Message Queuing (also known as MSMQ) and an additional compliance database (mgccomp) to process compliance data. As an example of how compliance events are processed, the following sequence of events describes how a message post event is processed.

1. A user posts a message to a room.
2. Persistent Chat Server places information pertaining to the event in a private Message Queuing queue.
3. Persistent Chat Compliance server reads this event from the queue, and places it into the mgccomp database for processing later.
4. Periodically, the Persistent Chat Compliance server processes a set of events in the database, and sends them to the Persistent Chat Compliance adapter for processing.
5. If the adapter successfully processes the data, Persistent Chat Compliance server deletes the events from the mgccomp database.

1.7.6.2 Using Categories to Administer Persistent Chat Server

Using Categories to Administer Persistent Chat Server

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013, Persistent Chat Server >

Topic Last Modified: *2012-10-18*

Your Persistent Chat Server deployment can host many concurrent Persistent Chat rooms. Chat rooms can be organized into a set of categories on the server. Each chat room belongs to one category, and inherits some settings from that category. This organization creates a useful structure for identifying conversations, based on their business purpose, and facilitates delegated administration and simplified management.

Note:

Although many of the management features of chat rooms are available in computers running Persistent Chat (Lync client) for the user, Persistent Chat Administrators (in the **cspersistentchatadministrator** role) must use the Lync Server Control Panel or Windows PowerShell cmdlets to create or manage categories.

Persistent Chat administrators use Lync Server Control Panel or Windows PowerShell cmdlets to create and manage categories, and to design access for chat rooms for the users in their organization.

Persistent Chat room managers, who have the ability to manage one or more chat rooms, can use the Lync client to launch a room management Web application to create and manage rooms (or customers can create custom solutions and workflows to be invoked). Persistent Chat administrators can also use Lync Server Control Panel or Windows PowerShell cmdlets to create and manage rooms.

Chat room managers can make changes to all chat room properties, except for changing the category of the room. They cannot be restricted from performing the following actions:

- Disabling a chat room

- Changing a chat room name
- Changing a chat room description
- Changing a chat room type (Auditorium versus Normal)
- Changing the privacy of a room (open versus closed versus secret)
- Adding or removing members
- Adding or removing chat room managers
- Adding or removing an add-in
- Changing settings such as invitations (according to what's permitted by the category)

Delegated Administration

Creating and managing Persistent Chat rooms is much easier with the correct use of categories. A Persistent Chat Administrator can define **AllowedMembers** and **Creators** for each category, and can also define the default chat room settings and behaviors that will be applied to all chat rooms created in the category. Persistent Chat administrators create and manage categories by using Lync Server Control Panel or Windows PowerShell cmdlets.

Users, Organizational Units (OUs), and user groups that are identified as Creators of the category are the only individuals and groups that are allowed to create rooms in the category. After the category is created, they can choose users, OUs, and user groups from the category's **AllowedMembers** list as chat room managers and members to manage and participate in the room.

Chat rooms that are created in a category adhere to the policies and settings enforced by the category (such as who can be in the room's membership, who can manage the room, whether file uploads are allowed, whether invitations are sent, and so on).

1.7.6.3 Understanding Persistent Chat Membership

Understanding Persistent Chat Membership

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013, Persistent Chat Server >

Topic Last Modified: *2013-02-22*

User access to Persistent Chat rooms is managed by membership; users must be members of a chat room to be able to post and read messages. Only **Presenters** who have a designated affiliation with chat rooms are allowed to use **Posting to Auditorium rooms**. An auditorium is a type of chat room (the other is **Normal**), where only Presenters can post and everyone can read.

In addition, Persistent Chat rooms operate under the rules of a category. For details about categories, see Managing Categories, Rooms, and Add-Ins, and also the sections "How Category Scoping Works" and "Room Category Strategies" later in this topic.

A Persistent Chat administrator can create and manage chat room categories. As part of creating and managing chat room categories, the Persistent Chat administrator can configure principals (Active Directory Domain Services (AD DS) groups, containers, and users) that have access to be members or creators of chat rooms of a particular category.

Active Directory Domain Services and Persistent Chat

Persistent Chat Server relies on Active Directory for the pool of internal Persistent Chat users. After you install Persistent Chat (client), you can add domains of users and user groups to the room category. You can then add these users and groups to the membership of your room categories.

Important:

You must ensure that there are no duplicate names for users who want to make changes to their Persistent Chat room(s). If duplicate user names exist, change them to different names to unblock users from making those changes. If a user has duplicate names in Active Directory and tries to make changes in their room(s), an error message appears prompting the user to contact the administrator for resolution.

How Category Scoping Works

A category specifies all the users and groups that can be members in a membership list of a Persistent Chat room in that category, based on its **AllowedMembers** property. For example, if you set the category's **AllowedMembers** to contoso.com, you can add any group or user at *Contoso* as a member to chat rooms in that category. If you set the **AllowedMembers** on a category to *Sales*, only groups and users in this distribution list can be added as members to chat rooms in that category. Similarly, the **Creators** property enables you to control who can create chat rooms in that category. After the chat room is created, anyone from the **AllowedMembers** group can be designated as a **Manager** for ongoing management operations on the rooms (for example, membership changes and approvals).

Defining **AllowedMembers** and **Creators** for a category has the following benefits:

- All chat rooms in this category are bound by the restrictions set at the category level. You can use this to segregate chat rooms based on business need and access policies.
- A user who is in the **Creators** list can create new chat rooms in that category. If you want to implement a system where a restricted number of personnel in the organization can create chat rooms, this control can be used to meet that requirement.

Room Category Strategies

A category's **AllowedMembers** must include all users who will use any Persistent Chat room in this category. Depending on your requirements to protect business data and ensure the appropriate level of access, you may want to define one or more categories to specify who can search and participate in rooms. If you want to allow only a particular set of users (a central helpdesk, or only full-time employees) to create rooms, you can scope the **Creators** of a category to satisfy that requirement.

Categories can also be used to create ethical walls. Ethical walls prevent any conflict of interest in an organization. For example, an administrator can create chat rooms in a category for traders only, whereas chat rooms in another category can be used by analysts only.

Note:

In Lync Server 2013, Persistent Chat Server, we do not support access to federated users. If there are chats from federated users in previous versions of Persistent Chat Server, they will be migrated. The federated users are added as disabled principals.

Narrowing the Members to User Groups

When you add a domain to a category, the user groups whose group objects are contained in that domain are available to you so that you can specify them as members of rooms in that category.

We recommend, as a general rule, that you use Active Directory containers, such as domains and organizational units, for defining a category's **AllowedMembers** and **Creators**. You can add objects from any domain to an **AllowedMembers** or **Creators** list. Only objects within the **AllowedMembers** or **Creators** list can be added to rooms under that category.

1.7.6.4 Persistent Chat Server Best Practices

Persistent Chat Server Best Practices

See Also

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013, Persistent Chat Server >

Topic Last Modified: *2012-10-06*

As you create your categories and Persistent Chat rooms and design your scoping and membership, the following tips can help your planning:

- If your company does not require an ethical wall, do not narrow the scope in your category tree. Put all your users in the scope of one category, and create all chat rooms in that category. Subsequently, use only membership lists to grant or restrict access to each chat room.
- In most cases, you should enable users to create new chat rooms so that discussions about new topics can be started any time. Do this by making the **Creators** list the same as the **AllowedMembers** list. However, if you want to allow only a central support team or designated users to create rooms, then make the **Creators** list as the appropriate subset.
- Give each chat room a complete name and description summary that describes where it fits in with your organization. Because users cannot see the category name when they use the chat room, you cannot rely on the category name to help users determine the intended discussion forum for the chat room.
- You may want to have a custom room creation workflow if you have certain naming conventions or other access controls or validations to implement. The Persistent Chat configuration enables you to customize the **RoomManagementUrl** to something that you host. For example, when users click **Create a room** in their Lync client, they can be redirected to your custom solution.
- Create a variety of add-ins that help to enhance the experience of chat rooms by bringing in other business data into chat rooms. Administrators must register the add-ins that they want to allow in the system. Chat room managers and creators can choose from the list of allowed add-ins for the ones most relevant to their respective rooms.

Other Resources

Managing Categories, Rooms, and Add-Ins

1.7.6.5 Managing Categories, Rooms, and Add-Ins

Managing Categories, Rooms, and Add-Ins

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013, Persistent Chat Server >

Topic Last Modified: *2012-10-06*

In Lync Server 2013 Control Panel, or by using Windows PowerShell cmdlets, Persistent Chat Administrators can use the **Persistent Chat** page to create categories and add-ins. For managing Persistent Chat rooms, Administrators can use Windows PowerShell cmdlets. Alternatively, if the Persistent Chat administrator is also SIP-enabled, they can use the Lync client to launch a web page to create and manage chat rooms.

The following topics describe how to create and work with categories and chat rooms.

- Creating or Editing a New Category
- Creating or Editing a New Room
- Creating New Add-ins for Rooms
- Setting Who Can Post Messages in an Auditorium Chat Room
- Disabling or Enabling a Chat Room
- Moving a Chat Room from One Category to Another
- Deleting a Chat Room or Category
- Deleting a Message or Purging Obsolete Messages

1.7.6.5.1 Creating or Editing a New Category

Creating or Editing a New Category

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Categories, Rooms, and Add-Ins >

Topic Last Modified: *2012-10-06*

To create a new category, see Configure Categories in the Deployment documentation. If you are a Persistent Chat administrator, you can create categories by using the Lync Server Control Panel or Windows PowerShell cmdlets.

1.7.6.5.2 Creating or Editing a New Room

Creating or Editing a New Room

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Categories, Rooms, and Add-Ins >

Topic Last Modified: *2012-10-06*

Configuring Persistent Chat rooms is commonly handled by users; a Persistent Chat administrator typically does not configure or manage chat rooms. Windows PowerShell cmdlets to manage rooms are available only to **CsPersistentChatAdministrator** Administrators.

Users who are **Creators** in any given category can use the Lync client to create and manage rooms. Users who have been designated as managers for a specific chat room can also perform ongoing management of the room, such as editing the room properties or membership.

Tip:
Persistent Chat administrators can also be Creators, and they are not subject to the restrictions placed on Creators.

Optionally, if you are a Persistent Chat administrator, you can employ a user interface to create and manage chat rooms instead of using Windows PowerShell cmdlets. To do this, SIP-enable an administrator for Persistent Chat Server, and then use the Lync client to create and manage chat rooms.

If you want to create a custom room management workflow for your users, you can set the **RoomManagementUrl** property on your Persistent Chat Server configuration to redirect users to your custom solution from the Lync client.

For details about configuring chat rooms by using the Windows PowerShell command-line interface, see "Room Management" in Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets.

For details about configuring chat rooms, see Configure Rooms in the Deployment documentation.

1.7.6.5.3 Creating New Add-ins for Rooms

Creating New Add-ins for Rooms

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Categories, Rooms, and Add-Ins >

Topic Last Modified: *2012-10-06*

To create Add-ins for Persistent Chat rooms, see Configure Add-ins for Rooms in the Deployment documentation. If you are a Persistent Chat administrator, you can create add-ins by using the Lync Server Control Panel or Windows PowerShell cmdlets.

1.7.6.5.4 Setting Who Can Post Messages in an Auditorium Chat Room

Setting Who Can Post Messages in an Auditorium Chat Room

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Categories, Rooms, and Add-Ins >

Topic Last Modified: *2012-10-06*

In an auditorium chat room, only users who have been granted the role of Presenter can post messages. All other members can only read messages. Presenters in an auditorium chat room must be members of the chat room.

For details about using the Windows PowerShell command-line interface to manage auditorium chat rooms, see Manage Rooms in the Deployment documentation.

Although Persistent Chat room administrators and chat room managers can manage chat room settings, they cannot post in an auditorium chat room unless they are **Presenters**.

1.7.6.5.5 Disabling or Enabling a Chat Room

Disabling or Enabling a Chat Room

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Categories, Rooms, and Add-Ins >

Topic Last Modified: *2012-10-06*

If the topic of a Persistent Chat room is no longer relevant, you can make the chat room unavailable to users by disabling it. When a chat room is disabled, all members are immediately disconnected from the room. After a chat room is disabled, users cannot rejoin it or find it in chat room searches.

A disabled chat room can be enabled later by a Persistent Chat administrator. If a chat room is disabled, its membership list and other settings are preserved. If you enable the room again, you do not need to manually re-create the settings.

If the chat room’s history persists (chat room history persistence is an optional setting on a category that applies to all rooms within the category; the default is that it is persisted, but can be turned off by setting the category’s **Enable Chat History** to false), the content is preserved when the chat room is disabled. However, that content will not appear in searches during the time that the chat room remains in a disabled state. If you later enable the chat room, users can search for messages that were posted before the chat room was disabled.

For details about disabling and enabling chat rooms by using the Windows PowerShell command-line interface, see "Room Management" in Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets.

For details about configuring chat rooms, see Configure Rooms in the Deployment documentation.

1.7.6.5.6 Moving a Chat Room from One Category to Another

Moving a Chat Room from One Category to Another

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Categories, Rooms, and Add-Ins >

Topic Last Modified: *2012-11-01*

We recommend that you do not change the category of a Persistent Chat room after the chat room is created. However, if the chat room manager has **Creator** privileges in another category, he or she can move the room from one category to another. The room is not deleted and recreated. It is a change of association within the database.

Changing a chat room category should be done rarely. A category determines the allowed membership for the chat room, so when a chat room is moved to another category, all the system access control lists (SACLs) that are no longer supported by the new category are purged. For example, if a user was a member of the room and is no longer an **AllowedMember** in the new category, the room membership will be modified and the user will be removed from the room.

For details about moving a chat room by using the Windows PowerShell command-line interface, see "Room Management" in Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets.

For details about configuring chat rooms, see Configure Rooms in the Deployment documentation.

1.7.6.5.7 Deleting a Chat Room or Category

Deleting a Chat Room or Category

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Categories, Rooms, and Add-Ins >

Topic Last Modified: *2012-11-01*

Persistent Chat rooms can be deleted. If you have a chat room that is no longer being used, you can disable it. For details, see Disabling or Enabling a Chat Room.

A Persistent Chat administrator can query for disabled chat rooms, and can periodically purge and permanently delete the chat rooms, by using the Windows PowerShell cmdlet, **Remove-CsPersistentChatRoom**.

Categories can be deleted. However, to delete a category, you must first either delete all chat rooms under it or move the chat rooms to a new category, leaving an empty category for deletion. Persistent Chat Server does not allow you to delete a category that contains chat rooms. For details, see Moving a Chat Room from One Category to Another.

For details about deleting empty categories by using the Windows PowerShell command-line interface, see "Room Management" in Configuring Persistent Chat Server by Using Windows PowerShell Cmdlets.

For details about chat rooms and categories, see Configure Rooms and Configure Categories in the Deployment documentation.

1.7.6.5.8 Deleting a Message or Purging Obsolete Messages

Deleting a Message or Purging Obsolete Messages

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Categories, Rooms, and Add-Ins >

Topic Last Modified: *2012-10-06*

A Persistent Chat administrator can delete a message from a Persistent Chat room (and, optionally, can replace it with another message). Administrators can also purge obsolete messages as part of ongoing maintenance, to minimize growth of the database.

1.7.6.6 Managing Persistent Chat User Access

Managing Persistent Chat User Access

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013, Persistent Chat Server >

Topic Last Modified: *2012-10-06*

The following topics describe how to use the Lync Server 2013 Control Panel and the **Persistent Chat** page to manage user access in Persistent Chat. To manage Persistent Chat Server, you must have Persistent Chat administrator rights and permissions in the system. When you install Persistent Chat Server, you specify one or more users who have the necessary Persistent Chat administrator rights and permissions. To grant administrator rights and permissions to additional user accounts, use **Manage Users and User Groups**. For details, see Enabling a User to Manage Categories, Chat Rooms, and User Rights and Permissions.

- Adding Domains of Users and User Groups to the Room Category
- Disabling Uploading and Downloading Files in Chat Rooms
- Enabling a User to Manage Categories, Chat Rooms, and User Rights and Permissions

1.7.6.6.1 Adding Domains of Users and User Groups to the Room Category

Adding Domains of Users and User Groups to the Room Category

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Persistent Chat User Access >

Topic Last Modified: *2012-08-01*

To add domains of users and user groups to the room category, see Configure Categories and Manage Categories in the Deployment documentation.

1.7.6.6.2 Disabling Uploading and Dow nloading Files in Chat Rooms

Disabling Uploading and Downloading Files in Chat Rooms

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Persistent Chat User Access >

Topic Last Modified: *2012-09-12*

By default, users can upload and download files in the messages that they post. You can disable this functionality and prevent users from uploading and downloading files in two ways:

- Prevent all users from uploading and downloading files in a certain Persistent Chat room or chat room category.
- Prevent a certain user from uploading and downloading files in any chat room. The user cannot upload and download files in any chat room, including chat rooms that allow file uploading and downloading.

For details about enabling and disabling file uploading and downloading, see Configure Categories and Manage Categories in the Deployment documentation.

1.7.6.6.3 Enabling a User to Manage Categories, Chat Rooms, and User Rights and Permissions

Enabling a User to Manage Categories, Chat Rooms, and User Rights and Permissions

Operations > Managing Lync Server 2013, Persistent Chat Server > Managing Persistent Chat User Access >

Topic Last Modified: *2012-11-01*

Members of the **CsPersistentChatAdministrator** role (Persistent Chat administrators) can grant chat room manager rights and permissions to other users and to themselves.

A Persistent Chat administrator can do the following:

- Create room categories and chat rooms.
- Set the membership of all categories and chat rooms.
- Manage all settings of all categories and chat rooms.
- Enable or disable policy for Persistent Chat Server.
- Set and manage configuration settings on a Persistent Chat Server pool.

For details, see Adding a Persistent Chat Administrator in the Deployment documentation.

1.7.6.7 Operating and Maintaining the Persistent Chat System

Operating and Maintaining the Persistent Chat System

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013, Persistent Chat Server >

Topic Last Modified: *2012-11-01*

The following topics describe how to maintain the computer that is running Persistent Chat Server and how to manage Persistent Chat Server operations.

- Backing Up the Persistent Chat Database and Compliance Database
- Customizing the XSLT Definition File
- Replacing the XmlAdapter with a Customized Persistent Chat Server Compliance Adapter
- Managing System Health
- Monitoring, Starting, and Stopping the Persistent Chat Services
- Managing High Availability and Disaster Recovery

1.7.6.7.1 Backing Up the Persistent Chat Database and Compliance Database

Backing Up the Persistent Chat Database and Compliance Database

Operations > Managing Lync Server 2013, Persistent Chat Server > Operating and Maintaining the Persistent Chat System >

Topic Last Modified: *2012-08-01*

You should regularly back up the Persistent Chat database and the compliance database. Contact the database administrator to determine the best way to do this in your environment.

1.7.6.7.2 Customizing the XSLT Definition File

Customizing the XSLT Definition File

Operations > Managing Lync Server 2013, Persistent Chat Server > Operating and Maintaining the Persistent Chat System >

Topic Last Modified: *2012-11-01*

The Compliance service records and archives data related to each Lync Server 2013, Persistent Chat Server conversation, including when a participant:

- Joins a Persistent Chat room
- Leaves a chat room
- Posts a message
- Views chat history
- Uploads a file
- Downloads a file

The data is delivered as XML, which you can transform into the format that best fits your organization, by using an XSLT definition file. This topic describes the XML file that the Compliance service creates. It also provides samples of XSLT definition and output files.

Output Format

The Compliance service output is categorized by conversation (the Conversation element) and then by message (the Messages element), as shown in the following code sample.

```
<?xml version="1.0" encoding="utf-8" ?>
<Conversations xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="h
  <Conversation>
    <Channel uri="ma-chan://litwareinc.com/300" name="ma-chan://litwareinc.com/30
    <!--FirstMessage goes here --!>
    <Messages>
      <!–Messages go here--!>
    </Messages>
    <StartTimeUTC since1970="1212610540953" string="2008-06-04T20:15:40.9535482Z"
    <EndTimeUTC since1970="1212610602532" string="2008-06-04T20:16:42.5324614Z" l
  </Conversation>
</Conversations>
```

A Conversation element contains four elements (Channel, FirstMessage, StartTimeUTC, and EndTimeUTC). The Channel element contains the Uniform Resource Identifier (URI) of the chat room, and the FirstMessage element describes the first message in the Messages element. The StartTimeUTC and EndTimeUTC elements provide the start and end times for the conversation, as shown in the following code sample.

```
<<FirstMessage type="JOIN" content="" id="0">
      <Sender UserName="TestUser kazuto" id="10" email="kazuto@litwareinc.com" in
      <DateTimeUTC since1970="1212610540953" string="2008-06-04T20:15:40.9535482Z
</FirstMessage>
```

A Message element contains two elements (Sender and DateTimeUTC) and three attributes (Type, Content, and ID). The Sender element represents the user who sends the message, and the DateTimeUTC element represents when an event occurs, as shown in the following code sample.

```
<Message type="JOIN" content="" id="0">
  <Sender UserName="TestUser kazuto" id="10" email="kazuto@litwareinc.com" intern
  <DateTimeUTC since1970="1206211842612" string="2008-03-22T18:50:42.6127374Z" lo
</Message>
```

The following table describes the message attributes Type, Content, and ID.

Messages Element Attributes

Attribute	Description	Optional/Required
Type	Specifies the message type. The message types are described in the Message Elements Message Types table.	Required
Content	Contains the content of the message. Messages with a Type of Join or Part do not use this attribute.	Optional
ID	Specifies the unique ID of the content. This attribute is used only with messages	Optional

	with a Type of Chat.	

Each Sender element contains five attributes: the user name, ID, email, internal, and URI. These attributes are described in the following table.

Sender Element Attributes

Attribute	Description	Optional/Required
Username	The name of the sender.	Optional
ID	The sender’s unique ID.	Required
Email	The sender’s email address.	Optional
Internal	Determines whether the user is an internal user or a federated user. If the value is set to true, the user is internal.	Optional
Uri	The user’s SIP URI.	Required

The following table describes the message types that the Messages element can contain. It also provides examples of how each element is used.

Message Element Message Types

Message Type	Description	Code example

Join	A user joins a chat room.	<Message type="JOIN" conten
		  <Sender UserName="TestUse
		  <DateTimeUTC since1970="
		</Message

Part	A user leaves a chat room.	<Message type="PART" conten
		  < Sender UserName="TestUs
		  <DateTimeUTC since1970="
		</Message>

Chat	The sender’s email address.	<Message type="CHAT" conten
		  <Sender UserName="TestUse
		  <DateTimeUTC since1970="
		</Message>

Backchat	A user requests content from chat history.	<Message type="BACKCHAT" co
		  <Sender UserName="TestUse
		  <DateTimeUTC since1970="
		</Message>

File upload	A user uploads a file.	<Message type="FILEUPLOAD"
		  <Sender UserName="TestUse
		  <DateTimeUTC since1970="
		</Message>

File download	A user downloads a file.	<Message type="FILEDOWNLOAD
		  <Sender UserName="kazuto
		  <DateTimeUTC since1970="
		</Message>

Default Persistent Chat Output XSD and Example XSL Transform

The following code sample contains the default output from the Compliance Server.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="Conversations" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema
```

```
 <xs:simpleType name="ComplianceMessageType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="JOIN"/>
      <xs:enumeration value="PART"/>
      <xs:enumeration value="CHAT"/>
      <xs:enumeration value="BACKCHAT"/>
      <xs:enumeration value="FILEUPLOAD"/>
      <xs:enumeration value="FILEDOWNLOAD"/>
    </xs:restriction>
  </xs:simpleType>
<xs:element name="Sender">
  <xs:complexType>
    <xs:attribute name="UserName" type="xs:string" />
    <xs:attribute name="id" type="xs:int" />
    <xs:attribute name="email" type="xs:string" use="optional" />
    <xs:attribute name="internal" type="xs:boolean" use="optional" >
      <xs:annotation><xs:documentation>If the user is internal or federated</xs
    </xs:attribute>
    <xs:attribute name="uri" type="xs:anyURI" use="optional" />
  </xs:complexType>
</xs:element>
<xs:element name="DateTimeUTC">
  <xs:complexType>
    <xs:attribute name="since1970" type="xs:long" />
    <xs:attribute name="string" type="xs:string" />
    <xs:attribute name="long" type="xs:long" />
  </xs:complexType>
</xs:element>
<xs:element name="Conversations" msdata:IsDataSet="true" msdata:UseCurrentLocal
  <xs:complexType>
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:element ref="Sender" />
      <xs:element ref="DateTimeUTC" />
      <xs:element name="Conversation">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="Channel" minOccurs="0" maxOccurs="unbounded">
              <xs:complexType>
                <xs:attribute name="uri" type="xs:anyURI" />
                <xs:attribute name="name" type="xs:string" use="optional" />
              </xs:complexType>
            </xs:element>
            <xs:element name="FirstMessage" minOccurs="0" maxOccurs="unbounded"
              <xs:complexType>
                <xs:sequence>
                  <xs:element ref="Sender" minOccurs="0" maxOccurs="unbounded"
                  <xs:element ref="DateTimeUTC" minOccurs="0" maxOccurs="unboun
                </xs:sequence>
                <xs:attribute name="type" type="ComplianceMessageType" />
                <xs:attribute name="content" type="xs:string" />
                <xs:attribute name="id" type="xs:int" />
              </xs:complexType>
            </xs:element>
            <xs:element name="Messages" minOccurs="0" maxOccurs="unbounded">
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="Message" minOccurs="0" maxOccurs="unbounded
                    <xs:complexType>
                      <xs:sequence>
                        <xs:element ref="Sender" minOccurs="0" maxOccurs="unbou
                        <xs:element ref="DateTimeUTC" minOccurs="0" maxOccurs="
                      </xs:sequence>
                      <xs:attribute name="type" type="ComplianceMessageType" />
                      <xs:attribute name="content" type="xs:string" />
                      <xs:attribute name="id" type="xs:int" />
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
```

```
              <xs:element name="StartTimeUTC" minOccurs="0" maxOccurs="unbounded"
                <xs:complexType>
                  <xs:attribute name="since1970" type="xs:long" />
                  <xs:attribute name="string" type="xs:string" />
                  <xs:attribute name="long" type="xs:long" />
                </xs:complexType>
              </xs:element>
              <xs:element name="EndTimeUTC" minOccurs="0" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:attribute name="since1970" type="xs:long" />
                  <xs:attribute name="string" type="xs:string" />
                  <xs:attribute name="long" type="xs:long" />
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

The following code sample contains a sample XSL transform.

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xm
   <xsl:output method="xml" encoding="UTF-8" indent="yes" />
   <xsl:template match="/">
      <FileDump>
         <xsl:apply-templates />
      </FileDump>
   </xsl:template>
   <xsl:template match="Conversation">
      <xsl:variable name="chanName" select="Channel/@name" />
      <Conversation Perspective="{$chanName}_group_channel">
         <RoomID><xsl:value-of select="Channel/@name" /></RoomID>
         <StartTimeUTC><xsl:value-of select="StartTimeUTC/@since1970" /></StartTi
         <xsl:apply-templates />
         <EndTimeUTC><xsl:value-of select="EndTimeUTC/@since1970" /></EndTimeUTC>
      </Conversation>
   </xsl:template>
   <xsl:template match="Message">
      <xsl:choose>
         <xsl:when test="@type='JOIN'">
            <ParticipantEntered>
               <xsl:call-template name="DateTimeAndLogin" />
               <InternalFlag><xsl:value-of select="Sender/@internal" /></Internal
               <ConversationID><xsl:value-of select="../../Channel/@name" /></Con
               <CorporateEmailID><xsl:value-of select="Sender/@email" /></Corpora
            </ParticipantEntered>
         </xsl:when>
         <xsl:when test="@type='PART'">
            <ParticipantLeft>
               <xsl:call-template name="DateTimeAndLogin" />
               <InternalFlag><xsl:value-of select="Sender/@internal" /></Internal
               <ConversationID><xsl:value-of select="../../Channel/@name" /></Con
               <CorporateEmailID><xsl:value-of select="Sender/@email" /></Corpora
            </ParticipantLeft>
         </xsl:when>
         <xsl:when test="@type='FILEUPLOAD' or @type='FILEDOWNLOAD'">
            <FileTransferStarted>
               <xsl:call-template name="DateTimeAndLogin" />
               <FileName><xsl:value-of select="@content" /></FileName>
            </FileTransferStarted>
            <FileTransferEnded>
               <xsl:call-template name="DateTimeAndLogin" />
               <FileName><xsl:value-of select="@content" /></FileName>
               <Status>Completed</Status>
            </FileTransferEnded>
         </xsl:when>
         <xsl:when test="@type='CHAT' or @type='BACKCHAT'">
            <Message>
               <xsl:call-template name="DateTimeAndLogin" />
               <Content><xsl:value-of select="@content" /></Content>
            </Message>
         </xsl:when>
         <xsl:otherwise />
      </xsl:choose>
   </xsl:template>
   <xsl:template name="DateTimeAndLogin">
      <LoginName><xsl:value-of select="Sender/@userName" /></LoginName>
      <DateTimeUTC><xsl:value-of select="DateTimeUTC/@since1970" /></DateTimeUTC>
   </xsl:template>

</xsl:stylesheet
```

1.7.6.7.3 Replacing the XmlAdapter with a Customized Persistent Chat Server Compliance Adapter

Replacing the XmlAdapter with a Customized Persistent Chat Server Compliance Adapter

Operations > Managing Lync Server 2013, Persistent Chat Server > Operating and Maintaining the Persistent Chat System >

Topic Last Modified: *2012-11-01*

You can write a custom adapter instead of using the XmlAdapter that is installed with Persistent Chat Server. To accomplish this, you must provide a .NET Framework assembly that contains a public class that implements the **IComplianceAdapter** interface. You must place this assembly in the Persistent Chat Server installation folder of each server in your Persistent Chat Server pool. Any one of the Compliance servers can provide compliance data to your adapter, but the compliance servers will not provide duplicate compliance data to multiple instances of your adapter.

Implementing the IComplianceAdapter interface

The interface is defined in the Compliance.dll assembly in the namespace `Microsoft.Rtc.Internal.Chat.Server.Compliance`. The interface defines two methods that your custom adapter must implement.

```
void SetConfig(AdapterConfig config)
```

The Persistent Chat Compliance server will call this method when the adapter first loads. The `AdapterConfig` contains the Persistent Chat compliance configuration that is relevant to the compliance adapter.

```
void Translate(ConversationCollection conversations)
```

The Persistent Chat Compliance server calls this method at periodic intervals as long as there is new data to translate. This time interval is equal to the `RunInterval` as set in the Persistent Chat Compliance configuration.

The `ConversationCollection` contains the conversation information that was collected from the last time this method was called.

1.7.6.7.4 Managing System Health

Managing System Health

Operations > Managing Lync Server 2013, Persistent Chat Server > Operating and Maintaining the Persistent Chat System >

Topic Last Modified: *2012-11-01*

System health management and monitoring is integrated into the overall Lync Server 2013 health management and monitoring. For details, see Health Configuration in Lync Server 2013.

1.7.6.7.5 Monitoring, Starting, and Stopping the Persistent Chat Services

Monitoring, Starting, and Stopping the Persistent Chat Services

Operations > Managing Lync Server 2013, Persistent Chat Server > Operating and Maintaining the Persistent Chat System >

Topic Last Modified: *2012-10-06*

The Persistent Chat services and Persistent Chat Compliance services are part of the Lync Server 2013 topology and can therefore be monitored, stopped, and started by using the Windows PowerShell cmdlets, **get-CsWindowsService**, **stop-CsWindowsService**, and **start-CsWindowsService**, respectively.

1.7.6.7.6 Managing High Availability and Disaster Recovery

Managing High Availability and Disaster Recovery

Operations > Managing Lync Server 2013, Persistent Chat Server > Operating and Maintaining the Persistent Chat System >

Topic Last Modified: *2012-08-03*

The following topics describe how to configure high availability, disaster recovery, failing over, and failing back for Persistent Chat Server.

- Configuring for Persistent Chat High Availability and Disaster Recovery
- Failing Over and Failing Back Persistent Chat Server

1.7.6.7.6.1 Configuring for Persistent Chat High Availability and Disaster Recovery

Configuring for Persistent Chat High Availability and Disaster Recovery

Managing Lync Server 2013, Persistent Chat Server > Operating and Maintaining the Persistent Chat System > Managing High Availability and Disaster Recovery >

Topic Last Modified: *2012-10-06*

For details about how to configure the Persistent Chat services for high availability and disaster recovery, see Deploying Persistent Chat Server.

1.7.6.7.6.2 Failing Over and Failing Back Persistent Chat Server

Failing Over and Failing Back Persistent Chat Server

Managing Lync Server 2013, Persistent Chat Server > Operating and Maintaining the Persistent Chat System > Managing High Availability and Disaster Recovery >

Topic Last Modified: *2012-08-03*

To fail over and fail back Lync Server 2013, Persistent Chat Server, you should be familiar with replication and failover processes for Microsoft SQL Server 2008 R2 and later. You should also be familiar with the Persistent Chat Server services.

In This Section

- Failing Over Persistent Chat Server
- Failing Back Persistent Chat Server

Failing Over Persistent Chat Server

Operating and Maintaining the Persistent Chat System > Managing High Availability and Disaster Recovery > Failing Over and Failing Back Persistent Chat Server >

Topic Last Modified: *2012-11-01*

Failover for Persistent Chat Server is designed to be mainly a manual process.

The failover procedure is based on the assumption that the secondary data center is up and running, but the Persistent Chat Server services where the primary Persistent Chat database is located are completely unavailable, including the following:

- Persistent Chat Server primary database and Persistent Chat Server mirror database are down.
- Lync Server Front End Server is down.

The procedure is based on two basic steps:

- Recover the primary Persistent Chat database (mgc).
- Establish mirroring for the new primary database.

The Persistent Chat compliance database (mgccomp) is not failed over. The contents of this database are transient and are purged as the compliance adapter processes the data. It is your responsibility, as Persistent Chat Administrator, to correctly manage the adapter output to avoid data loss.

To fail over Persistent Chat Server

1. Remove log shipping from the Persistent Chat Server Backup Log Shipping database.
   1.a. Using SQL Server Management Studio, connect to the database instance where the Persistent Chat Server backup mgc database is located.
   1.b. Open a query window to the master database.
   1.c. Use the following command to drop log shipping:

```
exec sp_delete_log_shipping_secondary_database mgc
```

2. Copy any uncopied backup files from the backup share to the copy destination folder of the backup server.
3. Apply any unapplied transaction log backups in sequence to the secondary database. For details, see "How to: Apply a Transaction Log Backup (Transact-SQL)" at http://go.microsoft.com/fwlink/p/?linkid=247428.
4. Bring the backup mgc database online. Using the query window that opens in step 1b, do the following:
   4.a. End all connections to the mgc database, if there are any:
      4.a.a. **\exec sp_who2** to identify connections to the mgc database.
      4.a.b. **\kill <spid>** to end these connections.
   4.b. Bring the database online:
      4.b.a. **\restore database mgc with recovery**.
5. In Lync Server Management Shell, use the **Set-CsPersistentChatState service:PersistentChatPoolFqdn –PoolState FailedOver** cmdlet to fail over to the mgc backup database.
   The mgc backup database now serves as the primary database.
6. In Lync Server Management Shell, use the **Install-CsMirrorDatabase** cmdlet to establish a high availability mirror for the backup database that now serves as the primary database. Use the backup database instance as the primary database and the backup mirror database instance as the mirror instance. This is not the same mirror as the one that was initially configured for the primary database during setup. For details, see the section "Using Lync Server Management Shell Cmdlets" in Deploying SQL Mirroring for Back End Server High Availability.
7. Set the Persistent Chat Server active servers. From the Lync Server Command Shell, use the **Set-CsPersistentChatActiveServer** cmdlet to set the list of active servers.

   > **Important:**
   > All the active servers must be located within the same data center as the new primary database, or in a data center that has a low latency/high bandwidth connection to the database.

   At this point, the failover from the Persistent Chat Server primary database to the Persistent Chat Server backup database completes successfully.

Failing Back Persistent Chat Server

Operating and Maintaining the Persistent Chat System > Managing High Availability and Disaster Recovery > Failing Over and Failing Back Persistent Chat Server >

Topic Last Modified: *2012-11-01*

This procedure outlines the steps necessary to recover from a Persistent Chat Server failure, and to reestablish operations from the primary data center.

During Persistent Chat Server failure, the primary data center suffers complete outage, and the primary and mirror databases become unavailable. The primary data center fails over to the backup server.

The following procedure restores normal operation after the primary data center is back up, and the servers have been rebuilt. The procedure assumes that the primary data center has been recovered from total outage, and that the mgc database and the mgccomp database have been rebuilt and reinstalled by using Topology Builder.

The procedure also assumes that no new mirror and backup servers were deployed during the failover period, and that the only server deployed is the backup server and its mirror server, as defined in Failing Over Persistent Chat Server.

These steps are designed to recover configuration as it existed prior to the disaster, resulting in failover from the primary server to the backup server.

To fail back Persistent Chat Server

1. Clear all servers from the Persistent Chat Server Active Server list by using the `Set-CsPersistentChatActiveServer` cmdlet from the Lync Server Management Shell. This stops all Persistent Chat Servers from connecting to the mgc database and the mgccomp database during failback.

> **Important:**
>
> The SQL Server agent on the secondary Persistent Chat Server Back End Server should be running under a privileged account. Specifically, the account must include:
>
> - Read access to the network share that backups are being placed in.
> - Write access to the specific local directory that the backups are being copied to.

1. Disable mirroring on the backup mgc database:
   - Using SQL Server Management Studio, connect to the backup mgc instance.
   - Right-click the mgc database, point to **Tasks**, and then click **Mirror**.
   - Click **Remove Mirroring**.
   - Click **OK**.
   - Perform the same steps with the mgccomp database.
2. Back up the mgc database so that it can be restored to the new primary database:
   - Using SQL Server Management Studio, connect to the backup mgc instance.
   - Right-click the mgc database, point to **Tasks**, and then click **Back Up**. The **Back Up Database** dialog box appears.
   - In **Backup type**, select **Full**.
   - For **Backup component**, click **Database**.
   - Either accept the default backup set name suggested in **Name**, or enter a different name for the backup set.
   - *<Optional>* In **Description**, enter a description of the backup set.
   - Remove the default backup location from the destination list.
   - Add a file to the list by using the path to the share location that you established for log shipping. This path is available to the primary database and to the backup database.
   - Click **OK** to close the dialog box and begin the backup process.
3. Restore the primary database by using the backup database created in the previous step.
   - Using SQL Server Management Studio, connect to the primary mgc instance.
   - Right-click the mgc database, point to **Tasks**, point to **Restore**, and then click **Database**. The **Restore Database** dialog box appears.
   - Select **From Device**.
   - Click the browse button, which opens the **Specify Backup** dialog box. In **Backup media**, select **File**. Click **Add**, select the backup file that you created in step 3, and then click **OK**.
   - In **Select the backup sets to restore**, select the backup.
   - Click **Options** in the **Select a page** pane.
   - In **Restore options**, select **Overwrite the existing database**.
   - In **Recovery State**, select **Leave the database ready to use**.
   - Click **OK** to begin the restoration process.
4. Configure SQL Server Log Shipping for the primary database. Follow the procedures in Configuring Persistent Chat Server for High Availability and Disaster Recovery to establish log shipping for the primary mgc database.

5. Set the Persistent Chat Server active servers. From the Lync Server Management Shell, use the **Set-CsPersistentChatActiveServer** cmdlet to set the list of active servers.

Important:
All the active servers must be located within the same data center as the new primary database, or in a data center that has a low latency/high bandwidth connection to the database.

1.7.7 Managing Voice Routing

Managing Voice Routing

See Also

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-11-01*

Topics in this section provide step-by-step procedures for tasks that you can perform by using the **Voice Routing** group in Lync Server Control Panel.

- Defining Translation Rules and Normalization Rules
- Configuring Trunks
- Configuring Voice Policies, PSTN Usage Records, and Voice Routes
- Configuring Dial Plans

⊟See Also

Concepts

Planning for Enterprise Voice

Other Resources

Managing Call Management Features

1.7.7.1 Defining Translation Rules and Normalization Rules

Defining Translation Rules and Normalization Rules

See Also

Microsoft Lync Server 2013 > Operations > Managing Voice Routing >

Topic Last Modified: *2012-10-18*

Use the topics in the section to learn how to configure Trunks for Lync Server 2013.

- Defining Translation Rules
- Defining Normalization Rules

⊟See Also

Other Resources

Managing Voice Routing

1.7.7.1.1 Defining Translation Rules

Defining Translation Rules

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2013-02-22*

Lync Server 2013 Enterprise Voice routes calls based on phone numbers normalized to E.164 format. This means that all dialed strings must be normalized to E.164 format for the purpose of performing reverse number lookup (RNL) so they can be translated to their matching SIP URI. Lync Server 2013 provides the ability to manipulate the called ID and the caller ID presentation.

This section discusses how to manipulate the called ID and caller ID.

- Caller ID Presentation
- Called ID Presentation

⊟See Also

Other Resources

Defining Normalization Rules

1.7.7.1.1.1 Caller ID Presentation

Caller ID Presentation

Deploying Enterprise Voice > Configuring Trunks > Defining Translation Rules >

Topic Last Modified: *2013-02-22*

With Lync Server 2010, the called party’s phone number (that is, the phone number called) can be translated from E.164 format to the local dialing format that is required by the *trunk peer* (that is, the associated gateway, private branch exchange (PBX), or SIP trunk). To do this, you must define one or more translation rules to translate the Request URI before routing it to the trunk peer.

Lync Server 2013 introduces the option to also translate the calling party’s phone number (that is, the phone number that the caller is calling from) from E.164 format to the local dialing format that is required by the trunk peer. For example, you can write a translation rule to remove +44 from the beginning of a dial string and replace it with 0144.

To configure Caller ID by using Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
4. On the **Trunk Configuration** page, double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
5. To configure caller ID presentation:
    - To choose one or more rules from a list of all translation rules available in your Enterprise Voice deployment, click **Select**. In **Calling number translation rules**, click the rules that you want to associate with the trunk, and then click **OK**.
    - To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
    - To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
    - To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.

- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

⚠Warning:

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

1.7.7.1.1.2 Called ID Presentation

Called ID Presentation

See Also

Deploying Enterprise Voice > Configuring Trunks > Defining Translation Rules >

Topic Last Modified: *2012-09-21*

With Lync Server 2010, the called party’s phone number (that is, the phone number called) can be translated from E.164 format to the local dialing format that is required by the *trunk peer* (that is, the associated gateway, private branch exchange (PBX), or SIP trunk). To do this, you must define one or more translation rules to translate the Request URI before routing it to the trunk peer.

Important:

The ability to associate one or more translation rules with an Enterprise Voice trunk configuration is intended to be used as an *alternative* to configuring translation rules on the trunk peer. Do not associate translation rules with an Enterprise Voice trunk configuration if you have configured translation rules on the trunk peer because the two rules might conflict.

You can use either of the following methods to create or modify a translation rule:

- Use the **Build a Translation Rule** tool to specify values for the starting digits, length, digits to remove and digits to add, and then let Lync Server Control Panel generate the corresponding matching pattern and translation rule for you.
- Write regular expressions manually to define the matching pattern and translation rule.

Note:

For information about how to write regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.

- Create or Modify a Translation Rule by Using the Build a Translation Rule Tool
- Create or Modify a Translation Rule Manually

See Also

Concepts

Caller ID Presentation

Create or Modify a Translation Rule by Using the Build a Translation Rule Tool

See Also

Configuring Trunks > Defining Translation Rules > Called ID Presentation >

Topic Last Modified: *2012-10-05*

Follow these steps if you want to define a translation rule by entering a set of values in the **Build a Translation Rule** tool and enabling Lync Server Control Panel to generate the corresponding matching pattern and translation rule for you. Alternatively, you can a write regular expression manually to define the matching pattern and translation rule. For details, see Create or Modify a Translation Rule Manually.

⊟To define a rule by using the Build a Translation Rule tool

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. To begin defining a translation rule, follow the steps in Configure a Trunk with Media Bypass through step 10 or Configure a Trunk without Media Bypass through step 9.
4. Under **Name** on the **New Translation Rule** or **Edit Translation Rule** page, type a name that describes the number pattern being translated.
5. (Optional) Under **Description**, type a description of the translation rule, for example **US International long-distance dialing**.
6. In the **Build a Translation Rule** section of the dialog box, enter values in the following fields:
   - **Starting digits**: (Optional) Specify the leading digits of numbers you want the pattern to match. For example, enter **+** in this field to match numbers in E.164 format (which begin with +).
   - **Length**: Specify the number of digits in the matching pattern and select whether you want the pattern to match numbers that are this length exactly, at least this length, or any length. For example, enter **11** and select **At least** in the drop-down list to match numbers that are at least 11 digits in length.
   - **Digits to remove**: (Optional) Specify the number of starting digits to be removed. For example, enter **1** to strip out the **+** from the beginning of the number.
   - **Digits to add**: (Optional) Specify digits to be prepended to the translated numbers. For example, enter **011** if you want 011 to be prepended to the translated numbers when the rule is applied.

   The values you enter in these fields are reflected in the **Pattern to match** and **Translation rule** fields. For example, if you specify the preceding example values, the resulting regular expression in the **Pattern to match** field is:

   ^\+(\d{9}\d+)$

   The **Translation rule** field specifies a pattern for the format of translated numbers. This pattern has two parts:

   - A value (for example, **$1**) that represents the number of digits in the matching pattern
   - (Optional) A value that you can prepend by entering it in the **Digits to add** field

   Using the preceding example values, **011$1** appears in the **Translation rule** field.

   When this translation rule is applied, +441235551010 becomes 011441235551010.
7. Click **OK** to save the translation rule.
8. Click **OK** to save the trunk configuration.
9. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

> **Note:**
>
> Whenever you create or modify a translation rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Translation Rule Manually
Configure a Trunk with Media Bypass
Configure a Trunk without Media Bypass
Publish Pending Changes to the Voice Routing Configuration

Concepts

Global Media Bypass Options

Create or Modify a Translation Rule Manually

See Also

Configuring Trunks > Defining Translation Rules > Called ID Presentation >

Topic Last Modified: *2012-08-06*

Follow these steps if you want to define a translation rule by writing a regular expression for the matching pattern and translation rule. Alternatively, you can enter a set of values in the **Build a Translation Rule** tool and enable Lync Server Control Panel to generate the corresponding matching pattern and translation rule for you. For details, see Create or Modify a Translation Rule by Using the Build a Translation Rule Tool.

To define a translation rule manually

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. To begin defining a translation rule, follow the steps in Configure a Trunk with Media Bypass through step 10 or Configure a Trunk without Media Bypass through step 9.
4. In the **Name** field on the **New Translation Rule** or **Edit Translation Rule** page, type a name that describes the number pattern being translated.
5. (Optional) In **Description**, type a description of the translation rule, for example **US International long-distance dialing**.
6. Click **Edit** at the bottom of the **Build a Translation Rule** section.
7. Enter the following in **Type a Regular Expression**:
   - In **Match this pattern**, specify the pattern that will be used to match the numbers to be translated.
   - In **Translation rule**, specify a pattern for the format of translated numbers.

   For example, if you enter **^\+(\d{9}\d+)$** in **Match this pattern** and **011$1** in **Translation rule**, the rule will translate +441235551010 to 011441235551010.
8. Click **OK** to save the translation rule.
9. Click **OK** to save the trunk configuration.
10. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

> **Note:**
> Whenever you create or modify a translation rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Translation Rule by Using the Build a Translation Rule Tool
Configure a Trunk with Media Bypass
Configure a Trunk without Media Bypass

Publish Pending Changes to the Voice Routing Configuration

Concepts

Global Media Bypass Options

1.7.7.1.2 Defining Normalization Rules

Defining Normalization Rules

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-09-23*

Lync Server 2013 normalization rules use .NET Framework regular expressions to translate dialed phone numbers to E.164 format. Each dial plan must be assigned one or more normalization rules.

For details about normalization rules, see Dial Plans and Normalization Rules in the Planning documentation.

For details about how to write regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.

You can use either of the following methods to define or edit a normalization rule:

- Use the **Build a Normalization Rule** tool to specify values for the starting digits, length, digits to remove and digits to add, and then let Lync Server Control Panel generate the corresponding matching pattern and translation rule for you.
- Write regular expressions manually to define the matching pattern and translation rule.
- Create or Modify a Normalization Rule by Using Build a Normalization Rule
- Create or Modify a Normalization Rule Manually

⊟See Also

Tasks

Create a Dial Plan
Modify a Dial Plan

1.7.7.1.2.1 Create or Modify a Normalization Rule by Using Build a Normalization Rule

Create or Modify a Normalization Rule by Using Build a Normalization Rule

See Also

Deploying Enterprise Voice > Configuring Dial Plans > Defining Normalization Rules >

Topic Last Modified: *2012-11-01*

Complete the following steps if you want to create or modify a normalization rule in Lync Server Control Panel. Alternatively, if you want to create or modify a normalization rule manually, see Create or Modify a Normalization Rule Manually.

⊟To define a rule by using Build a Normalization Rule

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. (Optional) Follow the steps in Create a Dial Plan through step 11 or Modify a Dial Plan through step 10.
4. In **New Normalization Rule** or **Edit Normalization Rule**, type a name that describes the number pattern being normalized in **Name** (for example, **5DigitExtension**).
5. (Optional) In **Description**, type a description of the normalization rule (for example, "Translates 5-digit extensions").
6. In **Build a Normalization Rule**, enter values in the following fields:
   - **Starting digits** (Optional) Specify the leading digits of dialed numbers you want the pattern to match. For example, type **425** if you want the pattern to match dialed numbers beginning with 425.
   - **Length** Specify the number of digits in the matching pattern and select whether you want the pattern to match this length exactly, match dialed numbers that are at least this length, or match dialed numbers of any length.
   - **Digits to remove** (Optional) Specify the number of starting digits to be removed from dialed numbers you want the pattern to match.
   - **Digits to add** (Optional) Specify digits to be added to dialed numbers you want the pattern to match.

   The values you enter in these fields are reflected in **Pattern to match** and **Translation rule**. For example, if you leave **Starting digits** empty, type **7** into the **Length** field and select **Exactly**, and specify **0** in **Digits to remove**, the resulting regular expression in the **Pattern to match** is:

   ^(\d{7})$
7. In **Translation rule**, specify a pattern for the format of translated E.164 phone numbers as follows:
   - A value that represents the number of digits specified in the matching pattern. For example, if the matching pattern is **^(\d{7})$** then **$1** in the translation rule represents 7-digit dialed numbers.
   - (Optional) Type a value into the **Digits to add** field to specify digits to be prepended to the translated number (for example, **+1425**).

   For example, if **Pattern to match** contains **^(\d{7})$** as the pattern for dialed numbers and **Translation rule** contains **+1425$1** as the pattern for E.164 phone numbers, the rule normalizes 5550100 to +14255550100.
8. (Optional) If the normalization rule results in a phone number that is internal to your organization, select **Internal extension**.
9. (Optional) Enter a number to test the normalization rule, and then click **Go**. The test results are displayed under **Enter a number to test**.

   Note:
   You can save a normalization rule that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.
10. Click **OK** to save the normalization rule.
11. Click **OK** to save the dial plan.
12. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

    Note:
    Whenever you create or change a normalization rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Normalization Rule Manually
Create a Dial Plan
Modify a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

1.7.7.1.2.2 Create or Modify a Normalization Rule Manually

Create or Modify a Normalization Rule Manually

See Also

Deploying Enterprise Voice > Configuring Dial Plans > Defining Normalization Rules >

Topic Last Modified: *2012-09-22*

Complete the following steps if you want to create or modify a normalization rule manually. If you want to create or modify a normalization rule by using Build a Normalization Rule in Lync Server Control Panel, see Create or Modify a Normalization Rule by Using Build a Normalization Rule.

⊟To define a normalization rule manually

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. (Optional) Follow the steps in Create a Dial Plan or Modify a Dial Plan.
4. In **New Normalization Rule** or **Edit Normalization Rule**, type a name that describes the number pattern being normalized in **Name** (for example, name the normalization rule **5DigitExtension**).
5. (Optional) In **Description** field, type a description of the normalization rule (for example, "Translates 5-digit extensions").
6. In **Build a Normalization Rule**, click **Edit**.
7. Enter the following in **Type a Regular Expression**:
   - In **Match this pattern**, specify the pattern that you want to use to match the dialed phone number.
   - In **Translation rule**, specify a pattern for the format of translated E.164 phone numbers.

   For example, if you enter **^(\d{7})$** in **Match this pattern** and **+1425$1** in **Translation rule**, the rule normalizes 5550100 to +14255550100.
8. (Optional) If the normalization rule results in a phone number that is internal to your organization, select **Internal extension**.
9. (Optional) Enter a number to test the normalization rule and then click **Go**. The test results are displayed under **Enter a number to test**.

   > **Note:**
   > You can save a normalization rule that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.
10. Click **OK** to save the normalization rule.
11. Click **OK** to save the dial plan.
12. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

   > **Note:**
   > Whenever you create or change a normalization rule, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create or Modify a Normalization Rule by Using Build a Normalization Rule

Create a Dial Plan
Modify a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

1.7.7.2 Configuring Trunks

Configuring Trunks

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-11-01*

As part of Enterprise Voice deployment, you can configure a trunk between a Mediation Server and one or more of the following peers to provide public switched telephone network (PSTN) connectivity for Enterprise Voice clients and devices in your organization:

- SIP trunk connection to an Internet telephony service provider (ITSP)
- PSTN gateway
- Private branch exchange (PBX)

For details, see Planning for PSTN Connectivity in the Planning documentation.

Important:
Before you begin trunk configuration, verify that the topology has been created and that the Mediation Server and its peer have been configured and associated with one another. For details, see Define a Gateway in Topology Builder in the Deployment documentation.

Note:
As a part of trunk configuration, you can enable the Lync Server 2013 media bypass feature, which enables media to bypass the Mediation Server. Trunks can be configured either with or without media bypass enabled, but we strongly recommend that you enable it. For details, see Planning for Media Bypass in the Planning documentation.

- Multiple Trunk Support
- Inter-Trunk Routing
- View Trunk Configuration Information
- Configure a Trunk with Media Bypass
- Configure a Trunk without Media Bypass
- Create a New Collection of Trunk Configuration Settings
- Delete an Existing Collection of SIP Trunk Configuration Settings
- Modify SIP Trunk Configuration Settings
- Test SIP Trunk Configuration Settings
- View Information about Individual SIP Trunks

See Also

Tasks

Define a Gateway in Topology Builder

Other Resources

Planning for PSTN Connectivity
Planning for Media Bypass

1.7.7.2.1 Multiple Trunk Support

Multiple Trunk Support

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2012-11-01*

Lync Server 2013 functionality supports multiple associations between gateways and Mediation Servers. These associations are made by defining a trunk, which is a logical association between a Mediation Server pool and a public switched telephone network (PSTN) gateway, Session Border Controller (SBC), or IP-PBX. Use the Topology Builder to associate gateways with Mediation Servers (that is, trunks).

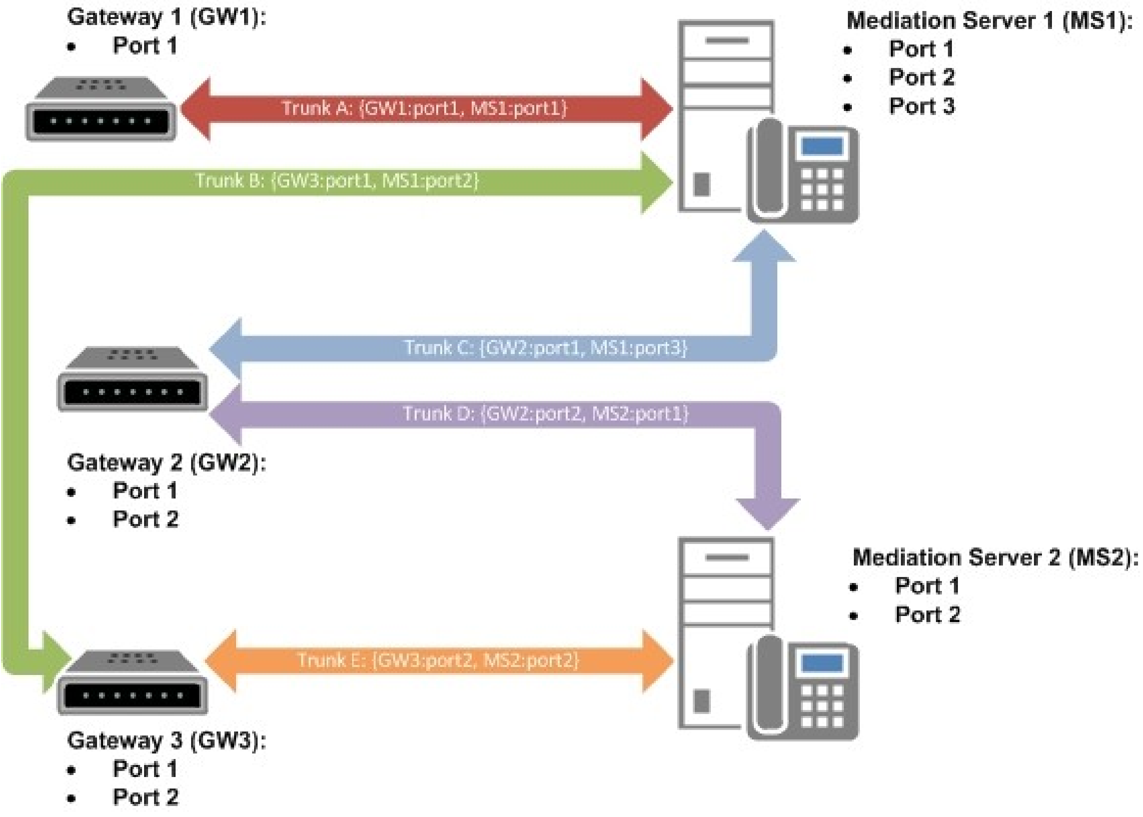
- To assign or remove a trunk in Lync Server 2013, you must first define a trunk in Topology Builder. A trunk consists of the following association: Mediation Server fully qualified domain name (FQDN), the Mediation Server listening port, the gateway FQDN, and the gateway listening port.
- To configure multiple trunks, you can create multiple associations between the same gateway and the Mediation Server. This provides additional resiliency to the Enterprise Voice infrastructure, which is especially useful in private branch exchange (PBX) interoperational scenarios.

When a trunk is defined, it must be associated to a route. To associate a trunk to a route, you define a simple name for the trunk in Topology Builder. This simple name is used as the trunk name in the Lync Server Control Panel, where trunks can be associated with routes. The simple trunk name is used as the gateway name from the Lync Server Management Shell.

```
New-CsVoiceRoute -Identity <RouteId> -NumberPattern <String> -PstnUsages @{add="<
```

The administrator must select a default trunk associated with a Mediation Server. From the Topology Builder, right-click the associated Mediation Server, and then click **Properties**. Specify the default gateway for the Mediation Server.

The following diagram illustrates the multiple trunks that are defined for each Mediation Server and gateway.


Gateway 1 (GW1):
Port 1
Trunk A: {GW1:port1, MS1:port1}
Trunk B: {GW3:port1, MS1:port2}
Mediation Server 1 (MS1):
Port 1
Port 2
Port 3
Trunk C: {GW2:port1, MS1:port3}
Trunk D: {GW2:port2, MS2:port1}
Gateway 2 (GW2):
Port 1
Port 2
Mediation Server 2 (MS2):
Port 1
Port 2
Trunk E: {GW3:port2, MS2:port2}
Gateway 3 (GW3):
Port 1
Port 2

1.7.7.2.2 Intertrunk Routing

Intertrunk Routing

Operations > Managing Voice Routing > Configuring Trunks >

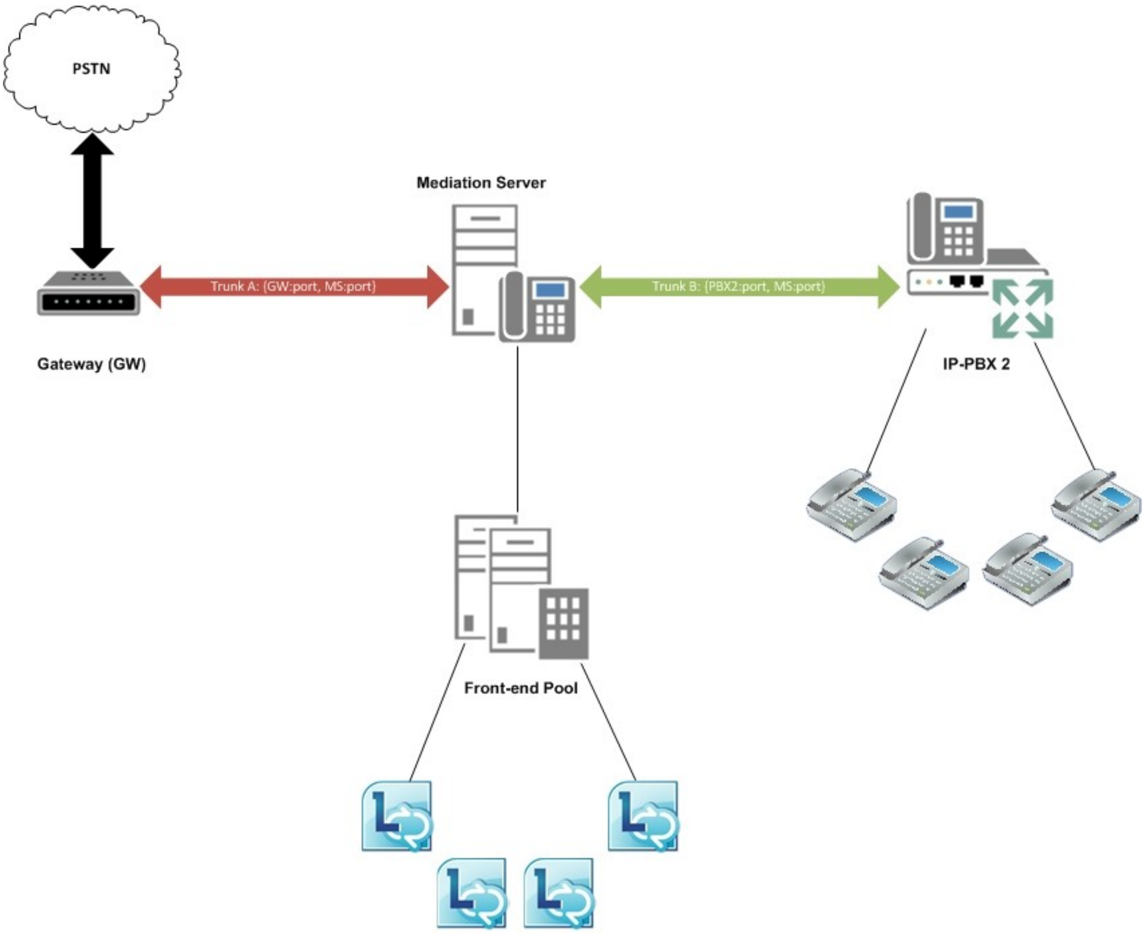
Topic Last Modified: *2012-10-20*

Lync Server 2013 can interconnect an IP-PBX to a public switched telephone network (PSTN) gateway so that calls from a PBX phone can be routed to the PSTN, and incoming PSTN calls can be routed to a private branch exchange (PBX) phone. Similarly, Lync Server 2013 can interconnect two or more IP-PBX systems so that calls can be placed and received between PBX phones from the different IP-PBX systems.

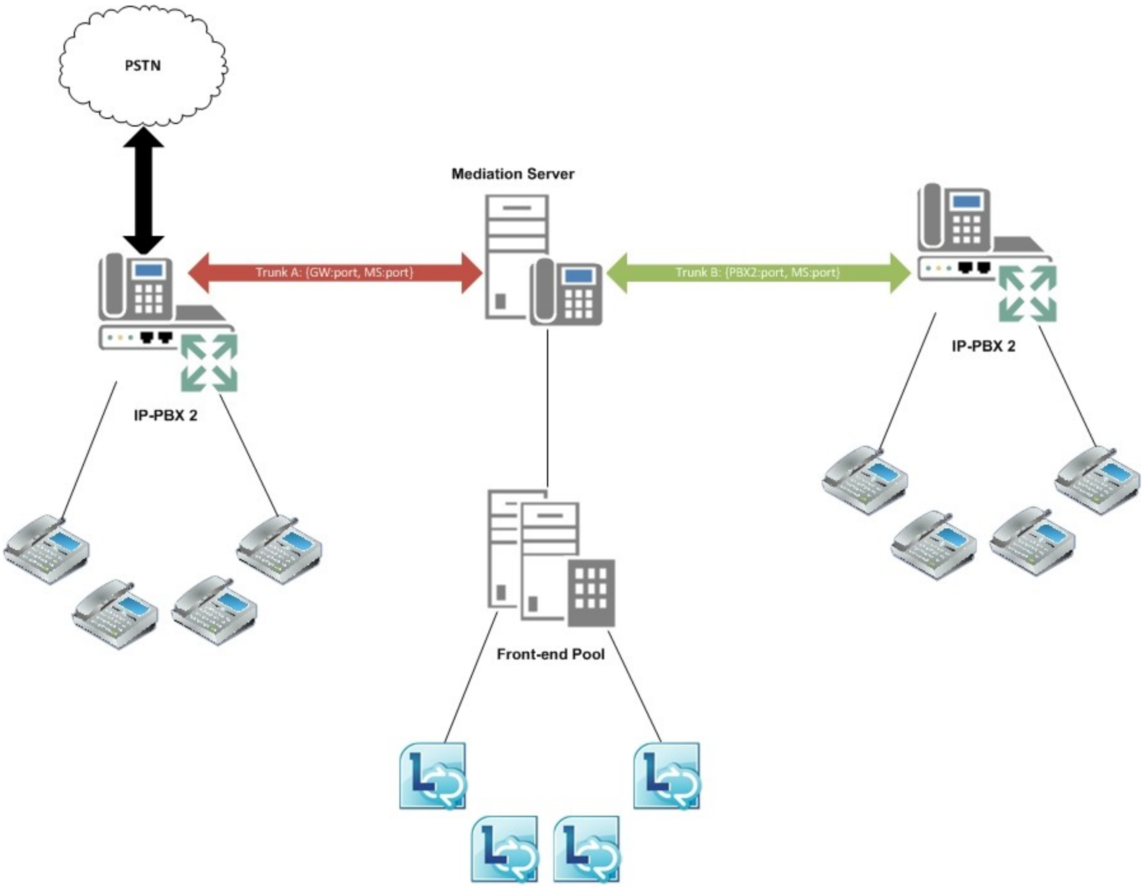
This intertrunk routing feature can be configured by using the Lync Server Management Shell cmdlet, **Set-CsTrunkConfiguration**, with the new parameter, PstnUsages. This parameter specifies the set of PSTN usage records to use. A trunk uses this PSTN usage to determine a route and to route all incoming calls accordingly.

```
Set-CsTrunkConfiguration -Identity <TrunkId> -PstnUsages @{add="<UsageString>"}
```

The following diagram illustrates Lync Server 2013 providing interconnectivity between a PSTN gateway and an IP-PBX.



The following diagram illustrates Lync Server 2013 interconnecting two IP-PBX systems.



1.7.7.2.3 View Trunk Configuration Information

View Trunk Configuration Information

Operations > Managing Voice Routing > Configuring Trunks >

Topic Last Modified: *2013-02-22*

SIP trunk configuration settings define the relationship and capabilities between a Mediation Server and the public switched telephone network (PSTN) gateway, an IP-public branch exchange (PBX), or a Session Border Controller (SBC) at the service provider. These settings do such things as specify:

- Whether media bypass should be enabled on the trunks.
- The conditions under which real-time transport control protocol (RTCP) packets are sent.
- Whether or not secure real-time protocol (SRTP) encryption is required on each trunk.

When you install Microsoft Lync Server 2013, a global collection of SIP trunk configuration settings is created for you. In addition, administrators can create custom setting collections at the site scope or at the service scope (for the PSTN gateway service, only).

⊟To view SIP trunk configuration information by using Lync Server Control Panel

1. In Lync Server Control Panel, click **Voice Routing** and then click **Trunk**

Configuration.

2. On the **Trunk Configuration** tab you will see a list of all your trunk configuration settings collection; for each collection you will see values for the **Name**, **Scope**, **State**, and **Media bypass** properties, along with the number of **PSTN usages**, **Calling number rules**, and **Called number rules** associated with the collection. To see additional details about a collection of trunk configuration settings, click the collection of interest, click **Edit**, and then click **Show details**. Note that you can view detailed information only for one collection of trunk configuration settings at a time.

Viewing SIP Trunk Configuration Information by Using Windows PowerShell Cmdlets

SIP trunk configuration settings can be viewed by using Lync Server PowerShell and the Get-CsTrunkConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view SIP trunk configuration information

- To view information about all your SIP trunk configuration settings, type the following command in the Lync Server Management Shell and then press ENTER:

```
Get-CsTrunkConfiguration
```

That will return information similar to this:

```
Identity                                  : Global
OutboundTranslationRulesList              : {}
SipResponseCodeTranslationRulesList       : {}
OutboundCallingNumberTranslationRulesList : {}
PstnUsages                                : {}
Description                               :
ConcentratedTopology                      : True
EnableBypass                              : False
EnableMobileTrunkSupport                  : False
EnableReferSupport                        : True
EnableSessionTimer                        : False
EnableSignalBoost                         : False
MaxEarlyDialogs                           : 20
RemovePlusFromUri                         : False
RTCPActiveCalls                           : True
RTCPCallsOnHold                           : True
SRTPMode                                  : Required
EnablePIDFLOSupport                       : False
EnableRTPLatching                         : False
EnableOnlineVoice                         : False
ForwardCallHistory                        : False
Enable3pccRefer                           : False
ForwardPAI                                : False
EnableFastFailoverTimer                   : True
```

For more information, see the help topic for the Get-CsTrunkConfiguration cmdlet.

Configure a Trunk with Media Bypass

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2013-02-24*

Follow these steps to configure a trunk with media bypass enabled. To configure a trunk with media bypass disabled, see Configure a Trunk without Media Bypass.

We strongly recommend that you enable media bypass. However, before you enable media bypass on a SIP trunk, confirm that your qualified SIP trunk provider supports media bypass and is able to accommodate the requirements for successfully enabling the scenario. Specifically, the provider must have the IP addresses of servers in your organization's internal network. If the provider cannot support this scenario, media bypass will not succeed. For details, see Planning for Media Bypass in the Planning documentation.

Note:

Media bypass will not interoperate with every public switched telephone network (PSTN) gateway, IP-PBX, and Session Border Controller (SBC). Microsoft has tested a set of PSTN gateways and SBCs with certified partners and has done some testing with Cisco IP-PBXs. Media bypass is supported only with products and versions that are listed on Unified Communications Open Interoperability Program – Lync Server at http://go.microsoft.com/fwlink/p/?linkId=214406.

A trunk configuration as described below groups a set of parameters that are applied to trunks assigned this trunk configuration. A particular trunk configuration can be scoped globally (to all trunks that do not have more specific site or pool configuration), or to a site, or to a pool. The pool-level trunk configuration is used to scope a specific trunk configuration to a single trunk.

To configure a trunk with media bypass

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
4. On the **Trunk Configuration** page, use one of the following methods to configure a trunk:
   - Double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
   - Click **New**, and then select a scope for the new trunk configuration:
     - **Site trunk:** Choose the site for this trunk configuration from **Select a Site**, and then click **OK**. Note that if a trunk configuration has already been created for a site, the site does not appear in **Select a Site**. This trunk configuration will be applied to all trunks in the site.
     - **Pool trunk:** Choose the name of the trunk that this trunk configuration applies to. This trunk can be the root trunk or any additional trunks defined in Topology Builder. From **Select a Service**, click **OK**. Note that if a trunk configuration has already been created for a specific trunk, the trunk does not appear in **Select a Service**.

> **Note:**
> After you select the scope of the trunk configuration, it cannot be changed. The **Name** field is prepopulated with the name of the trunk configuration's associated site or service and cannot be changed.

5. Specify a value in **Maximum early dialogs supported**. This is the maximum number of forked responses a public switched telephone network (PSTN) gateway, IP-PBX, or ITSP Session Border Controller (SBC) can receive to an INVITE that it sent to the Mediation Server. The default value is 20.

> **Note:**
> Before you change this value, consult your service provider or equipment manufacturer for details about the capabilities of your system.

6. Select one of the following **Encryption support level** options:
   - **Required:** Secure real-time transport protocol (SRTP) encryption must be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
   - **Optional:** SRTP encryption will be used if the service provider or equipment manufacturer supports it.
   - **Not Supported:** SRTP encryption is not supported by the service provider or equipment manufacturer and therefore will not be used.
7. Select the **Enable media bypass** check box if you want media to bypass the Mediation Server for processing by the trunk peer.

> **Important:**
> For media bypass to work successfully, the PSTN gateway, IP-PBX, or ITSP Session Border Controller must support certain capabilities. For details, see Planning for Media Bypass in the Planning documentation.

8. Select the **Centralized media processing** check box if there is a well-known media termination point (for example, a PSTN gateway where the media termination has the same IP as the signaling termination). Clear this check box if the trunk does not have a well-known media termination point.
9. If the trunk peer supports receiving SIP REFER requests from the Mediation Server, select the **Enable sending refer to the gateway** check box.

> **Note:**
> If you disable this option while the **Enable media bypass** option is selected, additional settings are required. If the trunk peer does not support receiving SIP REFER requests from the Mediation Server and media bypass is enabled, you must also run the **Set-CsTrunkConfiguration** cmdlet to disable RTCP for active and held calls in order to support proper conditions for media bypass. For details, see the Lync Server Management Shell documentation. Alternatively, you can select **Enable refer using third-party-call control** if you want transferred calls to be media bypassed, and the gateway does not support SIP REFER requests.

10. (Optional) To enable inter-trunk routing, associate and configure PSTN usage records to this trunk configuration. The PSTN usages associated to this trunk configuration will be applied for all incoming calls through the trunk that is not originating from a Lync endpoint. To manage PSTN usage records associated to a trunk configuration, use one of the following methods:
    - To select one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records you want to associate with this trunk configuration and then click **OK**.
    - To remove a PSTN usage record from this trunk configuration, select the record and click **Remove**.
    - To define a new PSTN usage record and associate it with this trunk configuration, do the following:
      - Click **New**.
      - In the **Name** field, specify a descriptive name for the record that is unique.

> **Note:**
> The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

  - Use one of the following methods to associate and configure routes for this PSTN usage record:
    - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
    - To remove a route from the PSTN usage record, select the route, and click **Remove**.
    - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
    - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
  - Click **OK**.
- To edit a PSTN usage record that is already associated with this trunk configuration, do the following:
  - Select the PSTN usage record you want to edit, and click **Show details**.
  - Use one of the following methods to associate and configure routes for this PSTN usage record:
    - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
    - To remove a route from the PSTN usage record, select the route, and click **Remove**.
    - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
    - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
  - Click **OK**.

> **Important:**
> It important to associate PSTN usage records according to the Mediation Server peer that is associated to the trunk being configured. If the Mediation Server peer is a PSTN gateway or a Session Border Controller (SBC), it is strongly recommended that the trunk configuration is not associated to a PSTN usage record that routes to a PSTN destination or any other downstream systems connected via Lync Server.

11. Arrange the PSTN usage records for optimum performance. To change a record’s position in the list, select the PSTN usage record, and click the up or down arrows.

> **Important:**
> The order in which PSTN usage records are listed in the trunk configuration is significant. Lync Server traverses the list from top to down.

12. **Enable RTP Latching** should be selected to enable bypass media for clients behind a network address translation (NAT) or firewall and an SBC that supports latching.
13. **Enable forward call history** should be selected to enable sending of call history information to the gateway peer of the Mediation Server.
14. **Enable forward P-Asserted-Identity data** should be selected to enable the P-Asserted-Identity (PAI) call originator information to be forwarded between the Mediation Server side and gateway side (and vice versa), when present.
15. **Enable outbound routing failover timer** should be selected to enable fast failover. The gateway associated with this trunk can give notification within 10 seconds that it is processing an outbound call. Rerouting to another trunk will occur if this notification is not received by the Mediation Server. On networks where latency may delay the response time or the gateway takes

longer than 10 seconds to respond, the fast failover should be disabled.

16.(Optional) Associate and configure **calling number translation rules** for the trunk. These translation rules apply to the calling number for outbound calls

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

> ⚠**Warning:**
>
> Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

17.(Optional) Associate and configure **called number translation rules** for the trunk. The translation rules apply to the called number in an outbound call.

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

> ⚠**Warning:**
>
> Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

18.Make sure that the trunk’s translation rules are arranged in the correct order. To change a rule’s position in the list, highlight the rule name and then click the up or down arrow.

> ◆**Important:**
>
> Lync Server 2013 traverses the translation rule list from the top down and uses the first rule that matches the dialed number. If you configure a trunk so that a dialed number can match more than one translation rule, be sure that the more restrictive rules are sorted above the less restrictive rules. For example, if you have included a translation rule that matches any 11-digit number and a translation rule that matches only 11-digit numbers that start with +1425, be sure that the rule that matches any 11-digit number is sorted *below* the more restrictive rule.

19.When you are finished configuring the trunk, click **OK**.

20. On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

Note:

Whenever you create or modify a trunk configuration, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

After you have configured the trunk, continue configuring media bypass by choosing between global media bypass options, as described in Global Media Bypass Options in the Deployment documentation.

Tasks

Configure a Trunk without Media Bypass

Concepts

Configure Media Bypass
Global Media Bypass Options

Other Resources

Defining Translation Rules

1.7.7.2.5 Configure a Trunk without Media Bypass

Configure a Trunk without Media Bypass

See Also

Deployment > Deploying Enterprise Voice > Configuring Trunks >

Topic Last Modified: *2013-02-24*

If you want to configure a trunk with media bypass disabled, follow these steps. If you want to configure a trunk with media bypass enabled, see Configure a Trunk with Media Bypass.

A trunk configuration, as described below, groups a set of parameters that are applied to trunks assigned this trunk configuration. A particular trunk configuration can be scoped globally (to all trunks that do not have more specific site or pool configuration), or to a site, or to a pool. The pool-level trunk configuration is used to scope a specific trunk configuration to a single trunk.

⊟To configure a trunk without media bypass

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Trunk Configuration**.
4. On the **Trunk Configuration** page, use one of the following methods to configure a trunk:
   - Double-click an existing trunk (for example, the **Global** trunk) to display the **Edit Trunk Configuration** dialog box.
   - Click **New**, and then select a scope for the new trunk configuration:
     - **Site trunk:** Choose the site for this trunk configuration in **Select a Site** , and then click **OK**. Note that if a trunk configuration has already been created for a site, the site does not appear in **Select a Site**. This trunk

configuration will be applied to all trunks in the site.
- **Pool trunk:** Choose the name of the trunk that this trunk configuration applies to in **Select a Service** and click **OK**. This trunk can be the root trunk, or any additional trunks defined in Topology Builder. Note that if a trunk configuration has already been created for a specific trunk, the trunk does not appear in **Select a Service**.

> **Note:**
> After you select the scope of the trunk configuration, it cannot be changed. The **Name** field is prepopulated with the name of the trunk configuration's associated site or service and cannot be changed.

5. Select one of the following **Encryption support level** options:
   - **Required:** Secure real-time transport protocol (SRTP) encryption must be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
   - **Optional:** SRTP encryption will be used if the service provider or equipment manufacturer supports it.
   - **Not Supported:** SRTP encryption is not supported by the service provider or equipment manufacturer and therefore will not be used.
6. Be sure that the **Enable media bypass** check box is cleared.
7. Select the **Centralized media processing** check box if there is a well-known media termination point (for example, a public switched telephone network (PSTN) gateway where the media termination has the same IP as the signaling termination). Clear this check box if the trunk does not have a well-known media termination point.
8. If the trunk peer supports receiving SIP REFER requests from the Mediation Server, select the **Enable sending refer to the gateway** check box.
9. (Optional) To enable inter-trunk routing, associate and configure PSTN usage records to this trunk configuration. The PSTN usages associated to this trunk configuration will be applied for all incoming calls through the trunk that is not originating from a Lync endpoint. To manage PSTN usage records associated to a trunk configuration, use one of the following methods:
   - To select one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records you want to associate with this trunk configuration and then click **OK**.
   - To remove a PSTN usage record from this trunk configuration, select the record and click **Remove**.
   - To define a new PSTN usage record and associate it with this trunk configuration, do the following:
     - Click **New**.
     - In the **Name** field, specify a descriptive name for the record that is unique.

       > **Note:**
       > The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

     - Use one of the following methods to associate and configure routes for this PSTN usage record:
       - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
       - To remove a route from the PSTN usage record, select the route, and click **Remove**.
       - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
       - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
     - Click **OK**.

- To edit a PSTN usage record that is already associated with this trunk configuration, do the following:
  - Select the PSTN usage record you want to edit, and click **Show details**.
  - Use one of the following methods to associate and configure routes for this PSTN usage record:
    - To select one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**. Highlight the routes you want to associate with this PSTN usage record, and click **OK**.
    - To remove a route from the PSTN usage record, select the route, and click **Remove**.
    - To define a new route and associate it to this PSTN usage record, click **New**. For details, see Create a Voice Route.
    - To edit a route that is associated with this PSTN usage record, select the route, and click **Show details**. For details, see Modify a Voice Route.
  - Click **OK**.

> ◆**Important:**
>
> It important to associate PSTN usage records according to the Mediation Server peer that is associated to the trunk being configured. If the Mediation Server peer is a PSTN gateway or a Session Border Controller (SBC), it is strongly recommended that the trunk configuration is not associated to a PSTN usage record that routes to a PSTN destination or any other downstream systems connected via Lync Server.

10.Arrange the PSTN usage records for optimum performance. To change a record’s position in the list, select the PSTN usage record, and click the up or down arrows.

> ◆**Important:**
>
> The order in which PSTN usage records are listed in the trunk configuration is significant. Lync Server traverses the list from top to down.

11.**Enable RTP Latching** should be selected to enable bypass media for clients behind a NAT or firewall and an SBC that supports latching.

12.**Enable forward call history** should be selected to enable sending of call history information to the gateway peer of the Mediation Server.

13.**Enable forward P-Asserted-Identity data** should be selected to enable PAI call originator information to be forwarded between the Mediation Server side and gateway side (and vice versa), when present.

14.**Enable outbound routing failover timer** should be selected to enable fast failover. The gateway associated with this trunk can give notification within 10 seconds that it is processing an outbound call. Rerouting to another trunk will occur if this notification is not received by the Mediation Server. On networks where latency may delay the response time or the gateway takes longer than 10 seconds to respond, the fast failover should be disabled.

15.(Optional) Associate and configure **calling number translation rules** for the trunk. These translation rules apply to the calling number for outbound calls

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

Security Note:

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

16.(Optional) Associate and configure **called number translation rules** for the trunk. The translation rules apply to the called number in an outbound call.

- To choose one or more rules from a list of all translation rules that are available in your Enterprise Voice deployment, click **Select**. In **Select Translation Rules**, click the rules that you want to associate with the trunk, and then click **OK**.
- To define a new translation rule and associate it with the trunk, click **New**. For details about defining a new rule, see Defining Translation Rules in the Deployment documentation.
- To edit a translation rule that is already associated with the trunk, click the rule name, and then click **Show details**. For details, see Defining Translation Rules in the Deployment documentation.
- To copy an existing translation rule to use as a starting point for defining a new rule, click the rule name and click **Copy**, and then click **Paste**. For details, see Defining Translation Rules.
- To remove a translation rule from the trunk, highlight the rule name and click **Remove**.

Caution:

Do not associate translation rules with a trunk if you have configured translation rules on the associated trunk peer, because the two rules might conflict.

17.Make sure that the trunk’s translation rules are arranged in the correct order. To change a rule’s position in the list, highlight the rule name, and then click the up or down arrow.

Important:

Lync Server traverses the translation rule list from the top down and uses the first rule that matches the dialed number. If you configure a trunk so that a dialed number can match more than one translation rule, be sure that the more restrictive rules are sorted above the less restrictive rules. For example, if you have included a translation rule that matches any 11-digit number and a translation rule that matches only 11-digit numbers that start with +1425, be sure that the rule that matches any 11-digit number is sorted *below* the more restrictive rule.

18.When you are finished configuring the trunk, click **OK**.

19.On the **Trunk Configuration** page, click **Commit**, and then click **Commit all**.

Note:

Whenever you create or modify a trunk configuration, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Configure a Trunk with Media Bypass

Other Resources

Defining Translation Rules

1.7.7.2.6 Create a New Collection of Trunk Configuration Settings

Create a New Collection of Trunk Configuration Settings

Operations > Managing Voice Routing > Configuring Trunks >

Topic Last Modified: *2012-11-01*

SIP trunk configuration settings define the relationship and capabilities between a Mediation Server and the public switched telephone network (PSTN) gateway, an IP-public branch exchange (PBX), or a Session Border Controller (SBC) at the service provider. These settings do such things as specify:

- Whether media bypass should be enabled on the trunks.
- The conditions under which real-time transport control protocol (RTCP) packets are sent.
- Whether or not secure real-time protocol (SRTP) encryption is required on each trunk.

When you install Microsoft Lync Server 2013, a global collection of SIP trunk configuration settings is created for you. In addition, administrators can create custom setting collections at the site scope or at the service scope (for the PSTN gateway service, only).

When creating SIP trunk configuration settings using Lync Server Control Panel, the following options are available to you:

UI Setting	PowerShell Parameter	Description
Name	Identity	Unique identifier for the collection. This property is read-only; you cannot change the Identity of a collection of trunk configuration settings.
Description	Description	Provides a way for administrators to store addition information about the settings (for example, the purpose of the trunk configuration).
Maximum early dialogs supported	MaxEarlyDialogs	The maximum number of forked responses a PSTN gateway, IP-PBX, or SBC at the service provider can receive to an Invite that it sent to the Mediation Server.
Encryption support level	SRTPMode	Indicates the level of support for protecting media traffic between the Mediation Server and the PSTN Gateway, IP-PBX, or SBC at the service provider. For media bypass cases, this value must be compatible with the EncryptionLevel setting in the media configuration. Media configuration is set by using the New-CsMediaConfiguration and Set-CsMediaConfiguration cmdlets. Allowed values are: • Required: SRTP encryption must be used. • Optional: SRTP will be used if the gateway supports it. • Not Supported: SRTP

		encryption is not supported and therefore will not be used. SRTPMode is used only if the gateway is configured to use Transport Layer Security (TLS). If the gateway is configured with Transmission Control Protocol (TCP) as the transport, SRTPMode is internally set to Not Supported.
Refer support	Enable3pccRefer EnableReferSupport	If set to **Enable sending refer to the gateway**, indicates that the trunk supports receiving Refer requests from the Mediation Server. If set to **Enable refer using third-party call control**, indicates that the 3pcc protocol can be used to allow transferred calls to bypass the hosted site. 3pcc is also known as "third party control," and occurs when a third-party is used to connect a pair of callers (for example, an operator placing a call from person A to person B).
Enable media bypass	EnableBypass	Indicates whether media bypass is enabled for this trunk. Media bypass can only be enabled if **Centralized media processing** is also enabled.
Centralized media processing	ConcentratedTopology	Indicates whether there is a well-known media termination point. (An example of a well-known media termination point would be a PSTN gateway where the media termination has the same IP as the signaling termination.)
Enable RTP latching	EnableRTPLatching	Indicates whether or not the SIP trunks support RTP latching. RTP latching is a technology that enables RTP/RTCP connectivity through a NAT (network address translator) device or firewall.
Enable forward call history	ForwardCallHistory	Indicates whether call history information will be forwarded through the trunk.
Enable forward P-Asserted-Identity data	ForwardPAI	Indicates whether the P-Asserted-Identity (PAI) header will be forwarded along with the call. The PAI header provides a way to verify the identity of the caller.
Enable outbound routing failover timer	EnableFastFailoverTimer	Indicates whether outbound calls that are not answered by the gateway within 10 seconds will be routed to

		the next available trunk; if there are no additional trunks then the call will automatically be dropped. In an organization with slow networks and gateway responses, that could potentially result in calls being dropped unnecessarily.
Associated PSTN usages	PSTNUsages	Collection of PSTN usages assigned to the trunk.
Translated number to test	N/A	Phone number that can be used to do an ad hoc test of the trunk configuration settings.
Associated translation rules	OutboundTranslationRulesList	Collection of phone number translation rules that apply to calls handled by Outbound Routing (calls routed to PBX or PSTN destinations).
Called number translation rules	OutboundCallingNumberTranslationRulesList	Collection of outbound calling number translation rules assigned to the trunk.
Phone number to test	N/A	Phone number that can be used to do an ad hoc test of the translation rules.
Calling number	N/A	Indicates that the phone number to test is the phone number of the caller.
Called number	N/A	Indicates that the phone number to test is the phone number of the person being called.

Note:

The Lync Server CsTrunkConfiguration cmdlets support additional properties not shown in Lync Server Control Panel. For more information, see the help topic for the New-CsTrunkConfiguration cmdlet.

To create new trunk configuration settings by using Lync Server Control Panel

1. In Lync Server Control Panel, click **Voice Routing**, and then click **Trunk Configuration**.
2. On the **Trunk Configuration** tab, click **New**, and then click **Site trunk** to create the new settings at the site scope, or **Pool trunk** to create the new settings at the service scope.
3. In the **Select a Site** or the **Select a Service** dialog box (the dialog box that appears will depend on whether you are creating site-scoped or service-scoped settings) select the location for the new configuration settings and then click **OK**. If the dialog box is blank, that means there is no place to create the new settings; for example, if the **Select a Site** dialog box is blank that means that all of your sites have already been assigned a collection of trunk configuration sites, and each site (and each service) can only host one such collection. In that case, you can either delete the existing collection and create a new collection, or simply modify the existing collection.
4. In the **New Trunk Configuration** dialog, make the appropriate selections and then click **OK**.
5. The **State** property for the collection will be updated to **Uncommitted**. To commit the changes, and to delete the collection, click **Commit** and then click **Commit All**.

6. In the **Uncommitted Voice Configuration Settings** dialog box, click **OK**.

7. In the **Microsoft Lync Server 2013 Control Panel** dialog box click **OK**.

1.7.7.2.7 Delete an Existing Collection of SIP Trunk Configuration Settings

Delete an Existing Collection of SIP Trunk Configuration Settings

Operations > Managing Voice Routing > Configuring Trunks >

Topic Last Modified: *2013-02-22*

SIP trunk configuration settings define the relationship and capabilities between a Mediation Server and the public switched telephone network (PSTN) gateway, an IP-public branch exchange (PBX), or a Session Border Controller (SBC) at the service provider. These settings do such things as specify:

- Whether media bypass should be enabled on the trunks.
- The conditions under which real-time transport control protocol (RTCP) packets are sent.
- Whether or not secure real-time protocol (SRTP) encryption is required on each trunk.

When you install Microsoft Lync Server 2013, a global collection of SIP trunk configuration settings is created for you. This global collection of settings cannot be deleted. However, you can use the Lync Server Control Panel or the Remove-CsTrunkConfiguration cmdlet to "reset" the properties in the global collection to their default values. For example, if you have set the Enable3pccRefer property to True, when you reset the global collection the Enable3pccRefer property will revert to its default value of False.

Administrators can also create custom trunk configuration settings at the site scope or at the service scope (for an individual PSTN gateway); these custom settings can be removed. When removing these custom settings keep the following in mind:

- If you remove service scope settings, then the SIP trunk managed by those settings will be managed by the settings applied to their site, if they exist. If site settings do not exist, those trunks will then be managed by the global collection of trunk configuration settings.
- If you remove site-scoped settings then any SIP trunks managed by those settings will now be managed by the global collection of trunk configuration settings.

⊟To remove trunk configuration settings with Lync Server Control Panel

1. In Lync Server Control Panel, click **Voice Routing** and then click **Trunk Configuration**.
2. On the **Trunk Configuration** tab, select the collection of SIP trunk configuration settings to be deleted, click **Edit** and then click **Delete**. To delete multiple collections in the same operation, click the first collection to be deleted, then hold down the Ctrl key and click any additional collections that you want to remove.
3. The **State** property for the collection will be updated to **Uncommitted**. To commit the changes, and to delete the collection, click **Commit** and then click **Commit All**.
4. In the **Uncommitted Voice Configuration Settings** dialog box, click **OK**.
5. In the **Microsoft Lync Server 2013 Control Panel** dialog box click **OK**.
6. If you change your mind and decide not to delete the collection, click **Commit** and then click **Cancel All Uncommitted Changes**. When the **Microsoft Lync Server 2013 Control Panel** dialog box appears, click **OK**.

Removing Trunk Configuration Settings by Using Windows PowerShell Cmdlets

You can delete trunk configuration settings by using Windows PowerShell and the **Remove-CsTrunkConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specified collection of settings

- The following command removes the trunk configuration settings applied to the Redmond site:

```
Remove-CsTrunkConfiguration -Identity site:Redmond
```

To remove all the collections applied to the site scope

- This command removes all the trunk configuration settings applied to the service scope:

```
Get-CsTrunkConfiguration -Filter "service:*" | Remove-CsTrunkConfigurat
```

To remove all the collections where media bypass is enabled

- The following command removes all the trunk configuration settings where media bypass has been enabled:

```
Get-CsTrunkConfiguration | Where-Object {$_.EnableBypass -eq $True} | R
```

For more information, see the help topic for the Remove-CsTrunkConfiguration cmdlet.

1.7.7.2.8 Modify SIP Trunk Configuration Settings

Modify SIP Trunk Configuration Settings

Operations > Managing Voice Routing > Configuring Trunks >

***Topic Last Modified:** 2013-02-22*

SIP trunk configuration settings define the relationship and capabilities between a Mediation Server and the public switched telephone network (PSTN) gateway, an IP-public branch exchange (PBX), or a Session Border Controller (SBC) at the service provider. These settings do such things as specify:

- Whether media bypass should be enabled on the trunks.
- The conditions under which real-time transport control protocol (RTCP) packets are sent.
- Whether or not secure real-time protocol (SRTP) encryption is required on each trunk.

When you install Microsoft Lync Server 2013, a global collection of SIP trunk configuration settings is created for you. In addition, administrators can create custom setting collections at the site scope or at the service scope (for the PSTN gateway service, only). Any of these collections can later be modified using either Lync Server Control Panel or Windows PowerShell.

When modifying SIP trunk configuration settings using Lync Server Control Panel, the following options are available to you:

UI Setting	PowerShell Parameter	Description
Name	Identity	Unique identifier for the collection. This property is read-only; you cannot change the Identity of a collection of trunk configuration settings.
Description	Description	Provides a way for administrators to store addition information about the settings (for example, the purpose of the trunk configuration).
Maximum early dialogs supported	MaxEarlyDialogs	The maximum number of forked responses a PSTN gateway, IP-PBX, or SBC at the service provider can receive to an Invite that it sent to the Mediation Server.
Encryption support level	SRTPMode	Indicates the level of support for protecting media traffic between the Mediation Server and the PSTN Gateway, IP-PBX, or SBC at the service provider. For media bypass cases, this value must be compatible with the EncryptionLevel setting in the media configuration. Media configuration is set by using the New-CsMediaConfiguration and Set-CsMediaConfiguration cmdlets. Allowed values are: • Required: SRTP encryption must be used. • Optional: SRTP will be used if the gateway supports it. • Not Supported: SRTP encryption is not supported and therefore will not be used. SRTPMode is used only if the gateway is configured to use Transport Layer Security (TLS). If the gateway is configured with Transmission Control Protocol (TCP) as the transport, SRTPMode is internally set to Not Supported.
Refer support	Enable3pccRefer EnableReferSupport	If set to **Enable sending refer to the gateway**, indicates that the trunk supports receiving Refer requests from the Mediation Server. If set to **Enable refer using third-party call control**, indicates that the 3pcc protocol can be used to allow transferred calls to bypass the hosted site. 3pcc is also known as "third party control," and occurs when a third-

		party is used to connect a pair of callers (for example, an operator placing a call from person A to person B).
Enable media bypass	EnableBypass	Indicates whether media bypass is enabled for this trunk. Media bypass can only be enabled if **Centralized media processing** is also enabled.
Centralized media processing	ConcentratedTopology	Indicates whether there is a well-known media termination point. (An example of a well-known media termination point would be a PSTN gateway where the media termination has the same IP as the signaling termination.)
Enable RTP latching	EnableRTPLatching	Indicates whether or not the SIP trunks support RTP latching. RTP latching is a technology that enables RTP/RTCP connectivity through a NAT (network address translator) device or firewall.
Enable forward call history	ForwardCallHistory	Indicates whether call history information will be forwarded through the trunk.
Enable forward P-Asserted-Identity data	ForwardPAI	Indicates whether the P-Asserted-Identity (PAI) header will be forwarded along with the call. The PAI header provides a way to verify the identity of the caller.
Enable outbound routing failover timer	EnableFastFailoverTimer	Indicates whether outbound calls that are not answered by the gateway within 10 seconds will be routed to the next available trunk; if there are no additional trunks then the call will automatically be dropped. In an organization with slow networks and gateway responses, that could potentially result in calls being dropped unnecessarily.
Associated PSTN usages	PSTNUsages	Collection of PSTN usages assigned to the trunk.
Translated number to test	N/A	Phone number that can be used to do an ad hoc test of the trunk configuration settings.
Associated translation rules	OutboundTranslationRulesList	Collection of phone number translation rules that apply to calls handled by Outbound Routing (calls routed to PBX or PSTN destinations).
Called number translation rules	OutboundCallingNumberTranslationRulesList	Collection of outbound calling number translation rules assigned to the

		trunk.
Phone number to test	N/A	Phone number that can be used to do an ad hoc test of the translation rules.
Calling number	N/A	Indicates that the phone number to test is the phone number of the caller.
Called number	N/A	Indicates that the phone number to test is the phone number of the person being called.

Note:
The Lync Server CsTrunkConfiguration cmdlets support additional properties not shown in Lync Server Control Panel. For more information, see the help topic for the Set-CsTrunkConfiguration cmdlet.

To modify SIP trunk configuration settings by using Lync Server Control Panel

1. In Lync Server Control Panel, click **Voice Routing**, and then click **Trunk Configuration**.
2. On the **Trunk Configuration** tab, double-click the trunk configuration settings to be modified. Note that you can only edit one collection of settings at a time. If you would like to make the same changes on multiple collections, use Windows PowerShell instead.
3. In the **Edit Trunk Configuration** dialog, make the appropriate selections and then click **OK**.
4. The **State** property for the collection will be updated to **Uncommitted**. To commit the changes, and to delete the collection, click **Commit** and then click **Commit All**.
5. In the **Uncommitted Voice Configuration Settings** dialog box, click **OK**.
6. In the **Microsoft Lync Server 2013 Control Panel** dialog box click **OK**.

1.7.7.2.9 Test SIP Trunk Configuration Settings

Test SIP Trunk Configuration Settings

Operations > Managing Voice Routing > Configuring Trunks >

Topic Last Modified: *2012-11-01*

SIP trunk configuration settings define the relationship and capabilities between a Mediation Server and the public switched telephone network (PSTN) gateway, an IP-public branch exchange (PBX), or a Session Border Controller (SBC) at the service provider. These settings do such things as specify:

- Whether media bypass should be enabled on the trunks.
- The conditions under which real-time transport control protocol (RTCP) packets are sent.
- Whether or not secure real-time protocol (SRTP) encryption is required on each trunk.

When you install Microsoft Lync Server 2013, a global collection of SIP trunk configuration settings is created for you. In addition, administrators can create custom setting collections at the site scope or at the service scope (for the PSTN gateway service, only). Administrators can also use the Test-CsTrunkConfiguration cmdlet to verify that a trunk can convert a number as dialed by a user to a number that can be handled by the gateway.

Trunk configuration settings can only be tested by using Windows PowerShell and the Test-CsTrunkConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To test SIP trunk configuration settings

- This command verifies that the trunk configuration settings for the Redmond site can correctly convert the dialed number 4255551212.

```
$trunk = Get-CsTrunkConfiguration -Identity "site:Redmond"
Test-CsTrunkConfiguration -DialedNumber 4255551212 -TrunkConfiguration
```

1.7.7.2.10 View Information about Individual SIP Trunks

View Information about Individual SIP Trunks

Operations > Managing Voice Routing > Configuring Trunks >

Topic Last Modified: *2013-02-21*

SIP trunks are used to connect Lync Server 2013 Voice over IP phone network with the Public Switched Telephone Network. In previous version of the product, trunks were used to route outbound calls from a Mediation Server to a PSTN gateway and each gateway was limited to a single trunk. As a result, a PSTN gateway and a SIP trunk were essentially identical. For administrators, that meant they could view information about an individual SIP trunk simply by viewing information about the associated PSTN gateway.

In Lync Server 2013, however, multiple trunks can now be assigned to a single PSTN gateway; this means that gateways and trunks are no longer one and the same. In turn, that means that administrators must use the new Get-CsTrunk cmdlet in order to view information about an individual SIP trunk.

The Get-CsTrunk cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view information for all your SIP trunks

- The following command returns information about all the SIP trunks in use in your organization:

```
Get-CsTrunk
```

To view information for a specific SIP trunk

- This command returns information only for the SIP trunk with the Identity PstnGateway:192.168.0.240:

```
Get-CsTrunk -Identity "PstnGateway:192.168.0.240"
```

Viewing Information for All the SIP Trunks Assigned to a Pool

- In this example, information is returned for all the SIP trunks assigned to the pool atl-cs-001.litwareinc.com:

```
Get-CsTrunk -PoolFqdn "atl-cs-001.litwareinc.com"
```

1.7.7.3 Configuring Voice Policies, PSTN Usage Records, and Voice Routes

Configuring Voice Policies, PSTN Usage Records, and Voice Routes

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-10-10*

Voice policies, PSTN usage records, and voice routes are integrally related. You configure voice policies by selecting a set of calling features and then assigning the policy a set of PSTN usage records, which specify what rights are authorized for the users or groups who are assigned the voice policy. Voice routes are also assigned PSTN usage records, which serve to match routes with the users who are authorized to use them. That is, users can only place calls that use the routes for which they have a matching PSTN usage record.

The recommended workflow for a new Enterprise Voice deployment is to start by configuring a voice policy that includes the appropriate PSTN usage records, and then associate the appropriate routes to each PSTN usage record.

Note:

You can also create voice policies with *user* scope and assign them to individual users or groups.

For the detailed steps to perform each of these tasks, see the procedures in this section.

- Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges
- View PSTN Usage Records
- Configuring Voice Routes for Outbound Calls
- Exporting and Importing Voice Routing Configuration
- Publish Pending Changes to the Voice Routing Configuration
- Test Voice Routing

1.7.7.3.1 Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges

Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges

Deployment > Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes >

Topic Last Modified: *2012-10-10*

A *voice policy* enables a set of calling features and associates one or more PSTN usage records to define the calling features and permissions of users who are assigned the policy.

Voice policy scope can be either *Site* (which defines the default features and permissions for a network site) or *User* (which defines the features and permissions to be assigned on a per-user or group basis). Users not assigned to a voice policy will automatically be assigned to the global policy, which is the default voice policy that is installed with the product.

Note:

For details, see Voice Policies in the Planning documentation.

- Create a Voice Policy and Configure PSTN Usage Records
- Modify a Voice Policy and Configure PSTN Usage Records
- Configuring Voice Mail Escape

1.7.7.3.1.1 Create a Voice Policy and Configure PSTN Usage Records

Create a Voice Policy and Configure PSTN Usage Records

See Also

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges >

Topic Last Modified: *2012-11-01*

Follow these steps if you want to create a new voice policy. If you want to edit a voice policy, see Modify a Voice Policy and Configure PSTN Usage Records for the procedure.

Note:

Each voice policy must have at least one associated public switched telephone network (PSTN) usage record. To see a listing of all PSTN usage records available in your Enterprise Voice deployment and view their properties, see View PSTN Usage Records.

⊟To create a voice policy

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Voice Policy**.
4. On the **Voice Policy** page, click **New** and then select a scope for the new policy:
   - **Site policy** applies to an entire site, except any users or groups that are assigned to a user policy. If you select Site for a policy scope, choose the site from the **Select a Site** dialog box. If a voice policy has already been created for a site, the site does not appear in the **Select a Site** dialog box.
   - **User policy** can be applied to specified users or groups.
5. If the voice policy scope is User, enter a descriptive name for the policy in the **Name** field.

   Note:

   If the voice policy scope is Site, the **Name** field in **New Voice Policy** is prepopulated with the site name and cannot be changed.
6. (Optional) Enter additional descriptive information for the voice policy.
7. Select or clear the following check boxes to enable or disable each of the **Calling features** for this voice policy:
   - **Voice mail escape** prevents calls from being immediately routed to the user’s mobile phone voice mail system when simultaneous ringing is configured and the phone is turned off, out of battery, or out of range.

     Note:

     This feature is only configurable through the Lync Server Management Shell
   - **Call forwarding** enables users to forward calls to other phones and client devices. Lync Server 2013 provides a significantly wider range of configuration options for call forwarding. For example, if an organization does not want to allow incoming calls to be forwarded externally to the

PSTN, an administrator can apply a special voice policy to deploy this restriction. Enabled by default.

- **Delegation** enables users to specify other users to send and receive calls on their behalf. In Lync Server 2013, a delegate can configure simultaneous ringing that enables incoming calls to his or her manager to ring all of the delegate’s simultaneous ringing targets. This provides the delegate with greater flexibility in responding to calls directed to the manager. Enabled by default.
- **Call transfer** enables users to transfer calls to other users. Enabled by default.
- **Call park** enables users to park calls on hold and then pick up the call from a different phone or client. Disabled by default.
- **Simultaneous ringing** enables incoming calls to ring on additional phones (for example, a mobile phone) or other endpoint devices. Lync Server 2013 provides a significantly wider range of configuration options for simultaneous ringing. Enabled by default.
- **Team call** enables users on a defined team to answer calls for other members of the team. Enabled by default.
- **PSTN re-route** enables calls made by users who are assigned this policy to other enterprise users to be rerouted on the public switched telephone network (PSTN) if the WAN is congested or unavailable. Enabled by default.
- **Bandwidth policy override** enables administrators to override call admission control policy decisions for a particular user. Disabled by default.

> **Note:**
> The policy will be overridden only for incoming calls to the user and not for outgoing calls that are placed by the user. After the session is established, the bandwidth consumption will be accurately recorded. This setting should be used sparingly and should be reserved for appropriate call admission control decisions.

- **Malicious call tracing** enables users to report malicious calls (such as bomb threats) by using the client UI, which in turn flags the calls in the call detail records (CDRs). Disabled by default.

8.To associate and configure PSTN usage records for this voice policy, do any of the following:

- To choose one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records that you want to associate with this voice policy, and then click **OK**.
- To remove a PSTN usage record from this voice policy, highlight the record and click **Remove**.
- To define a new PSTN usage record and associate it with this voice policy, do the following:

  8..a.Click **New**.

  8..b.In the **Name** field, enter a unique descriptive name for the record. For example, you may want to create a PSTN usage record named **Redmond** for full-time employees located in Redmond, and another named **RedmondTemps** for temporary employees.

  > **Note:**
  > The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

  8..c.Use any of the following methods to associate and configure routes for this PSTN usage record:

  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from the PSTN usage record, highlight the route, and then click **Remove**.

- To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
- To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.

8..d.Click **OK**.

- To edit a PSTN usage record that is already associated with this voice policy, do the following:

  8..a.Highlight the PSTN usage record that you want to edit, and then click **Show details**.

  8..b.Use any of the following methods to associate and configure routes for this PSTN usage record:

  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from this PSTN usage record, highlight the route, and then click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route and lick **Show details**. For details, see Modify a Voice Route.

  8..c.Click **OK**.

9.Arrange the PSTN usage records for optimum performance. To change a record's position in the list, highlight the record name and click the up or down arrow.

> **Important:**
> The order in which PSTN usage records are listed in the voice policy is significant. Lync Server traverses the list from the top down. We recommend that you organize the list by frequency of use, for example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup.

10.To associate and configure PSTN usage records for call forwarding and simultaneous ringing in this voice policy, do any of the following:

- To use the same PSTN usage records for call forwarding and simultaneous ringing as this voice policy, select the option **Route using the call PSTN usages** from the drop-down menu.
- To allow call forwarding and simultaneous ringing to internal Lync users only, select the option **Route to internal Lync users only** from the drop-down menu. Calls will not be forwarded to external PSTN numbers.
- To specify different PSTN usage records for call forwarding and simultaneous ringing than used for this voice policy, select the option **Route using custom PSTN usages** from the drop-down menu. This option displays a control to select existing PSTN usage records or create new PSTN usage records specifically for call forwarding and simultaneous ringing.

  10..a.To choose one or more records from a list of PSTN usage records for call forwarding and simultaneous ringing, click **Select**. Highlight the records that you want to associate with this call forwarding and simultaneous ringing policy, and then click **OK**.

  10..b.To remove a PSTN usage record from this call forwarding and simultaneous ringing policy, highlight the record and click **Remove**.

  10..c.To define a new PSTN usage record and associate it with this call forwarding and simultaneous ringing policy, do the following:

  - Click **New**.
  - In the **Name** field, enter a unique descriptive name for the record.

> **Note:**
> The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved,

the **Name** field cannot be edited.

- Use any of the following methods to associate and configure routes for this PSTN usage record:
  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from the PSTN usage record, highlight the route and click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.
- Click **OK**.

10..d.To edit a PSTN usage record that is already associated with this voice policy, do the following:

- Highlight the PSTN usage record you want to edit and click **Show details**.
- Use any of the following methods to associate and configure routes for this PSTN usage record:
  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from this PSTN usage record, highlight the route and click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.
- Click **OK**.

11.(Optional) Enter a number to test the voice policy and click **Go**. The test results are displayed under **Translated number to test**.

> **Note:**
> You can save a voice policy that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

12.Click **OK**.

13.On the **Voice Policy** page, click **Commit**, and then click **Commit all**.

> **Note:**
> Any time you create or modify a voice policy, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

14.(Optional) Voicemail Escape detects that a call was immediately answered by the user's mobile phone voice mail, and disconnects the call to the mobile phone voice mail. This allows the call to continue to ring on the user's other endpoints giving the user the opportunity to answer the call. For details on how to configure a voice mail policy, see Configuring Voice Mail Escape.

Tasks

Modify a Voice Policy and Configure PSTN Usage Records
View PSTN Usage Records
Create a Voice Route
Modify a Voice Route
Publish Pending Changes to the Voice Routing Configuration

Configuring Voice Mail Escape

Other Resources

Test Voice Routing

1.7.7.3.1.2 Modify a Voice Policy and Configure PSTN Usage Records

Modify a Voice Policy and Configure PSTN Usage Records

See Also

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges >

Topic Last Modified: *2012-11-01*

Follow these steps if you want to modify a voice policy. If you want to create a new voice policy, see Create a Voice Policy and Configure PSTN Usage Records for the procedure.

> **Note:**
> If a user is assigned to a voice policy has no associated public switched telephone network (PSTN) usage records, the user cannot place outbound calls. For a listing of all PSTN usage records available in your Enterprise Voice deployment and view their properties, see View PSTN Usage Records.

⊟To modify a voice policy

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Voice Policy**.
4. On the **Voice Policy** page, double-click a voice policy name.

   > **Note:**
   > The scope and name were set when the voice policy was created. They cannot be changed.

5. (Optional) In **Edit Voice Policy**, enter additional descriptive information for the voice policy.
6. Select or clear the following check boxes to enable or disable each of the **Calling features**:
   - **Voice mail escape** prevents calls from being immediately routed to the user's mobile phone voice mail system when simultaneous ringing is configured and the phone is turned off, out of battery, or out of range.

     > **Note:**
     > This feature is only configurable through the Lync Server Management Shell

   - **Call forwarding** enables users to forward calls to other phones and client devices. Lync Server 2013 provides a significantly wider range of configuration options for call forwarding. For example, if an organization does not want to allow incoming calls to be forwarded externally to the PSTN, an administrator can apply a special voice policy to deploy this restriction. Enabled by default.
   - **Delegation** enables users to specify other users to send and receive calls on their behalf. In Lync Server 2013, a delegate can configure simultaneous ringing that enables incoming calls to his or her manager to ring all of the delegate's simultaneous ringing targets. This provides the delegate with

greater flexibility in responding to calls directed to the manager. Enabled by default.

- **Call transfer** enables users to transfer calls to other users. Enabled by default.
- **Call park** enables users to park calls on hold, and then pick up the call from a different phone or client. Disabled by default.
- **Simultaneous ringing** enables incoming calls to ring on additional phones (for example, a mobile phone) or other endpoint devices. Lync Server 2013 provides a significantly wider range of configuration options for simultaneous ringing. Enabled by default.
- **Team call** enables users on a defined team to answer calls for other members of the team. Enabled by default.
- **PSTN re-route** enables calls made by users who are assigned this policy to other enterprise users to be rerouted on the public switched telephone network (PSTN) if the WAN is congested or unavailable. Enabled by default.
- **Bandwidth policy override** enables administrators to override call admission control (CAC) policy decisions for a particular user. Disabled by default.

  > **Note:**
  > The policy will be overridden only for incoming calls to the user and not for outgoing calls that are placed by the user. After the session is established, the bandwidth consumption will be accurately recorded. This setting should be used sparingly.

- **Malicious call tracing** enables users to report malicious calls (such as bomb threats) using the client UI, which in turn flags the calls in the call detail records (CDRs). Disabled by default.

7.To associate and configure PSTN usage records for this voice policy, do any of the following:

- To choose one or more records from a list of all PSTN usage records available in your Enterprise Voice deployment, click **Select**. Highlight the records that you want to associate with this voice policy, and then click **OK**.
- To remove a PSTN usage record from this voice policy, highlight the record and click **Remove**.
- To define a new PSTN usage record and associate it with this voice policy, do the following:

  7..a.Click **New**.

  7..b.In the **Name** field, enter a unique descriptive name for the record. For example, you may want to create a PSTN usage record named **Redmond** for full-time employees located in Redmond, and another record named **RedmondTemps** for temporary employees.

  > **Note:**
  > The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

  7..c.Use any of the following methods to associate and configure routes for this PSTN usage record:

  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from the PSTN usage record, highlight the route and click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.

  7..d.Click **OK**.

- To edit a PSTN usage record that is already associated with this voice policy, do the following:
  7..a.Highlight the PSTN usage record that you want to edit and click **Show details**.
  7..b.Use any of the following methods to associate and configure routes for this PSTN usage record:
  - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes that you want to associate with this PSTN usage record, and then click **OK**.
  - To remove a route from this PSTN usage record, highlight the route and click **Remove**.
  - To define a new route and associate it with this PSTN usage record, click **New**. For details, see Create a Voice Route.
  - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see Modify a Voice Route.

  7..c.Click **OK**.

8.Arrange the PSTN usage records for optimum performance. To change a record's position in the list, highlight the record name and click the up or down arrow.

> **Note:**
> The order in which PSTN usage records are listed in the voice policy is significant. Lync Server traverses the list from the top down. We recommend that you organize the list by frequency of use, for example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup.

9.To associate and configure PSTN usage records for call forwarding and simultaneous ringing in this voice policy, do any of the following:

- To use the same PSTN usage records for call forwarding and simultaneous ringing as this voice policy, select the option **Route using the call PSTN usages** from the drop-down menu.
- To allow call forwarding and simultaneous ringing to internal Lync users only, select **Route to internal Lync users only** from the drop-down menu. Calls will not be forwarded to external PSTN numbers.
- To specify different PSTN usage records for call forwarding and simultaneous ringing than those used for this voice policy, select the option **Route using custom PSTN usages** from the drop-down menu. This option displays a control to select existing PSTN usage records or to create new PSTN usage records, specifically for call forwarding and simultaneous ringing.
  9..a.To choose one or more records from a list of PSTN usage records for call forwarding and simultaneous ringing, click **Select**. Highlight the records that you want to associate with this call forwarding and simultaneous ringing policy, and then click **OK**.
  9..b.To remove a PSTN usage record from this call forwarding and simultaneous ringing policy, highlight the record and click **Remove**.
  9..c.To define a new PSTN usage record and associate it with this call forwarding and simultaneous ringing policy, do the following:
  - Click **New**.
  - In the **Name** field, enter a unique descriptive name for the record.

    > **Note:**
    > The PSTN usage record name must be unique within the Enterprise Voice deployment. After the record is saved, the **Name** field cannot be edited.

  - Use any of the following methods to associate and configure routes for this PSTN usage record:
    - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes

    that you want to associate with this PSTN usage record, and then click **OK**.
    - To remove a route from the PSTN usage record, highlight the route and click **Remove**.
    - To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create a Voice Route].
    - To edit a route that is already associated with this PSTN usage record, highlight the route, and then click **Show details**. For details, see [Modify a Voice Route].
  - Click **OK**.

9..d.To edit a PSTN usage record that is already associated with this voice policy, do the following:

  - Highlight the PSTN usage record that you want to edit and click **Show details**.
  - Use any of the following methods to associate and configure routes for this PSTN usage record:
    - To choose one or more routes from the list of all available routes in your Enterprise Voice deployment, click **Select**, highlight the routes you want to associate with this PSTN usage record, and then click **OK**.
    - To remove a route from this PSTN usage record, highlight the route and click **Remove**.
    - To define a new route and associate it with this PSTN usage record, click **New**. For details, see [Create a Voice Route].
    - To edit a route that is already associated with this PSTN usage record, highlight the route and click **Show details**. For details, see [Modify a Voice Route].
  - Click **OK**.

10. (Optional) Enter a number to test the voice policy and click **Go**. The test results are displayed under **Translated number to test**.

> **Note:**
> You can save a voice policy that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

11. Click **OK**.
12. On the **Voice Policy** page, click **Commit**, and then click **Commit all**.

> **Note:**
> Whenever you create or modify a voice policy, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

13. (Optional) Voicemail Escape detects that a call was immediately answered by the user’s mobile phone voice mail, and disconnects the call to the mobile phone voice mail. This allows the call to continue to ring on the user’s other endpoints giving the user the opportunity to answer the call. For details about how to configure a voice mail policy, see Configuring Voice Mail Escape.

Tasks

Create a Voice Policy and Configure PSTN Usage Records
View PSTN Usage Records
Create a Voice Route
Modify a Voice Route
Publish Pending Changes to the Voice Routing Configuration
Configuring Voice Mail Escape

Other Resources

Test Voice Routing

1.7.7.3.1.3 Configuring Voice Mail Escape

Configuring Voice Mail Escape

See Also Example

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges >

Topic Last Modified: *2013-02-22*

When a user configures simultaneous ringing to a mobile phone, a caller will typically be routed to the user's personal voice mail if the mobile phone is turned off, out of battery power, or out of range. With Lync Server 2013, users can opt to have business-related calls routed to their corporate voice mail system. Specifically, a timer can be configured, and if the call is answered by the carrier's voice mail within the range of time defined, Lync Server will disconnect from the carrier's voice mail system (and the user's personal voice mail), while the user's remaining endpoints in the corporate system continue to ring. This way, the caller is automatically routed to the user's corporate voice mail.

This configuration is performed using the Lync Server Management Shell cmdlet, **Set-CsVoicePolicy**, at the voice policy level, with the following parameters.

⊟To configure voice mail escape

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Specify the following parameters to **Set-CsVoicePolicy**:
   - **EnableVoicemailEscapeTimer** - Enables or disables the escape timer.
   - **PSTNVoicemailEscapeTimer** - Specifies the timeout value in milliseconds. The default value is 1500 milliseconds, and the value can range from 0 milliseconds to 8000 milliseconds.

```
Set-CsVoicePolicy UserVoicePolicy -EnableVoiceMailEscapeTimer $true - PSTNVoicema
Set-CsVoicePolicy -Identity site:SitePolicy -EnableVoiceMailEscapeTimer $true -PS
```

⊟See Also

Other Resources

Configuring Voice Policies and PSTN Usage Records to Authorize Calling Features and Privileges

1.7.7.3.2 View PSTN Usage Records

View PSTN Usage Records

See Also

Deployment > Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes >

Topic Last Modified: *2013-02-22*

A public switched telephone network (PSTN) usage record specifies a class of call (such as internal, local, or long distance) that can be made by various users or groups of users in an organization. For details, see PSTN Usage Records in the Planning documentation.

⊟To view a PSTN usage record by using Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **PSTN Usage**.
4. On the **PSTN Usage** page, highlight the PSTN usage record you want to view, click **Edit** and then click **Show details**.

> **Note:**
>
> A read-only page of the selected PSTN usage record shows the associated routes and associated voice policies.

Viewing PSTN Usage Information by Using Windows PowerShell Cmdlets

You can also view PSTN usages by using Windows PowerShell and the **Get-CsPstnUsage** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view PSTN usage information by using Windows PowerShell cmdlets

- To view information about all of your PSTN usages, type the following command in the Lync Server Management Shell, and then press ENTER:

```
Get-CsPstnUsage
```

This command returns information similar to the following:

```
Identity : Global
Usage    : {Internal, Local, Long Distance}
```

For details, see Get-CsPstnUsage.

See Also

Tasks

Create a Voice Policy and Configure PSTN Usage Records
Modify a Voice Policy and Configure PSTN Usage Records

1.7.7.3.3 Configuring Voice Routes for Outbound Calls

Configuring Voice Routes for Outbound Calls

See Also

Deployment > Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes >

***Topic Last Modified:** 2012-11-01*

A Lync Server 2013 voice route associates destination phone numbers with one or more public switched telephone network (PSTN) gateways or SIP trunks and one or more PSTN usage records.

To view voice routes by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. Click **Voice Routing**.

3. Click **Route**.
4. Double-click a voice route to view additional properties from the list of voice routes, or select the route and click **Edit**. Then click **Show details**.

Note:
You can only view detailed information for a single route at a time.

To view voice routes by using Windows PowerShell

- Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
  Voice routes can be viewed by using Windows PowerShell and the **Get-CsVoiceRoute** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.
  To view information about all of your voice routes, type the following command in the Lync Server Management Shell, and then press ENTER:

```
Get-CsVoiceRoute
```

  That will return information similar to this:

```
Identity            : global
Priority            : -1
Description         :
NumberPattern       : ^(\+1[0-9]{10})$
PstnUsages          : {}
PstnGatewayList     : {}
Name                : global
SuppressCallerId    :
AlternateCallerId   :
```

Note:
For details, see Voice Routes in the Planning documentation.

- Create a Voice Route
- Modify a Voice Route

See Also

Other Resources

Managing Voice Routing

1.7.7.3.3.1 Create a Voice Route

Create a Voice Route

See Also

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Routes for Outbound Calls >

Topic Last Modified: *2012-11-01*

The following procedure explains how to create a new voice route by using the Lync Server 2013 Control Panel. To edit an existing route, see Modify a Voice Route for the procedure.

To create a voice route by using the Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the **CsVoiceAdministrator**, **CsServerAdministrator**, or **CsAdministrator** administrative role.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to

start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Voice Routing**.
4. Click **Route**.
5. Click **New** to display the **New Voice Route** dialog box.
6. In **Name**, type a descriptive name for the voice route.
7. (Optional) In **Description**, type additional descriptive information for the voice route.
8. To specify the patterns that you want this route to accommodate, you can either use the **Build a pattern to match** tool to generate a regular expression, or write the regular expression manually.
   - To use the **Build a pattern to match** tool to generate a regular expression, enter values as follows. You can specify two types of pattern matching:
     - **Starting digits for numbers that you want to allow:** Enter prefix values that this route must accommodate (including the leading + if needed). For example, type **+425**, and then click **Add**. Repeat this for each prefix value that you want to include in the route.
     - **Exceptions:** If you want to specify one or more exceptions for a prefix value, highlight the prefix and click **Exceptions**. Type in one or more values for the matching patterns that you do *not* want this route to accommodate. For example, to exclude numbers starting with +425237 from the route, enter a value of **+425237** in the **Exceptions** field, and then click **OK**.
   - To define the matching pattern manually, click **Edit** in the **Build a pattern to match** tool and then type in a .NET Framework regular expression to specify the matching pattern for destination phone numbers to which the route is applied. For details about how to write regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.
9. Select **Suppress caller ID** if you do not want the ID of the phone making the outbound call to appear to the call recipient. If you select this option, you must specify an **Alternate caller ID** that will appear on the recipient's caller ID display.
10. To associate one or more trunks with the voice route, click **Add** and then select a trunk from the list.

Note:
If your deployment includes any Microsoft Office Communications Server 2007 R2 Mediation Servers, they will also be available in the list.

11. To associate one or more public switched telephone network (PSTN) usages with the voice route, click **Select** and choose a record from the list of PSTN usage records that have been defined for your Enterprise Voice deployment.

Note:
To view the properties of each of the available PSTN usage records, see View PSTN Usage Records.
To create or edit PSTN usage records, see Create a Voice Policy and Configure PSTN Usage Records or Modify a Voice Policy and Configure PSTN Usage Records.

12. Arrange the PSTN usage records for optimum performance. To change a record's position in the list, highlight the record name and click the up or down arrow.

Note:
In contrast to a voice policy, where the order in which PSTN usage records are listed is important, the order in which PSTN usage records are listed in the voice route is insignificant. However, we recommend that you organize the list by frequency of use. For example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup. (Lync Server traverses the list from the top down.)

13. (Optional) Type a value into the **Enter a translated number to test** field and

click **Go**. The test results are displayed under the field.

> **Note:**
> You can save a voice route that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

14. Click **OK** to save the voice route.

> **Important:**
> Whenever you create a voice route, you must run the **Commit All** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration.

Tasks

Modify a Voice Route
View PSTN Usage Records
Create a Voice Policy and Configure PSTN Usage Records
Modify a Voice Policy and Configure PSTN Usage Records
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

1.7.7.3.3.2 Modify a Voice Route

Modify a Voice Route

See Also

Deploying Enterprise Voice > Configuring Voice Policies, PSTN Usage Records, and Voice Routes > Configuring Voice Routes for Outbound Calls >

Topic Last Modified: *2012-11-01*

This topic explains how to edit a voice route. To create a new route, see Create a Voice Route.

⊟To modify a voice route

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Route**.
4. On the **Route** page, use either of the following methods to modify a voice route:
   - Click a voice route name, click **Edit**, and then click **Show details**.
   - Click a voice route name, click **Edit**, click **Copy**, and then click **Paste**. Click the new copy of the voice route that you just created, click **Edit**, and then click **Show details**.
5. In the **Name** field on the **Edit Voice Route** page, type a descriptive name for the voice route.
6. (Optional) In the **Description** field, type in additional descriptive information for the voice route.
7. To specify the patterns you want this route to accommodate, you can either use the **Build a pattern to match** tool to generate a regular expression, or write the regular expression manually.
   - To use the **Build a pattern to match** tool to generate a regular expression, enter values as follows. You can specify two types of pattern matching:
     - **Starting digits for numbers that you want to allow:** Enter prefix values that this route must accommodate (including the leading + if needed). For

        example, type **+425** and then click **Add**. Repeat this for each prefix value that you want to include in the route.
        - **Exceptions:** If you want to specify one or more exceptions for a prefix value, highlight the prefix and click **Exceptions**. Type in one or more values for the matching patterns that you do *not* want this route to accommodate. For example, to exclude numbers starting with +425237 from the route, enter a value of **+425237** in the **Exceptions** field, and then click **OK**.
    - To define the matching pattern manually, click **Edit** in the **Build a pattern to match** tool and then type in a .NET Framework regular expression to specify the matching pattern for destination phone numbers to which the route is applied. For information about how to write regular expressions, see ".NET Framework Regular Expressions" at http://go.microsoft.com/fwlink/p/?linkId=140927.

8. Select **Suppress caller ID** if you do not want the ID of the phone that is making the outbound call to appear to the call recipient. If you select this option, you must specify an **Alternate caller ID** that will appear on the recipient's caller ID display.
9. To associate one or more public switched telephone network (PSTN) trunks with the voice route, click **Add**, and then select a trunk from the list.

    Note:

    If your deployment includes any Microsoft Office Communications Server 2007 R2 Mediation Servers, they will also be available in the list.

10. To associate one or more PSTN usages with the voice route, click **Select** and choose a record from the list of PSTN usage records that have been defined for your Enterprise Voice deployment.

    Note:

    To view the properties of each of the available PSTN usage records, see View PSTN Usage Records.
    To create or edit PSTN usage records, see Create a Voice Policy and Configure PSTN Usage Records or Modify a Voice Policy and Configure PSTN Usage Records.

11. Arrange the PSTN usage records for optimum performance. To change a record's position in the list, highlight the record name and click the up or down arrow.

    Note:

    In contrast to a voice policy where the order in which PSTN usage records are listed is important, the order of PSTN usage records in a voice route is insignificant. However, we recommend that you organize the list by frequency of use, for example: RedmondLocal, RedmondLongDist, RedmondInternational, RedmondBackup. (Lync Server traverses the list from the top down.)

12. (Optional) Type a value into the **Enter a translated number to test** field and click **Go**. The test results are displayed under the field.

    Note:

    You can save a voice route that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

13. Click **OK**.
14. On the **Route** page, click **Commit**, and then click **Commit all**.

    Note:

    Whenever you create or modify a voice route, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create a Voice Route
View PSTN Usage Records
Create a Voice Policy and Configure PSTN Usage Records
Modify a Voice Policy and Configure PSTN Usage Records
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Test Voice Routing

1.7.7.3.4 Exporting and Importing Voice Routing Configuration

Exporting and Importing Voice Routing Configuration

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-11-01*

If you want to save your voice routing configuration without publishing it, follow these steps to use the Lync Server Control Panel configuration export and import commands to save and retrieve a snapshot of your voice routing configuration. When you import a voice routing configuration file (.vcfg), but changes have been made to the voice routing configuration on the server in the meantime, the pages in the **Voice Routing** group in Lync Server Control Panel will indicate that there are uncommitted changes to voice routing. Those uncommitted changes are the differences between the two configurations that require reconciliation.

Important:
If you have made any uncommitted changes to the settings on any page within the **Voice Routing** group, the changes are saved in the exported voice configuration file (.vcfg). This enables you to make voice routing configuration changes during multiple Lync Server Control Panel sessions before you publish the changes.

- Export a Voice Route Configuration File
- Import a Voice Route Configuration File

⊟Related Sections

1.7.7.3.4.1 Export a Voice Route Configuration File

Export a Voice Route Configuration File

See Also

Deployment > Deploying Enterprise Voice > Exporting and Importing Voice Routing Configuration >

Topic Last Modified: *2012-11-01*

If you want to save your voice routing configuration without publishing it, follow these steps to use the Lync Server Control Panel configuration export and import commands to save and retrieve a snapshot of your voice routing configuration. When you import a voice routing configuration file (.vcfg), but changes have been made to the voice routing configuration on the server in the meantime, the pages in the **Voice Routing** group in Lync Server Control Panel will indicate that there are uncommitted changes to voice routing. Those uncommitted changes are the differences between the two configurations that require reconciliation.

If you have made any uncommitted changes to the settings on any page within the group, the changes are saved in the exported voice configuration file (.vcfg). This enables you to make voice routing configuration changes during multiple sessions before you publish the changes.

⊟To export a voice routing configuration

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.
4. On the **Actions** menu, click **Export configuration**.
5. Specify a location and file name, and then click **Save**.

Tasks

Import a Voice Route Configuration File

1.7.7.3.4.2 Import a Voice Route Configuration File

Import a Voice Route Configuration File

See Also

Deployment > Deploying Enterprise Voice > Exporting and Importing Voice Routing Configuration >

Topic Last Modified: *2012-11-01*

If you want to save your voice routing configuration without publishing it, follow these steps to use the Lync Server Control Panel configuration export and import commands to save and retrieve a snapshot of your voice routing configuration. When you import a voice routing configuration file (.vcfg), but changes have been made to the voice routing configuration on the server in the meantime, the pages in the **Voice Routing** group in Lync Server Control Panel will indicate that there are uncommitted changes to voice routing. Those uncommitted changes are the differences between the two configurations that require reconciliation.

If you have made any uncommitted changes to the settings on any page within the group, the changes are saved in the exported voice configuration file (.vcfg). This enables you to make voice routing configuration changes during multiple sessions before you publish the changes.

⊟To import a voice routing configuration

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.
4. On the **Actions** menu, click **Import configuration**.
5. Find the configuration file you want to import and then click **Open**.
6. Click **Commit**, and then click **Commit all**.

> **Note:**
> Whenever you import a voice configuration file, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Export a Voice Route Configuration File
Publish Pending Changes to the Voice Routing Configuration

1.7.7.3.5 Publish Pending Changes to the Voice Routing Configuration

Publish Pending Changes to the Voice Routing Configuration

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2012-08-07*

After you make changes to any of the configuration settings in pages in the **Voice Routing** group, perform this procedure to review, publish, or cancel the pending changes.

Important:

Be sure that only one user at a time modifies the Voice Routing configuration settings. All pending changes must be published at the same time by running the **Commit all** command. You cannot selectively publish pending changes. Before you publish pending changes, run the **Review uncommitted changes** command and cancel any configuration changes that you do not want to publish.
If you navigate away from the pages in the **Voice Routing** group before committing pending changes, all pending changes will be lost. However, you can export the current configuration (including any pending changes) to a voice configuration file, and then import and publish the updated configuration. For details, see Export a Voice Route Configuration File.

⊟To review, publish, or cancel voice routing configuration changes

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.
4. Make the configuration changes you want to the settings on each page of the **Voice Routing** group.
5. To review pending changes without publishing them, select **Review uncommitted changes** from the **Commit** menu.
6. If you want to cancel any of the pending changes, do one of the following:
   - Select **Cancel all uncommitted changes** from the **Commit** menu.
   - Navigate to the tab of the **Voice Routing** page that has pending changes you want to cancel, select the item with the pending changes, click **Commit**, and then click **Cancel selected changes**.
7. After you have reviewed all pending changes and canceled any that you do not want to publish, click **Commit**, and then click **Commit all**.
8. In the **Uncommitted Voice Configuration Settings** dialog box, which displays a list of all of the pending changes, click **OK**.

   When Lync Server Control Panel has committed the changes, the **Successfully published voice routing configuration** message appears.

1.7.7.3.6 Test Voice Routing

Test Voice Routing

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2013-02-24*

You can use the Lync Server Control Panel **Test Voice Routing** tab to configure test case scenarios. To define a test case, you specify the dial plan, voice policy, PSTN usage, and voice route against which to test a specified phone number.

Before you actually deploy your voice routing configuration, we recommend that you test it on various phone numbers to make sure that the results are what you're expecting.

Tip:

You can use the **Export test cases** and **Import test cases** commands to save voice routing test cases and import them for use on another computer.

Caution:

If you delete any part of your voice routing configuration, such as a dial plan, voice policy, voice route, or phone usage, you should review and update your voice routing test cases. The Lync Server Control Panel will not alert you to test cases that are no longer valid due to changed configurations.

- Create a Voice Routing Test Case
- Export Voice Routing Test Cases
- Import Voice Routing Test Cases
- Running Voice Routing Tests

1.7.7.3.6.1 Create a Voice Routing Test Case

Create a Voice Routing Test Case

See Also

Deployment > Deploying Enterprise Voice > Test Voice Routing >

Topic Last Modified: *2012-10-10*

⊟To create a test case

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Test Voice Routing**.
4. On the **Test Voice Routing** page, click **New** to create a new test case.
5. In **Name**, type in a unique name for the test case.

   The name must be unique among all voice routing test cases in your Enterprise Voice deployment. It can be up to 32 characters in length and may contain any alphanumeric characters, in addition to the backslash (\), period (.), or underscore (_).
6. In **Dialed number to test**, type in the dialed number that you want to use to test the routing configuration that you specify for this test case. Based on the dial plan, route, and voice policy, this number will be normalized and displayed as output.

7. In the **Dial Plan** list, select the dial plan to use when running the test. Default is the Global dial plan.
8. In the **Voice Policy** list, select the voice policy to use when running the test. Default is the Global voice policy.
9. In **Expected translation**, type in the phone number in the format you expect to see it after translation. This is the value of the phone number that you are testing after it has been translated by the first normalization rule that matches in the selected dial plan. When you run the test case, if the number you are testing does not result in the value in **Expected translation**, the test fails.
10. (Optional) In the **Expected PSTN usage** list, you can select the public switched telephone network (PSTN) usage record that you expect to be used when you run the test case, based on the specified dial plan and voice policy. If a different PSTN usage record is used, the test fails.
11. (Optional) In the **Expected route** list, you can select the voice route that you expect to be used when you run the test case, based on the specified dial plan and voice policy. If a different voice route is used, the test fails.
12. (Optional) Click **Run** to run the test case. The results are shown in the right panel of the page.
13. Click **OK**.
14. Click **Commit**, and then click **Commit all**.

> **Note:**
> Whenever you create a voice routing test case, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Export Voice Routing Test Cases
Import Voice Routing Test Cases

Other Resources

Configuring Dial Plans
Configuring Voice Policies, PSTN Usage Records, and Voice Routes

1.7.7.3.6.2 Export Voice Routing Test Cases

Export Voice Routing Test Cases

See Also

Deployment > Deploying Enterprise Voice > Test Voice Routing >

Topic Last Modified: *2012-11-01*

Test cases provide a way for you to test voice routes in your organization: you define such things as the number to be dialed and the dial plan and voice policy to be employed, and Lync Server can then verify that that, given those conditions, the supplied number can successfully be routed to the PSTN network.

Test cases, which can be created by using Lync Server Control Panel, are typically saved only on the server where the case was originally created and run. However, these test cases can be exported as XML files (with the .vtest extension) and then imported on other servers. This enables you to run the same tests on different computers located at different points in your topology.

⊟To export a voice routing test case

1. In Lync Server Control Panel, click **Voice Routing** and then click **Test Voice Routing**.

2. On the **Test Voice Routing** tab, select the test case (or test cases) to be exported. To select multiple test cases, click the first case to be exported, then hold down the Ctrl key and select the additional cases to be exported.
3. Click **Action**, then click **Export test cases**.
4. In the **Save As** dialog box, select a folder to store the exported test cases and type a name for the resulting XML file in the **File name** box. Note that if you are exporting multiple tests cases all of these test cases will be saved to a single XML file.
5. To save the test cases, click **Save**.

Tasks

Import Voice Routing Test Cases

1.7.7.3.6.3 Import Voice Routing Test Cases

Import Voice Routing Test Cases

See Also

Deployment > Deploying Enterprise Voice > Test Voice Routing >

Topic Last Modified: *2013-02-21*

Test cases provide a way for you to test voice routes in your organization: you define such things as the number to be dialed and the dial plan and voice policy to be employed, and Lync Server 2013 can then verify that that, given those conditions, the supplied number can successfully be routed to the PSTN network.

Test cases, which can be created by using Lync Server Control Panel, are typically saved only on the server where the case was originally created and run. However, these test cases can be exported as XML files (with the .vtest extension) and then imported on other servers. This enables you to run the same tests on different computers located at different points in your topology.

⊟To import a voice routing test case

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**.
4. On the **Actions** menu, click **Import test cases**.
5. Find the test case file (.vtest) that you want to import, and then click **Open**.
6. Click **Commit**, and then click **Commit all**.

Note:
Whenever you import a .vtest file, you must run the **Commit all** command to publish the test case. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Export Voice Routing Test Cases

Running Voice Routing Tests

Deployment > Deploying Enterprise Voice > Test Voice Routing >

Topic Last Modified: *2013-02-21*

Lync Server 2013 provides two different methods for testing voice routes: you can do informal, ad hoc testing against any phone number and any voice route; or you can do more formal testing using voice route test cases. With formal testing, you define such things as the number to be dialed and the dial plan and voice policy to be employed, and Lync Server can then verify that that, given those conditions, the supplied number can successfully be routed to the PSTN network. Both of these methods are described in subsequent sections of this documentation.

- Run Informal Voice Routing Tests
- Run Voice Routing Test Cases

Run Informal Voice Routing Tests

See Also

Deploying Enterprise Voice > Test Voice Routing > Running Voice Routing Tests >

Topic Last Modified: *2012-08-07*

You can use the **Create voice routing test case information** dialog box to run informal tests before creating an actual test case. When you are satisfied with the outcome of a test, you have the option of saving it as a formal test case.

⊟To run an informal voice routing test

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Test Voice Routing**.
4. On the **Test Voice Routing** page, click **Create voice routing test case information**.
5. In the **Dialed number** field, type in the phone number you want to use for this test. This number will be normalized and displayed in the **Normalized number** field of the **Results** pane.
6. In the **Dial plan** list, select the dial plan to use for testing the dialed number. Default is the Global dial plan.

   When you run the test, the first normalization rule in this dial plan that matches the dialed number will be displayed in the **Normalization rule** field of the **Results** pane.
7. In the **Voice Policy** list, select the voice policy to use for testing the dialed number. Default is the Global voice policy.

   When you run the test, the first matching PSTN usage record in this voice policy will be displayed in the **First PSTN usage** field of the **Results** pane. Also, the first matching voice route that is associated with this PSTN usage record will be displayed in the **First route** field.
8. (Optional) Select the **Populate from user** check box if you want to test the dialed number against the voice policy assigned to a particular user.

   8.a.Click **Browse** to display the **Select Enterprise Voice Users** dialog box.

8.b.Click **Find** to display the list of users who are enabled for Enterprise Voice.

8.c.Double-click the user name whose assigned voice policy you want to use for this test. The **Policy** field is now populated with the voice policy assigned to the selected user.

When you run the test, the first matching public switched telephone network (PSTN) usage record in this voice policy will be displayed in the **First PSTN usage** field of the **Results** pane. Also, the first matching voice route that is associated with this PSTN usage record will be displayed in the **First route** field.

9.Click **Run** to run the test case. The results are shown in the right panel of the dialog box.

10.(Optional) Click **Save as** if you want to save this test configuration as a formal test case.

10.a.In the **Name** field of the **Save Voice Routing Test Case Information** dialog box, type a unique name for the test case.

The name must be unique among all voice routing test cases in your Enterprise Voice deployment. It can be up to 32 characters in length and may contain any alphanumeric characters, in addition to the backslash (\), period (.), or underscore (_).

10.b.Note that the remaining fields on the **Save Voice Routing Test Case Information** dialog box are read-only, and are prepopulated from the informal test configuration *and* results. Verify that this is the configuration that you want to save for the test case.

> **Note:**
>
> Values from the test results are used to prepopulate fields on the **Save Voice Routing Test Case Information** dialog box as follows:
>
> - **Expected translation** is prepopulated with the value in the **Normalized number** field.
> - **Expected route** is prepopulated with the value in the **First route** field.
> - **Expected PSTN usage record** is prepopulated with the value in the **First PSTN usage** field.
>
> If matches for any of these values were not found during the test run, the corresponding field is empty on the **Save Voice Routing Test Case Information** dialog box.

1.a.Click **Ok** to save the test case, or click **Cancel** to return to return to the **View voice routing test case information** dialog box to further develop the test before saving it.

2.Click **Commit**, and then click **Commit all**.

> **Note:**
>
> Whenever you create a voice routing test case, you must run the **Commit all** command to publish the test case. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create a Voice Routing Test Case
Run Voice Routing Test Cases
Export Voice Routing Test Cases
Import Voice Routing Test Cases

Other Resources

Configuring Dial Plans
Configuring Voice Policies, PSTN Usage Records, and Voice Routes

Run Voice Routing Test Cases

See Also

Deploying Enterprise Voice > Test Voice Routing > Running Voice Routing Tests >

Topic Last Modified: *2013-02-24*

You can run all of the test cases in your voice routing test case suite, or you can run one or more selected test cases.

⊟To run all voice routing test cases

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Test Voice Routing**.
4. On the **Test Voice Routing** page, click **Action** and then click **Run all**.

   The pass or fail status of each test case is shown in the **Pass/fail** column. If a test case has not yet been run, N/A is shown in the **Pass/fail** column.
5. (Optional) To see detailed results for each test case, double-click the test case name. Results are shown in the shaded area on the right side of the **Edit Test Case** page:
   - 5.a. **Test result:** Overall pass or fail status of the test case run.
   - 5.b. **Normalization rule:** The first normalization rule in the dial plan selected for this test case that matches the dialed number (the value in the **Number to test** field).
   - 5.c. **Normalized number:** The value of the dialed number after the normalization rule has translated it.
   - 5.d. **First PSTN usage:** The first public switched telephone network (PSTN) usage record in the voice policy selected for this test case that matches the dialed number.
   - 5.e. **First route:** The first voice route in the first PSTN usage record that matches the dialed number.

> **Note:**
>
> The **Expected PSTN usage record** and **Expected route** fields are optional in voice routing test case configuration. If the test case does not specify these values, the corresponding field in the test results will be empty.

⊟To run one or more selected voice routing test cases

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing**, and then click **Test Voice Routing**.
4. On the **Test Voice Routing** page, click the names of the test cases that you want to run.
5. On the **Action** menu, click **Run selected**.

   The pass or fail status of each test case is shown in the **Pass/fail** column. If a test case has not yet been run, N/A is shown in the **Pass/fail** column.
6. (Optional) To see detailed results for each test case, double-click the test case name. Results are shown in the shaded area on the right side of the

Edit Test Case page:

6.a.**Test result:** Overall pass or fail status of the test case run.

6.b.**Normalization rule:** The first normalization rule in the dial plan selected for this test case that matches the dialed number (the value in the **Number to test** field).

6.c.**Normalized number:** The value of the dialed number after the normalization rule has translated it.

6.d.**First PSTN usage:** The first PSTN usage record in the voice policy selected for this test case that matches the dialed number.

6.e.**First route:** The first voice route in the first PSTN usage record that matches the dialed number.

> **Note:**
> The **Expected PSTN usage record** and **Expected route** fields are optional in voice routing test case configuration. If the test case does not specify these values, the corresponding field in the test results will be empty.

Other Resources

Test Voice Routing
Running Voice Routing Tests

1.7.7.4 Configuring Dial Plans

Configuring Dial Plans

See Also

Microsoft Lync Server 2013 > Deployment > Deploying Enterprise Voice >

Topic Last Modified: *2013-02-22*

A Lync Server 2013 dial plan is a named set of normalization rules that translate phone numbers for a named location, individual user, or contact object for purposes of phone authorization and call routing.

> **Note:**
> For details, see Dial Plans and Normalization Rules in the Planning documentation.

- View Dial Plan Information
- Create a Dial Plan
- Modify a Dial Plan

⊟See Also

Concepts

Dial Plans and Normalization Rules

1.7.7.4.1 View Dial Plan Information

View Dial Plan Information

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-11-01*

To view information for an existing dial plan, perform the steps in the following procedure. If you want to create a new dial plan, see Create a Dial Plan.

⊟To view information about a dial plan from Lync Server Control Panel

1.Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, double-click a dial plan name.

> **Note:**
> You can view information for only one dial plan at a time.

To view dial plans by using Windows PowerShell cmdlets

- Dial plans can be viewed by using the Windows PowerShell command-line interface and the **Get-CsDialPlan** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

  To view information about all your dial plans, type the following command in the Lync Server Management Shell, and then press ENTER:

```
Get-CsDialPlan
```

  That command will return information similar to this:

```
Identity                  : Global
Description               :
DialinConferencingRegion  :
NormalizationRules        : {Description=;
                            Pattern=^(\d+)$;Translation=$1;Name=
                            KeepAll;IsInternalExtension=False}
CountryCode               :
State                     :
City                      :
ExternalAccessPrefix      :
SimpleName                : DefaultProfile
OptimizeDeviceDialing     : False
```

Tasks

Create a Dial Plan
Modify a Dial Plan

1.7.7.4.2 Create a Dial Plan

Create a Dial Plan

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-10-06*

To create a new dial plan, perform the steps in the following procedure. If you want to edit a dial plan, see Modify a Dial Plan.

To create a dial plan

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, click **New** and select a scope for the dial plan:
   - **Site dial plan** applies to an entire site, except any users or groups that are assigned to a user dial plan. If you select **Site** for a dial plan's scope, you must choose the site from the **Select a Site** dialog box. If a dial plan has already been created for a site, the site does not appear in the **Select a Site** dialog box.
   - **Pool dial plan** can apply to a public switched telephone network (PSTN) gateway or a Registrar. If you select **Pool** for a dial plan's scope, choose the PSTN gateway or Registrar from the **Select a Service** dialog box. If a dial plan has already been created for a service (PSTN gateway or Registrar), the service does not appear in the list.
   - **User dial plan** can be applied to specified users or groups.

   > **Note:**
   > After you select the dial plan scope, it cannot be changed.

5. If you are creating a user dial plan, enter a descriptive name in the **Name** field on the **New Dial Plan** dialog box. After this name is saved, it cannot be changed.

   > **Note:**
   > For site dial plans, the **Name** field is prepopulated with the site name and cannot be changed.
   > For pool dial plans, the **Name** field is prepopulated with the PSTN gateway or Registrar name and cannot be changed.

6. The **Simple name** field is prepopulated with the same name that appears in the **Name** field. You can optionally edit this field to specify a more descriptive name that reflects the site, service, or user to which the dial plan applies.

   > **Important:**
   > The **Simple name** must be unique among all dial plans within the Lync Server deployment. It cannot exceed 256 Unicode characters, each of which can be an alphabetic or numeric character, a hyphen (-), a period (.), a plus sign (+), or an underscore (_).
   > Spaces are not allowed in the **Simple name**.

7. (Optional) In the **Description** field, you can type additional descriptive information about the dial plan.
8. (Optional) If you want to use this dial plan as a region for dial-in access numbers, specify a **Dial-in conferencing region**. If you do not want to use this dial plan for dial-in access numbers, leave this field empty.

   > **Note:**
   > Dial-in conferencing regions are required to associate dial-in conferencing access numbers with one or more dial plans.

9. (Optional) In the **External access prefix** field, specify a value only if users need to dial one or more additional leading digits (for example, 9) to get an external line. You can type in a prefix value of up to four characters (#, *, and 0-9).

   > **Note:**
   > If you specify an external access prefix, you do not need to create a new normalization rule to accommodate the prefix.

10. Associate and configure normalization rules for the dial plan as follows:
    - To choose one or more rules from a list of all normalization rules available in your Enterprise Voice deployment, click **Select**. In **Select Normalization Rules**, highlight the rules you want to associate with the dial plan and then click **OK**.
    - To define a new normalization rule and associate it with the dial plan, click **New**. For details about defining a new rule, see Defining Normalization Rules.

- To edit a normalization rule that is already associated with the dial plan, highlight the rule name and click **Show details**. For details about editing the rule, see Defining Normalization Rules.
- To copy an existing normalization rule to use as a starting point for defining a new rule, highlight the rule name and click **Copy**, and then click **Paste**. For details about editing the copy, see Defining Normalization Rules.
- To remove a normalization rule from the dial plan, highlight the rule name and click **Remove**.

> **Note:**
> Each dial plan must have at least one associated normalization rule. For information about how to determine all of the normalization rules a dial plan requires, see Dial Plans and Normalization Rules in the Planning documentation.

11. Verify that the dial plan's normalization rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name and then click the up or down arrow.

> **Important:**
> Lync Server traverses the normalization rule list from the top down and uses the first rule that matches the dialed number. If you configure a dial plan so that a dialed number can match more than one normalization rule, make sure the more restrictive rules are sorted above the less restrictive ones.
> The default **Keep All** normalization rule **^(\d{11})$** matches any 11-digit number. For example, if you add a normalization rule that matches 11-digit numbers that start with 1425, make sure that **Keep All** is sorted below the more restrictive **^(1425\d{7})$** rule.

12. (Optional) Enter a number to test the dial plan and then click **Go**. The test results are displayed under **Enter a number to test**.

> **Note:**
> You can save a dial plan that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

13. Click **OK**.
14. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

> **Note:**
> Any time you create a dial plan, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Modify a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Defining Normalization Rules

1.7.7.4.3 Modify a Dial Plan

Modify a Dial Plan

See Also

Deployment > Deploying Enterprise Voice > Configuring Dial Plans >

Topic Last Modified: *2012-11-01*

To modify an existing dial plan, perform the steps in the following procedure. If you want to create a new dial plan, see Create a Dial Plan.

⊟To modify a dial plan

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Routing** and then click **Dial Plan**.
4. On the **Dial Plan** page, double-click a dial plan name.

   Note:
   The dial plan scope and name were set when the dial plan was created. They cannot be changed.

5. (Optional) In **Edit Dial Plan**, edit the **Simple name** field, which is prepopulated with the same name that appears in the **Name** field to specify a more descriptive name that reflects the site, service, or user to which the dial plan applies.

   Important:
   The **Simple name** must be unique among all dial plans within the Lync Server 2013 deployment. It cannot exceed 256 Unicode characters, each of which can be an alphabetic or numeric character, a hyphen (-), a period (.), a plus sign (+), or an underscore (_).
   Spaces are not allowed in the **Simple name** field.

6. (Optional) In the **Description** field, type descriptive information about the dial plan.
7. (Optional) If you want to use this dial plan as a region for dial-in access numbers, specify a **Dial-in conferencing region**. If you do not want to use this dial plan for dial-in access numbers, leave this field empty.

   Note:
   Dial-in conferencing regions are required to associate dial-in conferencing access numbers with one or more dial plans.

8. (Optional) In the **External access prefix** field, specify a value only if users need to dial one or more additional leading digits to get an external line (for example, 9). You can type in a prefix value of up to four characters (that is, #, *, and 0-9).

   Note:
   If you specify an external access prefix, you do not need to create a new normalization rule to accommodate the prefix.

9. Associate and configure normalization rules for the dial plan:
   - To choose one or more rules from a list of all normalization rules available in your Enterprise Voice deployment, click **Select**. In the **Select Normalization Rules** dialog box, highlight the rules that you want to associate with the dial plan and then click **OK**.
   - To define a new normalization rule and associate it with the dial plan, click **New**. For details about defining a new rule, see Defining Normalization Rules.
   - To edit a normalization rule that is already associated with the dial plan, highlight the rule name and click **Show details**. For details about editing the rule, see Defining Normalization Rules.
   - To copy an existing normalization rule to use as a starting point for defining a new rule, highlight the rule name and click **Copy**, and then click **Paste**. For details about editing the copy, see Defining Normalization Rules.
   - To remove a normalization rule from the dial plan, highlight the rule name and click **Remove**.

   Note:

Each dial plan must have at least one associated normalization rule. For details about how to determine all of the normalization rules a dial plan requires, see Dial Plans and Normalization Rules in the Planning documentation.

10. Verify that the dial plan's normalization rules are arranged in the correct order. To change a rule's position in the list, highlight the rule name and then click the up or down arrow.

Important:

Lync Server traverses the normalization rule list from the top down and uses the first rule that matches the dialed number. If you configure a dial plan so that a dialed number can match more than one normalization rule, make sure the more restrictive rules are sorted above the less restrictive ones.

The default **Keep All** normalization rule **^(\d{11})$** matches any 11-digit number. If, for example, you add a normalization rule that matches 11-digit numbers that start with 1425, make sure that **Keep All** is sorted below the more restrictive **^(1425\d{7})$** rule.

11. (Optional) Enter a number to test the dial plan and then click **Go**. The test results are displayed under **Enter a number to test**.

Note:

You can save a dial plan that does not yet pass the test and then reconfigure it later. For details, see Test Voice Routing.

12. Click **OK**.
13. On the **Dial Plan** page, click **Commit**, and then click **Commit all**.

Note:

Any time you create or modify a dial plan, you must run the **Commit all** command to publish the configuration change. For details, see Publish Pending Changes to the Voice Routing Configuration in the Operations documentation.

Tasks

Create a Dial Plan
Publish Pending Changes to the Voice Routing Configuration

Other Resources

Defining Normalization Rules

1.7.8 Managing Call Management Features

Managing Call Management Features

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-12-18*

Enterprise Voice call management features control how incoming calls are routed and answered. Lync Server 2013 provides the following call management features:

- **Call Park:** Enables voice users to temporarily park a call and then pick it up from the same phone or another phone.
- **Group Pickup:** Enables users to pick up calls that are ringing for other users by dialing a call pickup group number.
- **Response Group:** Routes incoming calls to groups of agents by using hunt groups or interactive voice response (IVR) questions and answers.
- **Announcement:** Plays a message for calls made to an unassigned number, or routes the call elsewhere, or both.

This section describes how to manage these call management features in your Enterprise

Voice deployment.

- Managing Call Park
- Managing Group Call Pickup
- Managing Response Groups
- Managing Calls to Unassigned Numbers

1.7.8.1 Managing Call Park

Managing Call Park

Microsoft Lync Server 2013 > Operations > Managing Call Management Features >

Topic Last Modified: *2012-09-10*

The Call Park application enables an Enterprise Voice user to put a call on hold from one telephone and then retrieve the call later from any telephone. When the user parks a call, Lync Server transfers the call to a temporary number, called an *orbit*, where the call is held until someone retrieves it or it times out.

Topics in this section provide step-by-step procedures for tasks that you can perform to customize and maintain the Call Park application in your deployment.

- Configure Phone Number Extensions for Parking Calls
- Configure Call Park Settings
- Customize Call Park Music on Hold
- Manage Call Park During Disaster Recovery

1.7.8.1.1 Configure Phone Number Extensions for Parking Calls

Configure Phone Number Extensions for Parking Calls

Operations > Managing Call Management Features > Managing Call Park >

Topic Last Modified: *2012-09-10*

The Call Park application uses extension numbers in the Call Park orbit table to park calls. You need to configure the Call Park orbit table with the ranges of extension numbers that your organization reserves for parked calls. These extensions need to be virtual extensions (that is, extensions that have no user or phone assigned to them). Each Lync Server pool where a Call Park application is deployed and configured can have one or more orbit ranges. Orbit ranges must be globally unique across the Lync Server deployment.

◆**Important:**
You must select the **Enable call park** check box in your voice policy before you can use Call Park. By default, this option is not selected.

- Create or Modify a Call Park Orbit Range
- Delete a Call Park Orbit Range

1.7.8.1.1.1 Create or Modify a Call Park Orbit Range

Create or Modify a Call Park Orbit Range

See Also

Deploying Call Management Features > Configuring Call Park > Configure the Call Park Orbit Table >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to create or modify a call park orbit range.

⊟To use Lync Server Control Panel to create or modify a range of numbers for parking calls

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Features** and then click **Call Park**.
4. On the **Call Park** page, do one of the following:
   - To create a new orbit range, click **New**. In **Name**, type an identifying name for this range of numbers.

     Note:

     After you commit the orbit range to the database, you cannot change this name.

   - To modify an existing orbit range, type all or part of the name of the orbit range in the search field. In the resulting list of orbits, click the orbit you want, click **Edit**, and then click **Show details**.
5. In the first **Number range** field, type the beginning number of the range of extensions for this call park orbit, and in the second **Number range** field, type the ending number of the range.

   Note:

   - The beginning number of the range must be less than or equal to the ending number of the range.
   - The value of the beginning number of the range must be the same length as the ending number of the range.
   - The orbit range must be unique. This range cannot overlap with any other range.
   - If the orbit range begins with the character * or #, the range must be greater than 100.
   - Valid values: Must match the regular expression string ([*|#]?[1-9]\d{0,7})|([1-9]\d{0,8}). This means the value must be a string beginning with either the character * or # or a number 1 through 9 (the first character cannot be a zero). If the first character is * or #, the following character must be a number 1 through 9 (it cannot be a zero). Subsequent characters can be any number 0 through 9 up to seven additional characters (for example, "#6000", "*92000", "*95551212", and "915551212"). If the first character is not * or #, the first character must be a number 1 through 9 (it cannot be zero), followed by up to eight characters, each a number 0 through 9 (for example, "915551212", "41212", "300").
   - You should not have more than a total of 50,000 orbits per pool. Each orbit range typically encompasses 100 or fewer orbits, but it can be much larger as long as it includes fewer than 10,000 orbits. For example, instead of specifying a starting number of "7000000" and an ending number of "8000000," consider specifying a starting number of "7000000" and an ending number of "7000100."

1. In **FQDN of destination server**, click the fully qualified domain name (FQDN) or service ID of the Application service that hosts the Call Park application. All calls parked to numbers within the range specified by the start number and

end number in the orbit range will be routed to this server or pool.
2. Click **Commit**.

⊟To use Windows PowerShell to create or modify a range of numbers for parking calls

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Use **New-CsCallParkOrbit** to create a new range of orbit numbers. Use **Set-CsCallParkOrbit** to modify an existing range of orbit numbers.

   At the command line, run:

   ```
   New-CsCallParkOrbit -Identity <name of orbit range> -NumberRangeStart
   ```

   For example:

   ```
   New-CsCallParkOrbit -Identity "Redmond orbit 1" -NumberRangeStart 100
   ```

   The following example shows how to modify the numbers in an existing orbit range,

   ```
   Set-CsCallParkOrbit -Identity "Redmond orbit 1" -NumberRangeStart 500
   ```

Tasks

Delete a Call Park Orbit Range

Other Resources

New-CsCallParkOrbit
Set-CsCallParkOrbit

1.7.8.1.1.2 Delete a Call Park Orbit Range

Delete a Call Park Orbit Range

See Also

Managing Call Management Features > Managing Call Park > Configure Phone Number Extensions for Parking Calls >

Topic Last Modified: *2013-02-20*

Use one of the following procedures to delete a Call Park orbit range.

⊟To use Lync Server Control Panel to delete a Call Park orbit range

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Features** and then click **Call Park**.
4. On the **Call Park** page, in the search field, type all or part of the name of the orbit range that you want to delete.
5. In the resulting list of orbits, click the orbit, click **Edit**, and then click **Delete**.
6. Click **OK**.

⊟To use Windows PowerShell to delete a Call Park orbit range

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.

2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. At the command line, type:

```
Remove-CsCallParkOrbit -Identity "<orbit range name>"
```

For example:

```
Remove-CsCallParkOrbit -Identity "Redmond orbit 1"
```

> **Note:**
> For details about more options, see Remove-CsCallParkOrbit.

Tasks

Create or Modify a Call Park Orbit Range

Other Resources

Remove-CsCallParkOrbit
Get-CsCallParkOrbit

1.7.8.1.2 Configure Call Park Settings

Configure Call Park Settings

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Call Park >

Topic Last Modified: *2012-11-01*

If you don't want to use default Call Park settings, you can customize them. When you install the Call Park application, global settings are configured by default. You can modify the global settings, and you can also specify site-specific settings. Use the **New-CsCpsConfiguration** cmdlet to create new site-specific settings. Use the **Set-CsCpsConfiguration** cmdlet to modify existing settings.

> **Note:**
> At a minimum, we recommend that you configure the **OnTimeoutURI** option for the fallback destination to use when a parked call times out and ringback fails.

Use **New-CsCpsConfiguration** cmdlet or the **Set-CsCpsConfiguration** cmdlet to configure any of the following settings:

This option:	Specifies this:
CallPickupTimeoutThreshold	The amount of time that elapses after a call has been parked before it rings back to the phone where the call was answered. The value must be entered in the format hh:mm:ss to specify the hours, minutes, and seconds. The minimum value is 10 seconds, and the maximum value is 10 minutes. The default is 00:01:30.
EnableMusicOnHold	Whether music plays for a caller while a call is parked. Values are True or False. The default is True.
MaxCallPickupAttempts	The number of times a parked call rings back to the answering phone before it is forwarded to the fallback Uniform Resource

	Identifier (URI) that is specified for **OnTimeoutURI**. The default is 1.
OnTimeoutURI	The SIP address of the user or response group to which an unanswered parked call is routed when **MaxCallPickupAttempts** is exceeded. Value must be a SIP URI beginning with the string sip:. For example, sip:bob@contoso.com. The default is no forwarding address.

⊟To configure Call Park settings

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

```
New-CsCpsConfiguration -Identity site:<sitename to apply settings> [-C
```

Tip:

Use the **Get-CsSite** cmdlet to identify the site. For details, see Lync Server Management Shell documentation.

For example:

```
New-CsCpsConfiguration -Identity site:Redmond1 -CallPickupTimeoutThres
```

Tasks

Customize Call Park Music on Hold

Other Resources

New-CsCpsConfiguration
Set-CsCpsConfiguration
Get-CsSite

1.7.8.1.3 Customize Call Park Music on Hold

Customize Call Park Music on Hold

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Call Park >

Topic Last Modified: *2012-09-10*

You can specify your own music file to use for music on hold, instead of the default music file that ships with Lync Server 2013. To customize music on hold, use the **Set-CsCallParkServiceMusicOnHoldFile** cmdlet.

Note:

If you customize music on hold and want the same music for multiple sites, you must configure the music file for each site that runs the Call Park application.

⊟To customize the music file

1. Log on to the computer where Lync Server Management Shell is installed as a

member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.

2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Run:

```
Set-CsCallParkServiceMusicOnHoldFile -Service <ServiceID where the Cal
```

Tip:
Use the **Get-CsService** cmdlet to identify the service. For details, see Get-CsService.

The following example shows how to obtain the contents of a file, soothingmusic.wma, as a byte array and assign it to a variable. Then the audio file is assigned as the music-on-hold file for Call Park. For details, see Set-CsCallParkServiceMusicOnHoldFile.

```
$a = Get-Content -ReadCount 0 -Encoding byte "C:\MoHFiles\soothingmusi
Set-CsCallParkServiceMusicOnHoldFile -Service Redmond1-applicationserv
```

Other Resources

Set-CsCallParkServiceMusicOnHoldFile
Get-CsService

1.7.8.1.4 Manage Call Park During Disaster Recovery

Manage Call Park During Disaster Recovery

Planning > Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery >

Topic Last Modified: *2012-09-10*

Lync Server 2013 supports Call Park in the backup pool during disaster recovery. This section describes things to consider if you want to support Call Park during an outage and what happens to parked calls during the stages of an outage.

- Planning for Call Park Disaster Recovery
- Call Park Experience During Pool Failure

1.7.8.1.4.1 Planning for Call Park Disaster Recovery

Planning for Call Park Disaster Recovery

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Manage Call Park During Disaster Recovery >

Topic Last Modified: *2012-10-30*

This section describes some ways to prepare the Call Park application for disaster recovery and some considerations for the disaster recovery process.

Preparing for Call Park Disaster Recovery

Keep the following in mind when preparing for and carrying out disaster recovery procedures.

- Plan for disaster recovery when you do your capacity planning. For disaster recovery capacity, each pool in a paired pool should be able to handle the workloads of the Call Park services in both pools. For details about Call Park capacity planning, see Capacity Planning for Call Park.

- During disaster recovery, users who have been redirected to the backup pool as part of the failover process use the Call Park service running in the backup pool. Therefore, support for Call Park during disaster recovery requires the Call Park application to be deployed and enabled in both the primary pool and the backup pool.
- Each pool must have a valid range of orbit numbers for users who are homed in that pool to use for parking calls.
- Always keep a separate backup copy of any customized music on hold that has been uploaded for Call Park. These files are not backed up as part of the Lync Server 2013 disaster recovery process and will be lost if the files uploaded to the pool are damaged, corrupted, or erased.

Call Park Disaster Recovery Considerations

You can define only one set of Call Park application configuration settings and one customized music-on-hold audio file per pool. These settings include the timeout threshold, music on hold, maximum call pickup attempts, and timeout URI. To view these configuration settings, run the **Get-CsCpsConfiguration** cmdlet. For details about the **Get-CsCpsConfiguration** cmdlet, see Get-CsCpsConfiguration.

During disaster recovery, Call Park uses the Call Park application in the backup pool, so settings in the primary pool are not backed up. If the primary pool can't be recovered and you deploy a new pool to replace the primary pool, the settings from the primary pool are lost, and you need to reconfigure the Call Park settings and any customized music-on-hold audio files in the new pool.

If you deploy a new pool with a different fully qualified domain name (FQDN) to replace the primary pool, you need to reassign all the Call Park orbit ranges that were associated with the primary pool to the FQDN of the new pool. To reassign orbit ranges to the new pool, you can use either Lync Server Control Panel or the **Set-CsCallParkOrbit** cmdlet. For details about the **Set-CsCallParkOrbit** cmdlet, see Set-CsCallParkOrbit.

1.7.8.1.4.2 Call Park Experience During Pool Failure

Call Park Experience During Pool Failure

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Manage Call Park During Disaster Recovery >

Topic Last Modified: *2012-09-10*

When a Front End pool becomes unavailable due an unplanned incident, calls that have been parked but not yet retrieved are disconnected. During failover to a backup pool, users are redirected to the backup pool and are in resiliency mode. While in resiliency mode, users cannot park calls, but they can place calls on hold and transfer them. When failover is complete, calls can again be parked and retrieved as usual. During failback, users cannot park calls until they are out of resiliency mode.

During disaster recovery, users who have been redirected to the backup pool as part of the failover process use the Call Park application that is deployed in the backup pool. Therefore, users who are redirected to the backup pool use the call park settings that are configured for the Call Park application in the backup pool.

The following table summarizes the Call Park experience through the phases of disaster recovery.

User Experience During Disaster Recovery

Call state	When outage occurs	During failover	During failback
Call not yet parked	Call remains connected, but cannot be parked.	• During failover, call cannot be parked while users are in resiliency mode, but can be put on hold and transferred. • When failover completes, call can be parked and retrieved.	• During failback, call cannot be parked while users are in resiliency mode, but can be put on hold and transferred. • When failback completes, call can be parked and retrieved.
Call parked, but not yet retrieved	Call is disconnected.	No calls in this state.	Call remains parked.
Parked call already retrieved	Call remains connected.	Call remains connected.	Call remains connected.

1.7.8.2 Managing Group Call Pickup

Managing Group Call Pickup

Microsoft Lync Server 2013 > Operations > Managing Call Management Features >

Topic Last Modified: *2013-02-22*

Cumulative update for Lync Server 2013: February 2013 introduces Group Call Pickup as a new Enterprise Voice feature. Group Call Pickup enables Enterprise Voice users to pick up calls that are ringing for another user by dialing a call pickup group number.

Topics in this section provide step-by-step procedures for tasks that you perform to configure Group Call Pickup in your deployment.

- Configure Group Call Pickup Number Ranges
- Assign Group Call Pickup Numbers to Users
- Enable or Disable Group Call Pickup for Users
- Manage Group Call Pickup During Disaster Recovery

1.7.8.2.1 Configure Group Call Pickup Number Ranges

Configure Group Call Pickup Number Ranges

Operations > Managing Call Management Features > Managing Group Call Pickup >

Topic Last Modified: *2013-02-22*

Group Call Pickup is based on the Call Park application. When you deploy Group Call Pickup, you configure the call park orbit table with ranges of phone numbers that are designated as call pickup group numbers. These group numbers are the numbers that users dial to pick up calls that are ringing for another user.

Like call park orbit numbers, call pickup group numbers need to be virtual extensions that have no user or phone assigned to them. Each Front End pool where you deploy Group Call Pickup can have one or more ranges of call pickup group numbers. The group number ranges must be globally unique across the Lync Server deployment.

- Create or Modify a Group Call Pickup Number Range
- Delete a Group Call Pickup Number Range

1.7.8.2.1.1 Create or Modify a Group Call Pickup Number Range

Create or Modify a Group Call Pickup Number Range

See Also

Deploying Call Management Features > Configuring Group Call Pickup > Configure Call Pickup Group Numbers >

Topic Last Modified: *2013-01-30*

Use the following procedure to create or modify a call pickup group number range in the call park orbit table.

Note:

You must use Lync Server Management Shell to create, modify, remove, and view Group Call Pickup number ranges in the call park orbit table. Group Call Pickup number ranges are not available in Lync Server Control Panel.

Important:

The call pickup group number range must be assigned a type of GroupPickup. Users are enabled for Group Call Pickup only if the group number that they are assigned is type GroupPickup.

The call pickup group number ranges must comply with the following rules:

- The beginning number of the range must be less than or equal to the ending number of the range.
- The value of the beginning number of the range must be the same length as the ending number of the range.
- The number range must be unique. This range cannot overlap with any other range.
- If the number range begins with the character * or #, the range must be greater than 100.
- Valid values: Must match the regular expression string ([*|#]?[1-9]\d{0,7})|([1-9]\d{0,8}). This means the value must be a string beginning with either the character * or # or a number 1 through 9 (the first character cannot be a zero). If the first character is * or #, the following character must be a number 1 through 9 (it cannot be a zero). Subsequent characters can be any number 0 through 9 up to seven additional characters (for example, "#6000", "*92000", "*95551212", and "915551212"). If the first character is not * or #, the first character must be a number 1 through 9 (it cannot be zero), followed by up to eight characters, each a number 0 through 9 (for example, "915551212", "41212", "300").

To create or modify a call pickup group range

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Use **New-CsCallParkOrbit** to create a new range of call pickup group

numbers. Use **Set-CsCallParkOrbit** to modify an existing range of call pickup numbers.

At the command line, run:

```
New-CsCallParkOrbit -Identity <name of call pickup group range> -Numbe
```

For example:

```
New-CsCallParkOrbit -Identity "Redmond call pickup" -NumberRangeStart
```

The following example shows how to change a range of numbers from call park orbits to call pickup groups.

```
Set-CsCallParkOrbit -Identity "Redmond call pickup" -Type GroupPickup
```

> **Important:**
> Use this cmdlet to change the type assigned to number ranges only if you initially specified the incorrect type and the group range is not yet in use. If you change the number range from CallPark to GroupPickup or vice versa and the number range is already in use, either Call Park or Group Call Pickup will stop working for that number range. For example, if you change a number range from CallPark to GroupPick, the Call Park application can no longer use that range of orbits to park calls.

Tasks

Delete a Call Park Orbit Range

Other Resources

New-CsCallParkOrbit
Set-CsCallParkOrbit

1.7.8.2.1.2 Delete a Group Call Pickup Number Range

Delete a Group Call Pickup Number Range

See Also

Managing Call Management Features > Managing Group Call Pickup > Configure Group Call Pickup Number Ranges >

Topic Last Modified: *2013-01-30*

Use the following procedure to delete a Group Call Pickup number range.

⊟To delete a call pickup group number range

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. At the command line, type:

   ```
   Remove-CsCallParkOrbit -Identity "<group number range name>"
   ```

   For example:

   ```
   Remove-CsCallParkOrbit -Identity "Redmond call pickup"
   ```

> **Note:**
> For details about more options, see Remove-CsCallParkOrbit.

Tasks

Create or Modify a Call Park Orbit Range

Other Resources

Remove-CsCallParkOrbit
Get-CsCallParkOrbit

1.7.8.2.2 Assign Group Call Pickup Numbers to Users

Assign Group Call Pickup Numbers to Users

See Also

Operations > Managing Call Management Features > Managing Group Call Pickup >

Topic Last Modified: *2013-01-30*

After you add Group Call Pickup group numbers to the call park orbit table, you can assign the groups to users. Use the secondary extension feature activation (SEFAUtil) resource kit tool to assign call pickup groups to users.

Note:

In a hybrid deployment, do not assign a Group Call Pickup group to users who are homed online. Users who are homed online cannot participate in Group Call Pickup. That is, their calls cannot be answered by other users, and they cannot answer calls to other users.

⊟To assign a Group Call Pickup group to a user

1. Log on to the computer where you installed the SEFAUtil tool with administrator rights.
2. At the command line, run:

```
SEFAUtil.exe sip:<sip address of user> /server:<pool FQDN> /enablegrou
```

For example:

```
SEFAUtil.exe katarina@contoso.com /server:pool01.contoso.com /enablegr
```

Tasks

Enable Group Call Pickup for Users
Disable Group Call Pickup for Users

1.7.8.2.3 Enable or Disable Group Call Pickup for Users

Enable or Disable Group Call Pickup for Users

Operations > Managing Call Management Features > Managing Group Call Pickup >

Topic Last Modified: *2013-02-22*

When a Group Call Pickup range is added to the call park orbit table, you can enable and disable Group Call Pickup for the user as necessary. This section describes how to use the SEFAUtil resource kit tool to enable and disable Group Call Pickup for users.

Note:

The SEFAUtil parameter, /enablegrouppickup, enables Group Call Pickup and assigns the group number.

- Enable Group Call Pickup for Users
- Disable Group Call Pickup for Users

1.7.8.2.3.1 Enable Group Call Pickup for Users

Enable Group Call Pickup for Users

See Also

Managing Call Management Features > Managing Group Call Pickup > Enable or Disable Group Call Pickup for Users >

Topic Last Modified: *2013-01-30*

Use the SEFAUtil resource kit tool to enable Group Call Pickup for users. Users must be assigned a group number with type GroupPickup in the call park orbit table to have Group Call Pickup enabled. You assign a call pickup group number and enable Group Call Pickup at the same time by using the /enablegrouppickup parameter when you run SEFAUtil.exe.

To enable Group Call Pickup for a user

1. Log on to the computer where you installed the SEFAUtil tool with administrator rights.
2. At the command line, run:

```
SEFAUtil.exe sip:<sip address of user> /server:<pool FQDN> /enablegrou
```

For example:

```
SEFAUtil.exe katarina@contoso.com /server:pool01.contoso.com /enablegr
```

Tasks

Assign Group Call Pickup Numbers to Users
Disable Group Call Pickup for Users

1.7.8.2.3.2 Disable Group Call Pickup for Users

Disable Group Call Pickup for Users

See Also

Managing Call Management Features > Managing Group Call Pickup > Enable or Disable Group Call Pickup for Users >

Topic Last Modified: *2013-01-30*

Use the following procedure to disable Group Call Pickup for a user.

> **Note:**
> When you disable Group Call Pickup for a user, the call pickup group number that was assigned to the user is not retained. If you subsequently want to re-enable Group Call Pickup for that user, you must assign the call pickup group number again with the /enablegrouppickup parameter.

To disable Group Call Pickup for a user

1. Log on to the computer where you installed the SEFAUtil tool with administrator rights.
2. At the command line, run:

```
SEFAUtil.exe sip:<sip address of user> /server:<pool FQDN> /disablegro
```

For example:

```
SEFAUtil.exe katarina@contoso.com /server:pool01.contoso.com /disableg
```

Tasks

Assign Group Call Pickup Numbers to Users
Enable Group Call Pickup for Users

1.7.8.2.4 Manage Group Call Pickup During Disaster Recovery

Manage Group Call Pickup During Disaster Recovery

Operations > Managing Call Management Features > Managing Group Call Pickup >

Topic Last Modified: *2013-01-30*

When a Front End pool becomes unavailable due an unplanned incident, service is failed over to the backup pool. During failover to the backup pool, users are redirected to the backup pool and are in resiliency mode. While in resiliency mode, users cannot pick up other users' calls or have their calls picked up by other users. When failover is complete, users can again use Group Call Pickup as usual.

During failback to the primary pool, users are redirected to the primary pool and are again in resiliency mode. Group Call Pickup functionality is not available until the users are out of resiliency mode.

This section discusses some considerations for Group Call Pickup during disaster recovery and also describes the user experience.

Considerations for Group Call Pickup During Disaster Recovery

During disaster recovery, users who have been redirected to the backup pool as part of the failover process use the Call Park application running in the backup pool for the call pickup group numbers. Therefore, support for Group Call Pickup during disaster recovery requires the Call Park application to be deployed and enabled in both the primary pool and the backup pool.

The Group Call Pickup number ranges in the call park orbit table must be redirected to the backup pool after the failover process to the backup pool is complete. The number ranges must be redirected back to the primary pool after the failback process to the primary pool is complete. To redirect the Group Call Pickup ranges, use the **Set-CsCallParkOrbit** cmdlet.

If you deploy a new pool with a different fully qualified domain name (FQDN) to replace the primary pool, you need to reassign all the Group Call Pickup number ranges that were associated with the primary pool to the FQDN of the new pool. To reassign number ranges to the new pool, you can use the **Set-CsCallParkOrbit** cmdlet. For details about the **Set-CsCallParkOrbit** cmdlet, see Set-CsCallParkOrbit.

Group Call Pickup Experience During Pool Failure

The following table summarizes the Group Call Pickup experience through the phases of disaster recovery.

User Experience During Disaster Recovery

Call state	Failover to backup pool	Failback to primary pool

New calls	**During failover process:** • Group Call Pickup not available for users in resiliency mode **After failover is complete:** • Group Call Pickup available when users out of resiliency and Group Call Pickup number ranges are redirected to backup pool	**During failback process:** • Group Call Pickup not available for users in resiliency mode **After failback is complete:** • Group Call Pickup available when users out of resiliency and Group Call Pickup number ranges are redirected back to primary pool
Calls in Group Call Pickup queue	**During failover process:** • Calls in queue cannot be answered through Group Call Pickup. **After failover is complete:** • No calls in this state	**During failback process:** • Calls in queue cannot be answered through Group Call Pickup. **After failback is complete:** • Calls in queue cannot be answered through Group Call Pickup.
Established call	**During failover process:** • Calls stay connected **After failover is complete:** • Calls stay connected	**During failback process:** • Calls stay connected **After failback is complete:** • Calls stay connected

1.7.8.3 Managing Response Groups

Managing Response Groups

Microsoft Lync Server 2013 > Operations > Managing Call Management Features >

***Topic Last Modified:** 2012-10-01*

Response groups are a call management feature that enables you to queue calls that are made to a specific area, such as a Help Desk, and then route the calls to a designated group of people, called *agents*.

To manage response groups, you configure agent groups, queues, and workflows, which define what happens to a call from the time it is placed until an agent answers it.

Note:

If you have more than 300 workflows in a single pool in your Response Group deployment, it is better to use Lync Server Management Shell cmdlets to create the workflows. If you use the Response Group Configuration Tool to create workflows for a pool that has more than 300 workflows, the webpage takes a long time to load.

Topics in this section provide step-by-step procedures for tasks that you can perform to customize and maintain the Response Group application in your deployment

- Managing Response Group Agent Groups
- Managing Response Group Queues
- Managing Response Group Workflows
- Managing Application-Level Response Group Settings
- Moving Response Groups to a New Pool
- Managing Response Groups During a Disaster

1.7.8.3.1 Managing Response Group Agent Groups

Managing Response Group Agent Groups

Operations > Managing Call Management Features > Managing Response Groups >

Topic Last Modified: *2012-10-01*

An agent group consists of a group of people who are designated to answer calls to a response group. When you create an agent group, you select the agents who are assigned to the group and specify additional group settings, such as the routing method and whether an agent can sign in to and out of the group.

Note:

Users must be enabled for Enterprise Voice before you can add them to agent groups. For details about how to enable a user for Enterprise Voice, see Enable Users for Enterprise Voice.

Note:

Only on-premises users can be agents. If an agent is moved from on-premises to online, Response Group calls will not be routed to that agent.

An agent who must sign in and out of the group, which is different from signing in or out of Lync Server, is called a *formal agent*. Formal agents must be signed in to the group before they can receive calls that are routed to the group. This can be useful for agents who answer calls from the group on a part-time basis. Formal agents sign in and out of their groups by clicking a menu item in Lync 2013 to open the Windows Internet Explorer Internet browser and display a webpage console.

An agent who does not sign in or out of the group is called an *informal agent*. Informal agents are automatically signed in to the group when they sign in to Lync Server, and they cannot sign out of the group.

Important:

When you assign users as response group agents, inform them that, if they have Privacy mode enabled, they need to search for "RGS Presence Watcher" contacts and add them to their Contacts list. Agents who have Privacy mode enabled, but who do not have "RGS Presence Watcher" in their Contacts list, cannot receive calls to the response group. Agents who do not have Privacy mode enabled are not affected.

- Create or Modify an Agent Group
- Delete an Agent Group

1.7.8.3.1.1 Create or Modify an Agent Group

Create or Modify an Agent Group

See Also

Deploying Call Management Features > Configuring Response Group > Create Response Group Agent Groups >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to create or modify an agent group.

Note:

An Administrator—for example, CsVoiceAdministrator—must enable users for Enterprise Voice and Lync Server before the users can be assigned to agent groups. If you are one of the delegated Response Group Managers for a managed workflow, you can create agent groups and use the agent groups in the workflows that you manage.

Important:

When you assign users as response group agents, inform them that, if they have Privacy mode enabled, they need to search for "RGS Presence Watcher" contacts and add them to their Contacts list. Agents who have Privacy mode enabled, but who do not have "RGS Presence Watcher" in their Contacts list, cannot receive calls to the response group. Agents who do not have Privacy mode enabled are not affected.

⊟To use Lync Server Control Panel to create or modify an agent group

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.

   Note:

   If you are one of the delegated Response Group Managers for a managed workflow, you can create groups and use them in the workflows that you manage.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Group**.
4. On the **Group** page, do one of the following:
   - To create a new agent group, click **New**. In the **Select a Service** search field, type all or part of the name of the **ApplicationServer** service where you want to add the group. In the resulting list of services, click the service that you want, and then click **OK**.
   - To modify an existing agent group, type all or part of the name of the agent group in the search field. In the resulting list, click the group that you want, click **Edit**, and then click **Show details**.
5. In **Name**, type an identifying name for the agent group.
6. In **Description**, type a description for the group.
7. In the **Participation policy**, select one of the following to set up the sign-in behavior for the group:
   - Select **Informal** to specify that agents in the group do not need to sign in and out of the group. Agents are automatically signed in to the group when they sign in to Lync Server 2013.
   - Select **Formal** to specify that agents in the group must sign in and out of the group. When you select this option, agents click a menu item in Lync to open Internet Explorer and display a webpage console for signing in and out of the group.
8. In **Alert time (seconds)**, specify the number of seconds to ring an agent before offering the call to the next available agent (the default is 20 seconds).

   Important:

   The agent alert time setting cannot exceed 180 seconds. If the agent alert time exceeds 180 seconds, the client application rejects the call because the SIP transaction timer reaches its maximum wait time.

9. In **Routing method**, select the method for routing calls to agents in the group as follows:
   - To offer a new call first to the agent who has been idle the longest (has had a presence of **Available** or **Inactive** in Lync Server the longest), click **Longest idle**.
   - To offer a new call to all available agents at the same time, click **Parallel**. The call is sent to the first agent who accepts it.
   - To offer a new call to each agent in turn, click **Round robin**.
   - To always offer a new call to the agents in the order in which they are listed in the **Agent** list, click **Serial**.
   - To offer a new call to all agents who are signed into Lync Server 2013 and

the Response Group application at the same time, regardless of their current presence, click **Attendant**. Lync 2010 Attendant users who are configured as agents can see all the calls that are waiting and answer waiting calls in any order. The call is sent to the first agent who accepts it, after which the other Lync 2010 Attendant users no longer see the call.

10. In **Agents**, specify how you want to create your agents list:
    - To use a custom list of agents, click **Define a custom group of agents**, and do one of the following:
      - To add a user to the agent group, click **Select**, and then in the **Select Agents** search field, type all or part of the name of the user that you want to add to this group, and then click **Find**. In the resulting list of agents, click the user, and then click **OK**.
      - To remove a user from the agent group, in the list of agents, click the user you want to remove, and then click **Remove**.
      - To change the order in which agents are offered calls in groups that use either round robin routing or serial routing, in the list of agents, click a user, and then click the up arrow or down arrow.
    - To use a Microsoft Exchange Server distribution list as your agent group, click **Use an existing email distribution list**, and then in **Distribution list address**, type the email address of the distribution list (for example, NetworkSupport@contoso.com).

      If you use an email distribution list, you are subject to the following constraints:

      - You cannot select multiple distribution lists for the agent group. Each group supports only a single distribution list.
      - If the distribution list contains one or more distribution lists, members of the nested distribution lists are not added to the agent list.
      - If serial or round robin routing is selected, the server offers an incoming call to the appropriate agent according to the routing method and according to the order in which agents are listed in the distribution list.

      > **Important:**
      > If you use an email distribution list, hidden memberships or hidden lists might become visible to the Response Group administrator or users.

      Hidden memberships or hidden lists can become visible as follows:

      - If a distribution list was configured so that the membership is hidden and the Response Group administrator assigns the distribution list to the agent list, users can call the group to find out who the members are.
      - If a distribution list was configured so that it is hidden in the Exchange Global Address List, the Response Group administrator might be able to see the distribution list and assign it to the agent list if the Response Group process has the appropriate user rights and permissions, even if the administrator does not have the appropriate user rights and permissions.
11. Click **Commit**.

To use Windows PowerShell to create or modify an agent group

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Retrieve the service name for the Response Group service and assign it to a variable. At the command line, run:

   ```
   $serviceId="service:"+(Get-CsService | ?{$_.Applications -Like "*RGS*"
   ```

   > **Note:**

> If you run **Get-CsService** in a topology that has multiple pools, the variable $serviceId returns an array of all the service elements found in the topology.

4. Use **New-CsRgsAgentGroup** to create a new agent group. Use **Set-CsRgsAgentGroup** to modify an existing agent group. At the command line, run:

   ```
   $ag = New-CsRgsAgentGroup -Name "<agent group name>" -Parent $serviceI
   ```

   For example:

   ```
   $ag = New-CsRgsAgentGroup -Name "Help Desk" -Parent $serviceId -Descri
   ```

   > ◆**Important:**
   >
   > The agent alert time setting cannot exceed 180 seconds. If the agent alert time is greater than 180 seconds, the client application rejects the call because the SIP transaction timer reaches its maximum wait time.

5. Confirm that the agent group is created. Run:

   ```
   Get-CsRgsAgentGroup -Name "Help Desk"
   ```

Tasks

Delete an Agent Group

Other Resources

Managing Response Group Agent Groups
Get-CsService
New-CsRgsAgentGroup
Set-CsRgsAgentGroup
Get-CsRgsAgentGroup

1.7.8.3.1.2 Delete an Agent Group

Delete an Agent Group

See Also

Managing Call Management Features > Managing Response Groups > Managing Response Group Agent Groups >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to delete an agent group.

⊟To use Lync Server Control Panel to delete an agent group

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Group**.
4. On the **Response Groups** page, type all or part of the name of the agent group that you want to delete in the search field.
5. In the resulting list, click the group that you want to delete, click **Edit**, and then click **Delete**.
6. Click **OK**.

⊟To use Windows PowerShell to delete an agent group

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

3. At the command line, run:

```
Get-CsRgsAgentGroup -Identity <Application Server service> -Name "<nam
```

For example:

```
Get-CsRgsAgentGroup -Identity service:ApplicationServer:redmond.contos
```

Tasks

Create or Modify an Agent Group

Other Resources

Remove-CsRgsAgentGroup
Get-CsRgsAgentGroup

1.7.8.3.2 Managing Response Group Queues

Managing Response Group Queues

Operations > Managing Call Management Features > Managing Response Groups >

Topic Last Modified: *2012-10-02*

Queues hold calls to a response group until an agent answers the call. When you manage a queue, you assign one or more agent groups to the queue and specify queue settings, such as the number of calls that the queue can hold before performing an overflow action and the length of time that a call waits for an agent before performing a time-out action. When the Response Group application searches for an available agent, it searches agent groups in the order that you list them.

- Create or Modify a Queue
- Delete a Response Group Queue

1.7.8.3.2.1 Create or Modify a Queue

Create or Modify a Queue

See Also

Deploying Call Management Features > Configuring Response Group > Create Response Group Queues >

Topic Last Modified: *2013-02-23*

Use one of the following procedures to create or modify a queue.

To use Lync Server Control Panel to create or modify a queue

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.

   Note:
   If you are one of the delegated Response Group Managers for a managed workflow, you can create or modify response group queues and assign them to the workflows that you manage.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Queue**.
4. On the **Queue** page, do one of the following:
   - To create a new queue, click **New**. In **Select a Service**, type part or all of the name of the **ApplicationServer** service where you want to add the queue in the search field. In the resulting list of services, click the service

that you want, and then click **OK**.
- To modify an existing queue, type all or part of the queue name in the search field. In the resulting list of queues, click the queue that you want, click **Edit**, and then click **Show details**.

5. In **Name**, type an identifying name for the queue.
6. In **Description**, type a description for the queue.
7. In **Groups**, specify the groups you want to assign to the queue. Do one of the following:
   - To add a group to the queue, click **Select**. In the **Select Groups** search field, type all or part of the name of the agent group that you want to assign to the queue, click the agent group that you want, and then click **OK**.
   - To remove a group from the queue, in the list of agent groups, click the group that you want to remove, and then click **Remove**.
   - To change the order in which agents are searched, in the list of agent groups, click a group, and then click the up arrow or down arrow.

Note:

When the server searches for an available agent for the queue, it uses group order. That is, the first group in the list is searched first, followed by the second group in the list, and so on.

8. To specify a maximum period of time for a caller to wait on hold before an agent answers the call, select the **Enable queue time-out** check box, and then do the following:
   - In **Time-out period (seconds)**, specify the maximum number of seconds a caller waits for an agent to answer the call.
   - In **Call Action**, select the action that occurs when a call times out as follows:
   - To disconnect the call after the timeout, click **Disconnect**.
   - To forward the call to voice mail, click **Forward to voice mail**, and then in the **SIP address** field, type a voice mail address in the format sip:<*username*>@<*domainname*> (for example, sip:bob@contoso.com).
   - To forward the call to another telephone number, click **Forward to telephone number**, and then in the **SIP address** field, type the telephone number in the format sip:<*number*>@<*domainname*> (for example, sip:+14255550121@contoso.com).
   - To forward the call to another user, click **Forward to SIP address**, and then in the **SIP address** field, type the URI for the user in the format sip:<*username*>@<*domainname*>.
   - To forward the call to another queue, click **Forward to another queue**, and then browse to the queue that you want to use.
9. To specify a maximum number of calls that the queue can hold, select the **Enable queue overflow** check box, and then do the following:
   - In **Maximum number of calls**, select the maximum number of calls that you want the queue to hold.
   - In **Forward the call**, select which call is to be forwarded when the queue is full: **Newest Call** or **Oldest Call**.
   - In **Call action**, select the action that occurs when the overflow threshold is met as follows:
   - To disconnect the call after the timeout, click **Disconnect**.
   - To forward the call to voice mail, click **Forward to voice mail**, and then in the **SIP address** field, type a voice mail address in the format sip:<*username*>@<*domainname*> (for example, sip:bob@contoso.com).
   - To forward the call to another telephone number, click **Forward to telephone number**, and then in the **SIP address** field, type the telephone number in the format sip:<*number*>@<*domainname*> (for example, sip:+14255550121@contoso.com).
   - To forward the call to another user, click **Forward to SIP address**, and then in the **SIP address** field, type the URI for the user in the format

sip:*<username>*@*<domainname>*.

- To forward the call to another queue, click **Forward to another queue**, and then browse to the queue that you want to use.

10. Click **Commit**.

To use Windows PowerShell to create or modify a queue

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.

   > **Note:**
   > If you are one of the delegated Response Group Managers for a managed workflow, you will be able to create agent groups and queues, and assign agent groups to queues.

2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Create the prompt to be played when the queue timeout threshold is met, and save it in a variable. At the command line, run:

   ```
   $promptTO = New-CsRgsPrompt -TextToSpeechPrompt "<text for TTS prompt>
   ```

   For example:

   ```
   "All agents are currently busy. Please call back later."
   ```

   > **Note:**
   > To use an audio file for the prompt, use the **Import-CsRgsAudioFile** cmdlet. For details, see Import-CsRgsAudioFile.

4. Define the action to be taken when the queue timeout threshold is met, and save it in a variable. At the command line, run:

   ```
   $actionTO = New-CsRgsCallAction -Prompt <saved prompt from previous st
   ```

   > **Note:**
   > For details about possible actions and their syntax, see New-CsRgsCallAction.

   For example:

   ```
   $action = New-CsRgsCallAction -Prompt $promptTO -Action Terminate
   ```

5. Create the prompt to be played when the queue overflow threshold is met, and save it in a variable. At the command line, run:

   ```
   $promptOV = New-CsRgsPrompt -TextToSpeechPrompt "<text for TTS prompt>
   ```

   For example:

   ```
   $promptOV = New-CsRgsPrompt -TextToSpeechPrompt "Too many calls are wa
   ```

   > **Note:**
   > To use an audio file for the prompt, use the **Import-CsRgsAudioFile** cmdlet. For details, see Import-CsRgsAudioFile.

6. Define the action to be taken when the queue overflow threshold is met, and save it in a variable. At the command line, run:

   ```
   $actionOV = New-CsRgsCallAction -Prompt <saved prompt from previous st
   ```

   > **Note:**
   > For details about possible actions and their syntax, see New-CsRgsCallAction.

   For example:

   ```
   $action = New-CsRgsCallAction -Prompt $promptOV -Action Terminate
   ```

7. Retrieve the service name for the Response Group service and assign it to a variable. At the command line, run:

```
$serviceId="service:"+(Get-CSService | ?{$_.Applications -Like "*RGS*"
```

8. Get the identity of the agent group to be assigned to the queue. At the command line, run:

   ```
   $agid = (Get-CsRgsAgentGroup -Name "Help Desk").Identity;
   ```

   > **Note:**
   > For details about creating the agent group, see New-CsRgsAgentGroup

9. Create the queue. At the command line, run:

   ```
   $q = New-CsRgsQueue -Parent <saved service ID from previous step> -Nam
   ```

   For example:

   ```
   $q = New-CsRgsQueue -Parent $serviceId -Name "Help Desk" -Description
   ```

10. Confirm that the queue is created. Run:

    ```
    Get-CsRgsQueue -Name "Help Desk"
    ```

Other Resources

New-CsRgsQueue
Set-CsRgsQueue
New-CsRgsPrompt
New-CsRgsCallAction
Get-CsRgsQueue
Import-CsRgsAudioFile
Remove-CsRgsQueue

1.7.8.3.2.2 Delete a Response Group Queue

Delete a Response Group Queue

Managing Call Management Features > Managing Response Groups > Managing Response Group Queues >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to delete a queue.

⊟To use Lync Server Control Panel to delete a queue

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Queue**.
4. In the search field, type part or all of the name of the queue you want to delete.
5. In the list of queues, click the queue that you want, click **Edit**, and then click **Delete**.
6. Click **OK**.

⊟To use Windows PowerShell to delete a queue

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. At the command line, run:

```
Get-CsRgsQueue -Identity <Application Server service> -Name "<name of
```

For example:

```
Get-CsRgsQueue -Identity service:ApplicationServer:redmond.contoso.com
```

1.7.8.3.3 Managing Response Group Workflows

Managing Response Group Workflows

Operations > Managing Call Management Features > Managing Response Groups >

Topic Last Modified: *2012-10-01*

A Response Group workflow defines the behavior of a call from the time that the phone rings to the time that an agent answers the call. The workflow includes queue and routing information, and includes either hunt group or interactive voice response (IVR) information.

Topics in this section identify best practices for designing IVR workflows, and explain how to create customized business hours and holiday sets, how to create or modify workflows, and how to delete workgroups.

- Design Interactive Voice Response Call Flows
- (Optional) Define Response Group Business Hours
- (Optional) Define Response Group Holiday Sets
- Create or Modify a Workflow
- Delete a Workflow

1.7.8.3.3.1 Design Interactive Voice Response Call Flows

Design Interactive Voice Response Call Flows

Deploying Call Management Features > Configuring Response Group > Create Response Group Workflows >

Topic Last Modified: *2013-02-25*

You can use interactive voice response (IVR) to obtain information from callers and direct the call to the appropriate queue. Question-and-answer pairs determine which queue to use. Depending on the caller’s response, the caller either hears a follow-up question, or is routed to the appropriate queue. The IVR questions and the caller’s responses are provided to the responding agent who accepts the call, providing valuable information to the agent.

Overview of IVR Features

The Response Group application offers speech recognition and text-to-speech capabilities in 26 languages. You can enter IVR questions using text-to-speech or a wave (.wav) or Windows Media audio (.wma) file. Callers can respond by using voice or dual-tone multifrequency (DTMF) responses.

Interactive workflows support up to two levels of questions, with each question having up to four possible answers. The IVR asks the caller a question, and depending on the caller’s response, routes the caller to a queue or asks a second question. The second question can also have four possible answers. Depending on the answer to the second-level question, the caller is routed to the appropriate queue.

Note:
When you design call flows by using Lync Server Management Shell, you can define any number levels of IVR questions and any number of answers. However, for caller usability, we recommend that you not use more than three levels of questions, with not more than five answers each. In addition, if you design a call flow that has more than two levels of questions with more than four answers each, you cannot edit the call flow by using Lync Server 2013 Control Panel.

The IVR questions and the caller’s responses are provided to the responding agent who accepts the call.

Working with Speech Technologies

Speech technologies, such as speech recognition and text-to-speech, can enhance customer experience and let people access information more naturally and effectively. However, there can be cases where the specified text or the user voice response is not recognized correctly by the speech engine. For example, the "#" symbol is translated by the text-to-speech engine as the word "number." This issue can be mitigated by the following:

- The speech engine gives the caller five attempts to answer the question. If the caller answers the question incorrectly (that is, the answer is not one of the specified responses) or does not provide an answer at all, the caller gets another chance to answer the question. The caller has five attempts to answer the question before being disconnected. You can configure the IVR to play a customized message after each caller error. The question is repeated each time.
- To minimize the potential for ambient noise to be interpreted by the speech engine as a response, use longer responses. For example, responses should have more than one syllable and should sound significantly different from each other.
- If your questions have both speech and DTMF responses, configure the speech responses with words that represent the concept rather than the DTMF response. For example, instead of using "Press or say one" use "Press 1 or say billing."
- After you design your IVR, call the workflow, listen to the prompts, respond to each of the prompts using voice, and verify that the IVR sounds and behaves as expected. You can then modify the IVR to fix any interpretation issues. Following the previous example, if you need to refer to the # key, you can rewrite your IVR prompt to use the key name, rather than the # symbol. For example, "To talk to sales, press the pound key."

IVR Design Examples

The following sections contain examples of different IVR scenarios and question-and-answer pairs.

IVR with One Level of Questions

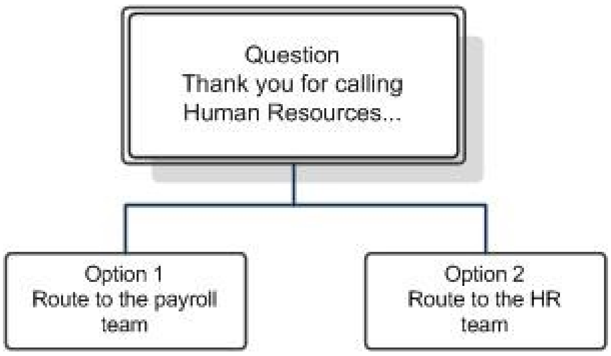
The following example shows an IVR that uses one level of questions. It uses speech recognition to detect the caller’s response.

Question: "Thank you for calling Human Resources. If you would like to speak to payroll, say payroll. Otherwise, say HR."

- **Option 1 is selected:** The caller is routed to the payroll team.
- **Option 2 is selected:** The caller is routed to the human resources team.

The following figure shows the call flow.

One-level interactive call flow



IVR with Two Levels of Questions

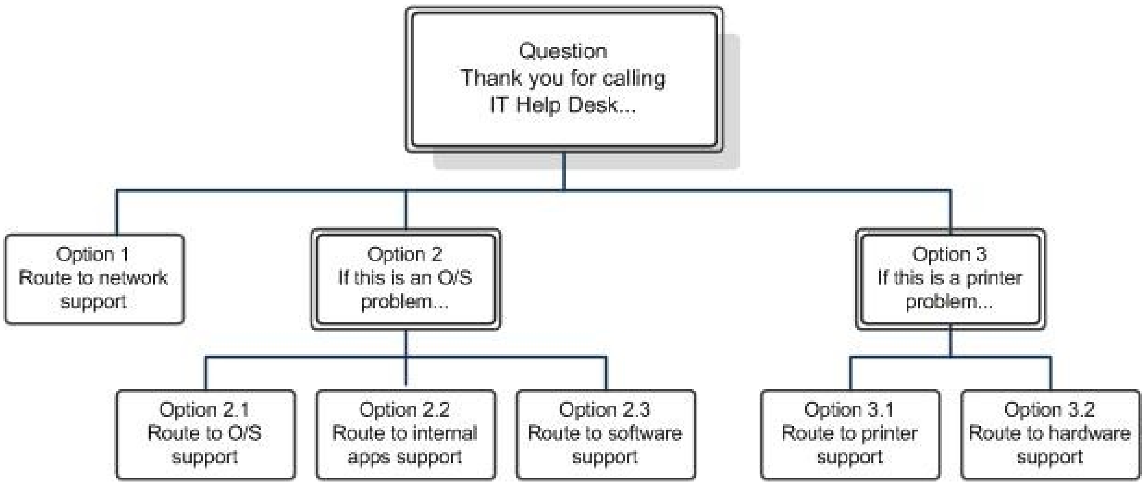
The following example shows an IVR that uses two levels of questions. It allows callers to respond using either speech or DTMF keypad input.

Question: "Thank you for calling the IT Help Desk. If you have a network access problem, press 1 or say network. If you have a software problem, press 2 or say software. If you have a hardware problem, press 3 or say hardware."

- **Option 1 is selected:** The caller is routed to the network support team.
- **Option 2 is selected:** The caller is asked a follow-up question:
  Question: "If this is an operating system problem, press 1 or say operating system. If this is a problem with an internal application, press 2 or say internal application. Otherwise, press 3 or say other."
  - **Option 1 is selected:** The caller is routed to the operating systems support team.
  - **Option 2 is selected:** The caller is routed to the internal applications support team.
  - **Option 3 is selected:** The caller is routed to the software support team.
- **Option 3 is selected:** The caller is asked a follow-up question:
  Question: "If this is a printer problem press 1. Otherwise, press 2."
  - **Option 1 is selected:** The caller is routed to the printer support team.
  - **Option 2 is selected:** The caller is routed to the hardware support team.

The following figure shows the call flow.

Two-level interactive call flow



Best Practices

The following list describes some best practices for designing your IVR:

- Let the caller get to the task quickly. Avoid providing too much information or lengthy marketing messages in your IVR.
- If you want to include a lengthy message, consider appending it to the first question instead of to the welcome message. Callers can bypass the message if it is part of the first question by answering the question, but they cannot bypass the welcome message.
- Speak in the caller’s language. Avoid stilted language. Speak naturally.
- Write efficient and effective prompts. Remove any unnecessary options. Structure the information so that the caller’s expected response is at the end of the sentence. For example, “To speak to the sales team, press 1."
- Make voice responses user friendly. For example, if you specify both DTMF and voice responses, use something like: "To speak to the sales team, press 1 or say sales."
- Test the IVR on a group of users before you deploy it across your organization.

1.7.8.3.3.2 (Optional) Define Response Group Business Hours

(Optional) Define Response Group Business Hours

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-11-01*

Defining Business Hours

Business hour settings define when the workflow is available to answer calls and specify the actions to take for calls outside of business hours. Response Group administrators can use the **New-CsRgsHoursOfBusiness** cmdlet to create predefined schedules that you can use for any number of response groups.

Tip:

When you create or modify a workflow, you can specify a custom schedule that applies only to that workflow. For details, see Create or Modify a Hunt Group Workflow or Create or Modify an Interactive Workflow.

Note:

If a workflow is defined as a Managed workflow, then any user who is assigned the CsResponseGroupManager role can set and modify custom business hours for workflows that they manage.

Important:

Use 24-hour notation for the parameters in the following cmdlets (for example, 20:00=8:00 P.M.).

To create a predefined business hours collection

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. For each unique range of hours you want to define, run:

```
$x = New-CsRgsTimeRange [-Name <name of time range>] -OpenTime <time w
```

To create the business hours collection that uses the ranges you defined, run:

```
New-CsRgsHoursOfBusiness -Parent <service where the workflow is hosted
```

The following example specifies business hours of 9:00 A.M. to 5:00 P.M. for weekdays, 8:00 A.M. to 10:00 A.M. and again from 2:00 P.M. to 6:00 P.M. for Saturdays, and no business hours for Sundays:

```
$a = NewRgsTimeRange -Name "Weekday Hours" -OpenTime "9:00" -CloseTime
$b = NewRgsTimeRange -Name "Saturday Morning Hours" -OpenTime "8:00" -
$c = NewRgsTimeRange -Name "Saturday Afternoon Hours" -OpenTime "14:00
New-CsRgsHoursOfBusiness -Parent "ApplicationServer:Redmond.contoso.co
```

See Also

Concepts

Create or Modify a Hunt Group Workflow
Create or Modify an Interactive Workflow

Other Resources

New-CsRgsTimeRange
New-CsRgsHoursOfBusiness

1.7.8.3.3.3 (Optional) Define Response Group Holiday Sets

(Optional) Define Response Group Holiday Sets

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-11-01*

Holiday settings define the days that a response group is closed for business and specify the action to take on those days. A holiday set is the collection of holidays that apply to a response group.

Note:

If a workflow is defined as a Managed workflow, then any user is assigned the CsResponseGroupManager role can set and modify holidays for workflows that they manage.

To create a holiday set

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. For each holiday you want to define, run:

```
$x = New-CsRgsHoliday [-Name <holiday name>] -StartDate <starting date
```

To create the holiday set that contains the holidays you defined, run:

```
New-CsRgsHolidaySet -Parent <service where the workflow is hosted> -Na
```

The following example shows a holiday set that includes two holidays:

```
$a = New-CsRgsHoliday -Name "New Year's Day" -StartDate "1/1/2013" -En
$b = New-CsRgsHoliday -Name "Independence Day" -StartDate "7/4/2013" -
New-CsRgsHolidaySet -Parent "ApplicationServer:Redmond.contoso.com -Na
```

Concepts

Create or Modify a Hunt Group Workflow
Create or Modify an Interactive Workflow

Other Resources

New-CsRgsHoliday
New-CsRgsHolidaySet

1.7.8.3.3.4 Create or Modify a Workflow

Create or Modify a Workflow

See Also

Managing Call Management Features > Managing Response Groups > Managing Response Group Workflows >

Topic Last Modified: *2012-10-02*

Lync Server 2013 supports two types of workflows: hunt group and interactive voice response (IVR). When you create a workflow, you use the Response Group Configuration Tool to specify the queue to use and other settings, such as a welcome message, music on hold, business hours, and questions that the Response Group application asks the caller.

Note:
You must create agent groups and queues before you create a workflow that uses them. If you want to create predefined business hours and holidays that you can use for multiple workflows, you must also define these hours and holidays before you create a workflow that uses them.

- Create or Modify a Hunt Group Workflow
- Create or Modify an Interactive Workflow

See Also

Tasks

Create or Modify an Agent Group
Create or Modify a Queue
(Optional) Define Response Group Holiday Sets

Concepts

(Optional) Define Response Group Business Hours

Create or Modify a Hunt Group Workflow

See Also

Deploying Call Management Features > Configuring Response Group > Create Response Group Workflows >

Topic Last Modified: *2012-11-27*

Use one of the following procedures to create or modify a hunt group workflow.

Note:
You can use Lync Server Management Shell or the Response Group Configuration Tool to create and modify hunt group workflows. You can access the Response Group Configuration Tool from Lync Server Control Panel, or by opening the webpage directly from a web browser by typing the following URL: **https://***<webPoolFqdn>***/RgsConfig**.

To use Response Group Configuration Tool to create or modify a hunt group workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Workflow**.
4. On the **Workflow** page, click **Create or edit a workflow**.
5. In the **Select a Service** search field, type all or part of the name of the **ApplicationServer** service that hosts the workflow that you want to create or change. In the resulting list of services, click the service that you want, and then click **OK**.

   Note:

   The Response Group Configuration Tool opens. You can also open the Response Group Configuration Tool directly from a web browser by typing the following URL: **https://**<*webPoolFqdn*>**/RgsConfig**.

6. Do one of the following:
   - Under **Create a New Workflow**, next to **Hunt Group, click Create**.
   - Under **Manage an Existing Workflow**, locate the workflow you want to change, and then under **Action**, click **Edit**.
7. If you are ready for users to start calling the workflow, select **Activate the workflow**.

   Note:

   If you are to creating a managed workflow, you need to select **Activate the workflow**. After you save the active, managed workflow, you can then modify and deactivate it.

8. To allow federated users to call the group, select the **Enable for federation** check box. You must also have an external access policy that applies to the Response Group application configured for federation.

   Note:

   The global external access policy applies to the Response Group application. You can configure the global policy for response group federation by using Lync Server Control Panel or by using the **Set-CsExternalAccessPolicy** cmdlet to set the EnableOutsideAccess parameter to True. Keep in mind that global policy settings apply to all users unless they are assigned a site or user policy. Therefore, before changing this setting for response groups, make sure that the federation setting meets the requirements of your organization. For details about how policies apply to users, see Manage External Access Policy for Your Organization. For details about the federation setting, see Set-CsExternalAccessPolicy.

9. To hide the identity of agents during calls, select the **Enable agent anonymity** check box.

   Note:

   Anonymous calls cannot start with instant messaging (IM) or video, although the agent or the caller can add IM and video after the call is established. An anonymous agent can also put calls on hold, transfer calls (both blind and consultative transfers), and park and retrieve calls. Anonymous calls do not support conferencing, application sharing and desktop sharing, file transfer, whiteboarding and data collaboration, and call recording. Agents using the Lync VDI Plugin can receive incoming calls anonymously, but they cannot

> make outgoing calls anonymously.

10. Under **Enter the address of the group that will receive the calls**, type the primary SIP uniform resource identifier (URI) address of the group that will answer calls to the workflow.

> **Note:**
>
> The primary URI for a workflow is how the workflow is identified and referenced. The SIP URI that you enter is created as a contact object in Active Directory Domain Services (AD DS). To create the URI, the object must be unique in Active Directory.

11. In **Display name**, type the name that you want to display for the workflow (for example, Sales Response Group).

> **Note:**
>
> Do not include the "<" or ">" characters in the display name. Do not use the following display names because they are reserved: **RGS Presence Watcher** or **Announcement Service**.

12. Under **Telephone number**, type the line URI for the response group (for example, +14255550165).
13. In **Display number**, type the number as you want it to appear for the response group (for example, +1 (425) 555-0165).
14. (Optional) In **Description**, type a description for the workflow as you want it to appear on the contact card in Lync client.
15. In **Workflow Type**, select **Managed** if this workflow will be managed by a Response Group Manager. Do the following to assign Response Group Managers to the workflow:
    - Type the SIP URI of a manager for this workflow, and click **Add**.
    - Type the SIP URI of additional managers to add to the workflow, and click **Add**.

> **Important:**
>
> Every user who is designated as a manager of a response group must be assigned the CsResponseGroupManager role. If users are not assigned this role, they cannot manage response groups.

16. Under **Step 2 Select a Language**, click the language that you want to use for speech recognition and text-to-speech.
17. If you want to configure a welcome message, under **Step 3 Configure a Welcome Message**, select the **Play a welcome message** check box, and then do one of the following:
    - To enter the welcome message as text that is converted to speech for callers, click **Use text-to-speech**, and then type the welcome message in the text box.

      > **Note:**
      >
      > Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

    - To use a wave (.wav) or Windows Media audio (.wma) file recording for the welcome message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the audio file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

      > **Note:**
      >
      > All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

18. Under **Step 4 Specify Your Business Hours**, in **Your time zone**, click the time zone for the workflow.

Note:
The time zone is the time zone where the callers and agents of the workflow reside. It is used to calculate the open and close hours. For example, if the workflow is configured to use the North American Eastern Time zone and the workflow is scheduled to open at 7:00 A.M. and close at 11:00 P.M., the open and close times are assumed to be 7:00 Eastern Time and 23:00 Eastern Time respectively. (You must enter the times in 24-hour time notation.)

19. Select the type of business hours schedule you want to use by doing one of the following:
    - To use a predefined schedule of business hours, click **Use a preset schedule**, and then select the schedule you want to use from the drop-down list.

      Note:
      You must have defined at least one preset schedule previously to be able to select this option. You define preset schedules by using the **New-CSRgsHoursOfBusiness** cmdlet. For details, see (Optional) Define Response Group Business Hours.

      Note:
      When you select a preset schedule, **Day**, **Open**, and **Close** are automatically filled with the days and hours that the response group is available.

    - To use a custom schedule that applies only to this workflow, click **Use a custom schedule**.
20. If you are creating a custom schedule for this workflow, click the check boxes for the days of the week that the response group is available.
21. If you are creating a custom schedule, type the **Open** and **Close** hours for each day of the week that the response group available.

Note:
The **Open** and **Close** hours must be in 24-hour time notation. For example, if your office works a 9-to-5 work day and closes at noon for lunch, the business hours are specified as **Open** 9:00, **Close** 12:00, **Open** 13:00, and **Close** 17:00.

22. If you want to play a message when the office is not open, select the **Play a message when the response group is outside of business hours** check box, and then specify the message to play by doing one of the following:
    - To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

      Note:
      Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

    - To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

      Note:
      All user-provided audio files must meet certain requirements. For details about supported audio file formats, see Technical Requirements for Response Groups.

23. Specify how to handle calls after the message is played (if a message is configured):
    - To disconnect the call, click **Disconnect Call**.
    - To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is

<username>@*<domainName>* (for example, bob@contoso.com).

- To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is *<username>*@*<domainName>*.
- To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is *<number>*@*<domainName>* (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.

24.Under **Step 5 Specify Your Holidays**, click the check boxes for one or more sets of holidays that define the days when the response group is closed for business.

> **Note:**
> You need to define holidays and holiday sets before you configure the workflow. Use the **New-CsRgsHoliday** and **New-CsRgsHolidaySet** cmdlets to define holidays and holiday sets. For details, see (Optional) Define Response Group Holiday Sets.

25.If you want to play a message on holidays, select the **Play a message during holidays** check box, and then specify the message to play by doing one of the following:

- To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

  > **Note:**
  > Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

  > **Note:**
  > All user-provided audio files must meet certain requirements. For details about supported audio file formats, see Technical Requirements for Response Groups.

26.Specify how to handle calls after the message is played (if a message is configured):

- To disconnect the call, click **Disconnect Call**.
- To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is *<username>*@*<domainName>* (for example, bob@contoso.com).
- To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is *<username>*@*<domainName>*.
- To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is *<number>*@*<domainName>* (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.

27.Under **Step 6 Configure a Queue**, in **Select the queue that will receive the calls**, select the queue that you want to hold callers until an agent becomes available.

28.Under **Step 7 Configure Music on Hold**, choose the music you want callers to listen to while waiting for an agent by doing one of the following:

- To use the default music-on-hold recording, click **Use default**.
- To use an audio file recording for the music on hold, click **Select a music file**. If you want to upload a new audio file, click the **a music file** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

Note:
All user provided audio files must meet certain requirements. For details about supported audio file formats, see Technical Requirements for Response Groups.

29. Click **Deploy**.

To use Windows PowerShell to create or modify a hunt group workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Create the prompt to be played for the welcome message, and save it in a variable. At the command line, run:

   ```
   $promptWM = New-CsRgsPrompt -TextToSpeechPrompt "<text for TTS prompt>
   ```

   For example:

   ```
   $promptWM = New-CsRgsPrompt -TextToSpeechPrompt "Welcome to Contoso. P
   ```

   Note:
   To use an audio file for the prompt, use the **Import-CsRgsAudioFile** cmdlet. For details, see Import-CsRgsAudioFile.

4. Get the identity of the queue or question where the calls will be directed. At the command line, run:

   ```
   $qid = (Get-CsRgsQueue -Name "Help Desk").Identity
   ```

   For details about creating the queue, see New-CsRgsQueue.
5. Define the default action to be taken when a workflow is opened during business hours, and save it in a variable. At the command line, run:

   ```
   $actionWM = New-CsRgsCallAction -Prompt <saved prompt from previous st
   ```

   Note:
   For hunt group workflows, the default action must direct the call to a queue. This is parameter is required for active workflows. It is not required for inactive workflows.

   For example:

   ```
   $actionWM = New-CsRgsCallAction -Prompt $promptWM -Action TransferToQu
   ```

6. If you want to define business hours and holidays, you need to create them before you create or modify the workflow. For details, see (Optional) Define Response Group Business Hours and (Optional) Define Response Group Holiday Sets.
7. If you want to have prompts for calls that are received out of business hours or on holidays, use the **New-CsRgsPrompt** cmdlet to define the prompt, and use the **New-CsRgsCallAction** to define the action to be taken after the prompt. For details, see New-CsRgsPrompt and New-CsRgsCallAction.
8. Retrieve the service name for the Lync Server Response Group service and assign it to a variable. At the command, run:

   ```
   $serviceId="service:"+(Get-CSService | ?{$_.Applications -like "*RGS*"
   ```

9. Create or modify the workflow. To create a workflow, use **New-CsRgsWorkflow**. To modify a workflow, use **Set-CsRgsWorkflow**. At the command line, type:

   ```
   $workflowHG = New-CsRgsWorkflow -Parent <service ID for the Response G
   ```

   For example:

```
$workflowHG = New-CsRgsWorkflow -Parent $serviceID -Name "Human Resour
```

Important:

All users who are designated managers for workflows must be assigned the CsResponseGroupManager role.

Note:

For details about additional optional parameters, see New-CsRgsWorkflow or Set-CsRgsWorkflow

See Also

Tasks

(Optional) Define Response Group Holiday Sets

Concepts

(Optional) Define Response Group Business Hours

Other Resources

New-CsRgsWorkflow
Set-CsRgsWorkflow
New-CsRgsPrompt
New-CsRgsCallAction

Create or Modify an Interactive Workflow

Deploying Call Management Features > Configuring Response Group > Create Response Group Workflows >

Topic Last Modified: *2012-11-27*

Use one of the following procedures to create or modify an interactive workflow.

Note:

You can use Lync Server Management Shell or the Response Group Configuration Tool to create and modify interactive workflows. You can access the Response Group Configuration Tool from Lync Server Control Panel, or by opening the webpage directly from a web browser by typing the following URL: **https://***<webPoolFqdn>***/RgsConfig**.

To use Response Group Configuration Tool to create or modify an Interactive workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Workflow**.
4. On the **Workflow** page, click **Create or edit a workflow**.
5. In the **Select a Service** search field, type all or part of the name of the **ApplicationServer** service that hosts the workflow that you want to create or modify. In the resulting list of services, click the service that you want, and then click **OK**.

Note:

The Response Group Configuration Tool opens. You can also open the

Response Group Configuration Tool directly from a web browser by typing the following URL: **https://***<webPoolFqdn>***/RgsConfig**.

6. Do one of the following:
   - Under **Create a New Workflow**, next to **Interactive**, click **Create**.
   - Under **Manage an Existing Workflow**, locate the workflow you want to change, and then under **Action**, click **Edit**.
7. If you are not ready for users to start calling the workflow, clear the **Activate the workflow** check box.

Note:

If you are to creating a managed workflow, you need to select **Activate the workflow**. After you save the active, managed workflow, you can then modify and deactivate it.

8. To allow federated users to call the group, select the **Enable for federation** check box. You must also have an external access policy that applies to the Response Group application configured for federation.

Note:

The global external access policy applies to the Response Group application. You can configure the global policy for response group federation by using Lync Server Control Panel or by using the **Set-CsExternalAccessPolicy** cmdlet to set the EnableOutsideAccess parameter to True. Keep in mind that global policy settings apply to all users unless they are assigned a site or user policy. Therefore, before changing this setting for response groups, make sure that the federation setting meets the requirements of your organization. For details about how policies apply to users, see Manage External Access Policy for Your Organization. For details about the federation setting, see **Set-CsExternalAccessPolicy** in Lync Server Management Shell documentation.

9. To hide the identity of agents during calls, select the **Enable agent anonymity** check box.

Note:

Anonymous calls cannot start with instant messaging (IM) or video, although the agent or the caller can add IM and video after the call is established. An anonymous agent can also put calls on hold, transfer calls (both blind and consultative transfers), and park and retrieve calls. Anonymous calls do not support conferencing, application sharing and desktop sharing, file transfer, whiteboarding and data collaboration, and call recording. Agents using the Lync VDI Plugin can receive incoming calls anonymously, but they cannot make outgoing calls anonymously.

10. Under **Enter the address of the group that will receive the calls**, type the primary SIP uniform resource identifier (URI) address of the group that will answer calls to the workflow.
11. In **Display name**, type the name that you want to display for the workflow (for example, Sales IVR Response Group).

Note:

Do not include the "<" or ">" characters in the display name. Do not use the following display names because they are reserved: RGS Presence Watcher or Announcement Service.

12. In **Telephone number**, type the line URI for the response group (for example, +14255550165).
13. In **Display number**, type the number as you want it to appear for the response group (for example, +1 (425) 555-0165).
14. (Optional) In **Description**, type a description for the workflow that you want to appear on the contact card in the Lync client.
15. In **Workflow Type**, select **Managed** if this workflow will be managed by a Response Group Manager. Do the following to assign Response Group Managers to the workflow:

- Type the SIP URI of a manager for this workflow, and click **Add**..
- Type the SIP URI of additional managers to add to the workflow, and click **Add**..

Important:

Every user who is designated as a manager of a response group must be assigned the CsResponseGroupManager role. If users are not assigned this role, they cannot manage response groups.

16.Under **Step 2 Select a Language**, click the language to use for speech recognition and text-to-speech.

17.If you want to configure a welcome message, under **Step 3 Configure a Welcome Message**, select the **Play a welcome message** check box, and then do one of the following:

- To enter the welcome message as text that is converted to speech for callers, click **Use text-to-speech**, and then type the welcome message in the text box.

  Note:

  Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

- To use a Wave or Windows Media Audio file recording for the welcome message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the audio file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

  Note:

  All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

18.Under **Step 4 Specify Your Business Hours**, in the **Your time zone** box, click the time zone of the workflow.

Note:

The time zone is the time zone where the callers and agents of the workflow reside. It is used to calculate the open and close hours. For example, if the workflow is configured to use the North American Eastern Time zone and the workflow is scheduled to open at 7:00 A.M. and close at 11:00 P.M., the open and close times are assumed to be 7:00 Eastern Time and 11:00 Eastern Time respectively. (You must enter the times in 24-hour time notation.)

19.Select the type of business hours schedule you want to use by doing one of the following:

- To use a predefined schedule of business hours, click **Use a preset schedule**, and then select the schedule you want to use from the drop-down list.

  Note:

  You must have defined at least one preset schedule previously to be able to select this option. You define preset schedules by using the **New-CSRgsHoursOfBusiness** cmdlet. For details, see (Optional) Define Response Group Business Hours. When you select a preset schedule, **Day**, **Open**, and **Close** are automatically filled with the days and hours that the response group is available.

- To use a custom schedule that applies only to this workflow, click **Use a custom schedule**.

20.If you are creating a custom schedule for this workflow, click the check boxes for the days of the week that the response group is available.

21.If you are creating a custom schedule, type the **Open** and **Close** hours when the response group available.

> **Note:**
> The **Open** and **Close** hours must be in 24-hour time notation. For example, if your office works a 9-to-5 work day and closes at noon for lunch, the business hours are specified as **Open** 9:00, **Close** 12:00, **Open** 13:00, and **Close** 17:00.

22. If you want to play a message when the office is not open, select the **Play a message when the response group is outside of business hours** check box, and then specify the message to play by doing one of the following:
    - To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

      > **Note:**
      > Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

    - To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

      > **Note:**
      > All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

23. Specify how to handle calls after the message is played (if a message is configured):
    - To disconnect the call, click **Disconnect Call**.
    - To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is *<username>*@*<domainname>* (for example, bob@contoso.com).
    - To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is *<username>*@*<domainname>*.
    - To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is *<number>*@*<domainname>* (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.
24. Under **Step 5 Specify Your Holidays**, click the check boxes for one or more sets of holidays that define the days when the response group is closed for business.

> **Note:**
> You need to define holidays and holiday sets before you configure the workflow. Use the **New-CsRgsHoliday** and **New-CsRgsHolidaySet** cmdlets to define holidays and holiday sets. For details, see (Optional) Define Response Group Holiday Sets.

25. If you want to play a message on holidays, select the **Play a message during holidays** check box, and then specify the message to play by doing one of the following:
    - To enter the message as text that is converted to speech for the caller, click **Use text-to-speech**, and then type the message in the text box.

      > **Note:**
      > Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

    - To use an audio file recording for the message, click **Select a recording**. If you want to upload a new audio file, click the **a recording** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

> **Note:**
> All user-provided audio files must meet certain requirements. For details about supported audio file formats, see Technical Requirements for Response Groups.

26. Specify how to handle calls after the message is played (if a message is configured):
    - To disconnect the call, click **Disconnect Call**.
    - To forward the call to voice mail, click **Forward to voice mail**, and then type the voice mail address. The format for the voice mail address is *<username>*@*<domainname>* (for example, bob@contoso.com).
    - To forward the call to another user, click **Forward to SIP URI**, and then type a user address. The format for the user address is *<username>*@*<domainname>*.
    - To forward the call to another telephone number, click **Forward to telephone number**, and then type the telephone number. The format for the telephone number is *<number>*@*<domainname>* (for example, +14255550121@contoso.com). The domain name is used to route the caller to the correct destination.
27. Under **Step 6 Configure Music on Hold**, choose what you want callers to listen to while waiting for an agent by doing one of the following:
    - To use the default music on-hold recording, click **Use default**.
    - To use an audio file recording for the on-hold music, click **Select a music file**. If you want to upload a new audio file, click the **a music file** link. In the new browser window, click **Browse**, select the file that you want to use, and then click **Open**. Click **Upload** to load the audio file.

> **Note:**
> All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

28. Under **Step 7 Configure Interactive Voice Response**, under the **The user will hear the following text or recorded message** heading, specify the question to ask callers as follows:
    - To enter the question in text format, click **Use text-to-speech**, and type the question in the text box.

> **Note:**
> Do not include HTML tags in the text you enter. If you include HTML tags, you will receive an error message.

> **Note:**
> The "#" symbol is translated by the text-to-speech engine as the word "number". If you need to refer to the # key, you should use the key name, rather than the symbol, in your prompt. For example, "To talk to sales, press the pound key."

- To use a prerecorded audio file that contains the question, click **Select a recording**, and then click the **a recording** link to upload the file. In the new browser window, click **Browse**, select the audio file, and then click **Open**. Click **Upload** to load the file, and then optionally you can type the question in the text box (this enables the question, and the caller’s response, to be forwarded to the responding agent).

> **Note:**
> All user-provided audio files must meet certain requirements. For details about supported file formats, see Technical Requirements for Response Groups.

29. Under **Response 1**, specify the first possible answer to the question by doing the following:

Important:
Do not use quotation marks (") in any voice responses. Quotation marks cause the IVR to fail.

Note:
You can choose to allow callers to answer using speech, alphanumeric keypad input, or both.

- If you want to allow the caller to respond using speech, enter the answer in **Enter a voice response**.
- If you want to allow the caller to respond by pressing a key on the keypad, in **Digit**, click the keypad digit.

30. Specify whether to route the caller to a queue, or to ask another question as follows:
    - To route the caller to a queue, click **Send to a queue**, and in **Select a queue**, click the queue that you want to use.
    - To ask another question, click **Ask another question**, and then click **Use text-to-speech** and type the question, or click **Select a recording**. Use the response groupings in this section to specify up to four possible responses to the additional question and the queue to use for each response. To specify a third or fourth possible response, click the **Response 3** check box or the **Response 4** check box.
31. Specify up to three more possible answers to the original question by repeating steps 28 and 29 to specify the possible responses and the action to take for each response. To specify a third or fourth possible answer, click the **Response 3** check box or the **Response 4** check box.
32. Click **Deploy**.

To use Windows PowerShell to create or modify an Interactive workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Retrieve the service name for the Response Group service and assign it to a variable. At the command line, run:

```
$serviceId="service:"+(Get-CSService | ?{$_.Applications -like "*RGS*"
```

4. An interactive workflow requires two or more queues and two or more agent groups. First, create the agent groups. Run:

```
$AGSupport = New-CsRgsAgentGroup -Parent $serviceId -Name "Technical S
$AGSales = New-CsRgsAgentGroup -Parent $serviceId -Name "Sales Team" [
```

5. Create the queues. Run:

```
$QSupport = New-CsRgsQueue -Parent $ServiceId -Name "Contoso Support"
$QSales = New-CsRgsQueue -Parent $ServiceId -Name "Contoso Sales" -Age
```

6. Create the first response group prompt. Run:

```
$SupportPrompt = New-CsRgsPrompt -TextToSpeechPrompt "Please be patien
```

7. Then create the action to be performed after the prompt. Run:

```
$SupportAction = New-CsRgsCallAction -Prompt $SupportPrompt -Action Tr
```

8. Create the first response group answer. Run:

```
$SupportAnswer = New-CsRgsAnswer -Action $SupportAction [-DtmfResponse
```

9. Now create the second prompt, call action, and answer. First create the prompt. Run:

```
$SalesPrompt = New-CsRgsPrompt -TextToSpeechPrompt "Please hold while
```

10. Create the second call action. Run:

```
$SalesAction = New-CsRgsCallAction -Prompt $SalesPrompt -Action Transf
```

11. Create the second response group answer. Run:

```
$SalesAnswer = New-CsRgsAnswer -Action $SalesAction [-DtmfResponse 2]
```

12. Create the top-level prompt. Run:

```
$TopLevelPrompt = New-CsRgsPrompt -TextToSpeechPrompt "Thank you for c
```

13. Create the top-level question. Run:

```
$TopLevelQuestion = New-CsRgsQuestion -Prompt $TopLevelPrompt [-Answer
```

14. Now create the workflow. Run:

```
$IVRAction = New-CsRgsCallAction -Action TransferToQuestion [-Question
$IVRWorkflow = New-CsRgsWorkflow -Parent $ServiceId -Name "Contoso Hel
```

Note:
All users who have been designated as manager of a response group must be assigned th CsResponseGroupManager role. If users are not assigned this role, they cannot manage response groups.

1.7.8.3.3.5 Delete a Workflow

Delete a Workflow

Managing Call Management Features > Managing Response Groups > Managing Response Group Workflows >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to delete a workflow.

To use Lync Server Control Panel delete a workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Response Groups**, and then click **Workflow**.
4. On the **Workflow** page, click **Create or edit a workflow**.
5. In the **Select a Service** search field, type part or all of the name of the **ApplicationServer** service that hosts the workflow that you want to delete.
6. In the list of services, click the service that you want, and then click **OK**.

Note:
The Response Group Configuration Tool webpage opens. You can also open the Response Group Configuration Tool webpage directly from a web browser by connecting to **https://*<webPoolFqdn>*/RgsConfig**.

7. Under **Manage an Existing Workflow**, locate the workflow you want to delete, and then under **Action**, click **Delete**.
8. Click **Yes**.

To use Windows PowerShell to delete a workflow

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

3. At the command line, run:

```
Get-CsRgsWorkflow -Identity <Application Server service> -Name "<name
```

For example:

```
Get-CsRgsWorkflow -Identity service:ApplicationServer:redmond.contoso.
```

1.7.8.3.4 Managing Application-Level Response Group Settings

Managing Application-Level Response Group Settings

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Response Group >

Topic Last Modified: *2012-11-01*

Application-level settings for Response Group application include the default music-on-hold configuration, the default music-on-hold audio file, the agent ringback grace period, and the call context configuration. You can define only one set of application-level settings per pool. To view application-level settings, use the **Get-CsRgsConfiguration** cmdlet. To modify the application-level settings, use the **Set-CsRgsConfiguration** cmdlet.

The default music on hold is played when a call is placed on hold only if no custom music on hold is defined. Call context is available only for queues assigned to interactive workflows. If call context is enabled, an agent can see information such as caller wait time or workflow questions and answers when the call is received.

⊟To modify Response Group application-level settings

1. Log on as a member of the RTCUniversalServerAdmins group, or as a member of one of the predefined administrative roles that support Response Group.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. At the command line, run:

```
Set-CsRgsConfiguration -Identity <name of service hosting Response Gro
```

For example:

```
Set-CsRgsConfiguration -Identity "service:ApplicationServer:redmond.co
```

To specify an audio file to use as the default music on hold, you need to import the audio file first. For example:

```
$x = Import-CsRgsAudioFile -Identity "service:ApplicationServer:redmon
Set-CsRgsConfiguration -Identity "service:ApplicationServer:redmond.co
```

Other Resources

Get-CsRgsConfiguration
Set-CsRgsConfiguration
Import-CsRgsAudioFile

1.7.8.3.5 Moving Response Groups to a New Pool

Moving Response Groups to a New Pool

Operations > Managing Call Management Features > Managing Response Groups >

Topic Last Modified: *2012-11-01*

Lync Server 2013 introduces new cmdlet support for moving response groups from one pool to another pool, even when the fully qualified domain name (FQDN) is different.

Use the steps in the following procedure to move response groups from one Front End pool to another Front End pool with a different FQDN.

Note:
In a coexistence environment, you can move response groups only between Lync Server 2013 Front End pools.

To move response groups to a pool with a different FQDN

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Export the response groups in the source pool. At the command line, type:

   ```
   Export-CsRgsConfiguration -Source "service:ApplicationServer:<source F
   ```

   For example:

   ```
   Export-CsRgsConfiguration -Source "service:ApplicationServer:source.co
   ```

   To remove the response groups from the source pool during the export, include the –RemoveExportedConfiguration parameter. For example:

   ```
   Export-CsRgsConfiguration -Source ApplicationServer:source.contoso.com
   ```

3. Import the response groups to the destination pool and assign the destination pool as the new owner. At the command line, type:

   ```
   Import-CsRgsConfiguration -Destination "service:ApplicationServer:<des
   ```

   If you also want to copy the Response Group application-level settings from the source pool to the destination pool, include the –ReplaceExistingSettings parameter. You can define only one set of application-level settings per pool. If you copy the application-level settings from the source pool to the destination pool, the settings from the source pool replace the settings for the destination pool. If you do not copy the application-level settings from the source pool, the existing settings from the destination pool apply to the imported response groups.
   For example:

   ```
   Import-CsRgsConfiguration -Destination "service:ApplicationServer:dest
   ```

   Note:
   Application-level settings include the default music-on-hold configuration, the default music-on-hold audio file, the agent ringback grace period, and the call context configuration. To view these configuration settings, run the **Get-CsRgsConfiguration** cmdlet. For details about this cmdlet, see Get-CsRgsConfiguration.

4. Verify that the import was successful by displaying the imported response group configuration by doing the following:
   - Verify that all the workflows were imported. At the command line, type the following:

     ```
     Get-CsRgsWorkflow -Identity "service:ApplicationServer:<dest
     ```

   - Verify that all the queues were imported. At the command line, type the following:

     ```
     Get-CsRgsQueue -Identity "service:ApplicationServer:<destina
     ```

   - Verify that all the agent groups were imported. At the command line, type the following:

     ```
     Get-CsRgsAgentGroup -Identity "service:ApplicationServer:<de
     ```

- Verify that all the hours of business were imported. At the command line, type the following:

```
Get-CsRgsHoursOfBusiness -Identity "service:ApplicationServe
```

- Verify that all the holiday sets were imported. At the command line, type the following:

```
Get-CsRgsHolidaySet -Identity "service:ApplicationServer:<de
```

5. Verify that the import was successful by placing a call to one of the response groups and verifying that the call is handled correctly.
6. Request agents who are members of formal agent groups to sign in to their agent groups in the destination pool.
7. If you did not previously remove response groups from the source pool, remove the response groups from the source pool. At the command line, type:

```
Export-CsRgsConfiguration -Source "service:ApplicationServer:<source p
```

For example:

```
Export-CsRgsConfiguration -Source "service:ApplicationServer:source.co
```

1.7.8.3.6 Managing Response Groups During a Disaster

Managing Response Groups During a Disaster

Planning > Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery >

Topic Last Modified: *2012-11-01*

Lync Server 2013 supports running response groups in the backup pool during disaster recovery. This section describes how to plan for response groups during an outage, how response groups work during the outage, and the steps required to fail over and fail back response groups.

- Planning for Response Group Disaster Recovery
- Response Group Experience During Pool Failure
- Response Group Disaster Recovery Procedures

1.7.8.3.6.1 Planning for Response Group Disaster Recovery

Planning for Response Group Disaster Recovery

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Managing Response Groups During a Disaster >

Topic Last Modified: *2012-11-01*

This section describes some ways to prepare response groups for disaster recovery and provides an overview of the disaster recovery process.

Preparing for Response Group Disaster Recovery

Keep the following in mind when you prepare for and carry out disaster recovery procedures.

Note:

In a coexistence environment, only the Lync Server 2013 response groups are supported for the disaster recovery procedures described in this document.

- Plan for disaster recovery when you do your capacity planning. For disaster recovery capacity, each pool in a paired pool should be able to handle the workloads of all the response groups in both pools. For details about Response Group capacity planning, see Capacity Planning for Response Group.
- Take regular backup copies of all the response group configurations in all the Front End pools where you deployed the Response Group application by using the export procedure described in this document. For details, see Response Group Disaster Recovery Procedures. Keep the backup copies in a safe location.
- Keep a separate backup copy of all the original audio files you used for the Response Group application, including any recordings and music-on-hold files. Keep the backup files in a safe location.
- For Lync Server 2013 disaster recovery, all Response Group settings must have unique names across your deployment. This requirement applies to workflows, queues, agent groups, holiday sets, and hours of business. You should verify that this requirement is met when the primary and backup pools are still active, and before you need to initiate any failover procedure. If you encounter name conflicts while importing response group data to the backup pool, the import fails. To complete the import and failover procedure, you need to resolve the name conflicts by renaming the response group object in the backup pool or by using the **Import-CsRgsConfiguration** cmdlet with the –ResolveNameConflicts parameter to automatically resolve the conflict by appending a unique identifying number to the response group object.
- In general, we recommend that you perform daily backups, but if you have a high volume of changes, you might want to schedule more frequent backups. The amount of information you can lose in the event of a disaster depends on the frequency of your backups, as well as the frequency and volume of changes.
- It is possible to import response groups to a backup pool before a disaster or failover operation occurs. Importing response groups in advance reduces downtime, because the Lync Server Response Group service can be restored in the backup pool as soon as calls are routed to the backup pool.

Note:

The Response Group application cannot reach any agents homed in an inactive pool until failover is complete. During this time, the Response Group application processes calls as if those agents are unavailable.

Response Group Disaster Recovery Process

In the event of a disaster, you can recover response groups by using either of the following recovery approaches:

- Fail over to a backup pool and then fail back to the original pool.
- Fail over to a backup pool, create a new pool with a different fully qualified domain name (FQDN), and then import the response groups to the new pool.

During the failover phase of disaster recovery, the response groups reside in multiple pools: in the primary pool (which is unavailable) and in the backup pool. The response groups in both pools have the same name and the same owner (the primary pool), but they have different parents.

When you recover by creating a new pool with a different FQDN, you need to assign the new pool as the owner of the response groups when you import them. Ownership of response groups remains with the original pool unless or until you explicitly reassign ownership by using the –OverwriteOwner parameter with the **Import-**

CsRgsConfiguration cmdlet.

Note:

You also need to use the –OverwriteOwner parameter if you rebuilt the pool during the recovery (that is, the Response Group database is empty), whether or not you use the same FQDN. You do not need to use the –OverwriteOwner parameter if you did not rebuild the pool, but it is permissible to use this parameter whenever you import response groups back to the primary pool.

You can define only one set of application-level Response Group configuration settings per pool. These settings include the default music-on-hold configuration, the default music-on-hold audio file, the agent ringback grace period, and the call context configuration. To view these configuration settings, run the **Get-CsRgsConfiguration** cmdlet. For details about the **Get-CsRgsConfiguration** cmdlet, see Get-CsRgsConfiguration.

You can transfer these application-level settings from one pool to another by using the **Import-CsRgsConfiguration** cmdlet with the –ReplaceExistingSettings parameter, but doing so overrides the settings in the destination pool.

Important:

This constraint about transferring settings to another pool is true only for the application-level settings and the default music-on-hold audio file. It does not apply to agent groups, queues, workflows, business hours, and holiday sets.

If you don't want to replace the application-level settings in the backup pool during a disaster and the primary pool can't be recovered, the application-level settings from the primary pool will be lost. If you need to create a new pool to replace the primary pool during recovery, either with the same FQDN or with a different FQDN, you can't recover the original application-level settings. In this case, you need to configure the new pool with these settings and include the music-on-hold audio file.

If you decide to use the **Import-CsRgsConfiguration** cmdlet to transfer application-level settings from the primary pool to the backup pool during a disaster, you can then transfer the settings from the backup pool to the new pool during recovery in the same way that you transferred them from the primary pool to the backup pool.

The following table is an overview of the steps involved in recovering response groups.

For details about performing these steps, see Response Group Disaster Recovery Procedures.

Response Group Disaster Recovery Steps

Phase	Steps	Required groups and roles
Before outage	On a routine basis, run the **Export-CsRgsConfiguration** cmdlet to create backups of all Response Group configurations in all Front End pools where Response Group application is deployed.	RTCUniversalServerAdmins CsResponseGroupAdministrator
During outage	Run the **Import-CsRgsConfiguration** cmdlet to import the backed up Lync Server Response Group service configuration from the primary pool to the backup pool. **Note:** Use the –ReplaceExistingSettings	RTCUniversalServerAdmins CsResponseGroupAdministrator

	parameter if you want to replace application-level Response Group settings in the backup pool with the settings from the primary pool. If you do not transfer the application-level settings from the primary pool to the backup pool, and the primary pool can't be recovered, you will lose the settings from the primary pool.	
After importing	Run Response Group cmdlets with either the –ShowAll parameter (to display all response groups) or the –Owner parameter (to display only imported response groups) to verify that all response group configurations were imported to the backup pool. ◆**Important:** If you do not use either the –ShowAll parameter or the –Owner parameter, the response groups that you imported to the backup pool will not be listed in the results returned by the cmdlets. Run the following cmdlets: • **Get-CsRgsWorkflow** • **Get-CsRgsQueue** • **Get-CsRgsAgentGroup** • **Get-CsRgsHoursOfBusiness** • **Get-CsRgsHolidaySet**	RTCUniversalServerAdmins CsResponseGroupAdministrator
After failover	• Place a test call to a response group that was imported to the backup pool and verify that the call is handled correctly. • All formal agents must sign in again to their formal groups on backup pool. • Manage configuration changes: Response groups in the backup pool, whether imported to the backup pool or owned by the backup pool, can be modified as usual during the outage. ◆**Important:** You must use Lync Server Management Shell to manage the response groups that you imported to the backup pool. You cannot use Lync Server Control Panel to manage these response groups while they are in the	N/A

	backup pool.	
After recovery, before failback	Run the **Export-CsRgsConfiguration** cmdlet specifying the -Source parameter as the backup pool and the –Owner parameter as the primary pool to export the response groups owned by the primary pool from the backup pool.	RTCUniversalServerAdmins CsResponseGroupAdministrator
After failback	• Run the **Import-CsRgsConfiguration** cmdlet to import the response groups back to the primary pool. **Note:** If the primary pool can't be recovered and you deploy a new pool to replace it, use the –ReplaceExistingSettings parameter to transfer the application-level settings from the backup pool to the new pool. If you do not transfer the settings from the backup pool, the new pool will use the default settings. • Run the following cmdlets with either the –ShowAll parameter (to display all response groups) or the –Owner parameter (to display only imported response groups) to verify that all response group configurations were successfully imported back to the primary pool: • **Get-CsRgsWorkflow** • **Get-CsRgsQueue** • **Get-CsRgsAgentGroup** • **Get-CsRgsHoursOfBusiness** • **Get-CsRgsHolidaySet** • Place a test call to a response group that was imported back to the primary pool and verify that the call is handled correctly. • Optionally, run the **Export-CsRgsConfiguration** cmdlet on the backup pool with the –	RTCUniversalServerAdmins CsResponseGroupAdministrator

		RemoveExportedConfiguration parameter to remove the response groups owned by the primary pool from the backup pool.	

1.7.8.3.6.2 Response Group Experience During Pool Failure

Response Group Experience During Pool Failure

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Managing Response Groups During a Disaster >

Topic Last Modified: *2012-10-30*

This section describes in detail how response group activity is affected in the following stages:

- An outage occurs in the primary pool, but failover is not yet initiated.
- Service is failed over to the backup pool.
- Service is failed back to the primary pool.

User Experience When Outage Occurs

When a pool or site outage occurs, but the administrator has not yet initiated failover, response group activity is handled as described in the following table.

Note:
During disaster recovery, calls behave differently depending on whether the primary pool response groups were imported to the backup pool during recovery. In the following table, references to imported response groups mean that primary pool response groups were imported to the backup pool during disaster recovery mode.

Outage Occurs

Type of call or user action	**During outage**
Calls connected to an agent	• Regular calls remain connected. • Anonymous calls are disconnected.
In progress calls not yet connected to an agent	Calls are disconnected.
New calls	• Calls are disconnected. • If response groups were imported, calls connect to backup pool, but agents homed in primary pool are unreachable.
Agent calls on behalf of response group	Feature is disabled during this stage.
Agent sign-in and agent information	• Agent groups owned by the primary pool can be viewed on agent console but agents cannot sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are not displayed on agent console.
Response group configuration	• Response groups owned by the primary pool can be viewed, depending on the availability of the primary pool's back-

	end database, but cannot be modified. • Response groups owned by the backup pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.

User Experience During Failover

When an administrator invokes failover to a backup pool, response group activity is handled during and after the failover as described in the following table. The first column describes the type of activity that might be taking place. The middle column describes how each activity is handled during the brief time that it takes to fail over to the backup pool. The last column describes how the activity is handled for the duration, after the failover process is complete and the backup pool is standing in for the primary pool.

Note:

During disaster recovery, calls behave differently depending on whether the primary pool response groups were imported to the backup pool during recovery. In the following table, references to imported response groups mean that primary pool response groups were imported to the backup pool during disaster recovery mode.

Failover Is Initiated

Type of call or user action	During Failover	After Failover Completes
Calls connected to an agent	• Regular calls remain connected. • Anonymous calls are disconnected.	• Regular calls remain connected. • For imported response groups, anonymous calls that have reached the backup pool remain connected.
In progress calls not yet connected to an agent	Calls are disconnected.	• If response groups were not imported, no calls are in this status. • For imported response groups, calls that have reached the backup pool remain connected.
New calls	• Calls are disconnected. • For imported response groups, calls connect to the backup pool, but agents homed in the primary pool are unreachable.	• If response groups were not imported, calls are disconnected. • For imported response groups, calls connect to the backup pool.
Agent calls on behalf of response group	Feature is disabled during this stage	• If response groups were not imported, calls fail. • For imported response groups, calls succeed.
Agent sign-in and	• Agent groups owned by the primary pool	• Agent groups owned by the primary pool

agent information	can be viewed on agent console but agents cannot sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are displayed on agent console and agents can sign in.	can be viewed on agent console but agents cannot sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are displayed on agent console and agents can sign in.
Response group configuration	• Response groups owned by the primary pool can be viewed, depending on the availability of the primary pool's back-end database, but cannot be modified. • Response groups owned by the backup pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.	• Response groups owned by the primary pool can be viewed, depending on the availability of the back end database, but cannot be modified. • Response groups owned by the backup pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.

User Experience During Failback

When an administrator invokes failback to the primary pool, response group activity is handled during and after the failback as described in the following table.

Note:

During disaster recovery, calls behave differently depending on whether the primary pool response groups were imported to the backup pool during recovery. In the following table, references to imported response groups mean that primary pool response groups were imported to the backup pool during disaster recovery mode.

Call Handling in Failback

Type of call or user action	During Failback	After Failback Completes
Calls connected to an agent	• Regular calls remain connected. • If response groups were not imported, no anonymous calls are in this status. • For imported response groups, anonymous	• Regular calls remain connected. • If response groups were not imported, no anonymous calls are in this status. • For imported response groups, anonymous

	calls remain connected.	calls remain connected.
In progress calls not yet connected to an agent	• If response groups were not imported, no calls are in this status. • For imported response groups, calls will be disconnected.	• If response groups were not imported, no calls are in this status. • For imported response groups, calls will be disconnected.
New calls	Calls connect to the primary pool, but agents homed in the primary pool are unreachable.	Calls connect to the primary pool.
Agent calls on behalf of response group	Feature is disabled during this stage.	Calls succeed.
Agent sign-in and agent information	• Agent groups owned by the primary pool can be viewed on agent console but agents cannot sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are displayed on agent console and agents can sign in.	• Agent groups owned by the primary pool can be viewed on agent console and agents can sign in. • Agent groups owned by the backup pool can be viewed on agent console and agents can sign in. • Imported agent groups are not displayed on agent console.
Response group configuration	• Response groups owned by the primary pool can be viewed, depending on the availability of the primary pool's back-end database, but cannot be modified. • Response groups owned by the backup pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.	• Response groups owned by the primary pool can be viewed and modified. • Response groups owned by the backup pool can be viewed and modified. • Imported response groups cannot be viewed with Lync Server Control Panel or the Response Group Configuration Tool, but can be configured by using Lync Server Management Shell cmdlets.

1.7.8.3.6.3 Response Group Disaster Recovery Procedures

Response Group Disaster Recovery Procedures

Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery > Managing Response Groups During a Disaster >

Topic Last Modified: *2012-11-01*

During the failover phase of disaster recovery, the response groups reside in multiple pools: in the primary pool (which is unavailable) and in the backup pool. The response groups in both pools have the same name and the same owner (the primary pool), but they have different parents. During this time, Response Group cmdlets work a little differently. Be sure to use parameters as specified in the following procedure. For details about how cmdlets work during the failover phase, see NextHop blog article "Lync Server 2013: Recovering Response Groups During Disaster Recovery" at http://go.microsoft.com/fwlink/p/?LinkId=263957. This blog article also applies to the released version of Lync Server 2013.

Use the steps in the following procedure to prepare for and perform disaster recovery for Lync Server Response Group service.

⊟To fail over and fail back Response Group

1. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
2. Routinely perform backups. At the command line, type:

   ```
   Export-CsRgsConfiguration -Source "service:ApplicationServer:<primary
   ```

   For example:

   ```
   Export-CsRgsConfiguration -Source "service:ApplicationServer:primary.c
   ```

3. During an outage, after failover to the backup pool, import the response groups to the backup pool. At the command line, type:

   ```
   Import-CsRgsConfiguration -Destination "service:ApplicationServer:<bac
   ```

   If you want to replace the application-level settings in the backup pool with the settings from the primary pool, include the –ReplaceExistingSettings parameter. For example:

   ```
   Import-CsRgsConfiguration -Destination "service:ApplicationServer:back
   ```

   Caution:

   If you do not replace the settings in the backup pool and the primary pool can't be recovered, the primary pool settings will be lost. For details, see Planning for Response Group Disaster Recovery.

4. Verify that the import was successful by displaying the imported response groups. The imported response groups are still owned by the primary pool. Do the following:
   - Display all the workflows in the backup pool that are owned by the primary pool, and verify that all the primary pool workflows are included. At the command line, type:

     ```
     Get-CsRgsWorkflow -Identity "service:ApplicationServer:<bac
     ```

     For example:

     ```
     Get-CsRgsWorkflow -Identity "service:ApplicationServer:backu
     ```

   - Display all the queues in the backup pool that are owned by the primary pool, and verify that all the primary pool queues are included. At the command line, type:

```
Get-CsRgsQueue -Identity "service:ApplicationServer:<backup
```

For example:

```
Get-CsRgsQueue -Identity "service:ApplicationServer:backup.c
```

- Display all the agent groups in the backup pool that are owned by the primary pool, and verify that all the primary pool agent groups are included. At the command line, type:

```
Get-CsRgsAgentGroup -Identity "service:ApplicationServer:<ba
```

For example:

```
Get-CsRgsAgentGroup -Identity "service:ApplicationServer:bac
```

- Display all the hours of business in the backup pool that are owned by the primary pool, and verify that all the primary pool hours of business are included. At the command line, type:

```
Get-CsRgsHoursOfBusiness -Identity "service:ApplicationServe
```

For example:

```
Get-CsRgsHoursOfBusiness -Identity "service:ApplicationServe
```

- Display all the holiday sets in the backup pool that are owned by the primary pool, and verify that all the primary pool holiday sets are included. At the command line, type:

```
Get-CsRgsHolidaySet -Identity "service:ApplicationServer:<ba
```

For example:

```
Get-CsRgsHolidaySet -Identity "service:ApplicationServer:bac
```

Alternatively, you can display all the response groups in the backup pool, including the ones owned by the primary pool and the ones owned by the backup pool by using the –ShowAll parameter instead of the –Owner parameter. For example:

```
Get-CsRgsWorkflow -Identity "service:ApplicationServer:<backup pool FQ
```

Important:

You must use either the –ShowAll parameter or the –Owner parameter. If you do not use either of these parameters, the response groups that you imported to the backup pool will not be listed in the results returned by the cmdlets.

5. Verify that the import was successful by placing a call to an imported response group and verifying that the call is handled correctly.
6. Request agents who are members of formal agent groups to sign in to their agent groups in the backup pool.
7. Manage and modify the imported response groups as usual.

Important:

While the response groups are in the backup pool, you need to use Lync Server Management Shell to manage them. You cannot use Lync Server Control Panel to manage the response groups that you imported to the backup pool.

8. After the primary pool is restored and failback is complete, export the primary pool response groups that were imported to the backup pool. At the command line, type:

```
Export-CsRgsConfiguration -Source ApplicationServer:<backup pool FQDN>
```

9. Import the response groups back to the primary pool. At the command line, type:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:<pri
```

For example:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:prim
```

Note:
If you rebuild a pool during recovery, whether with the same or a different fully qualified domain name (FQDN), you need to use the –OverwriteOwner parameter. As a rule of thumb, you can always use the –OverwriteOwner parameter when you import response groups back to the primary pool.

If you deployed a new pool (with the same or a different FQDN) to replace the primary pool, and you want to use the application-level settings from the backup pool for the new pool, include the –ReplaceExistingSettings parameter. At the command line, type:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:<new
```

For example:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:newp
```

Important:
If you don't want to replace the application-level settings and default music-on-hold audio file for the new pool with the settings from the backup pool, the new pool will use the default application-level settings.

10. Verify that the import back to the primary pool was successful by displaying the imported response group configuration. Do the following:
    - Display all the workflows in the primary pool, and verify that all the imported workflows are included. At the command line, type:

      ```
      Get-CsRgsWorkflow -Identity "service:ApplicationServer:<prim
      ```

      For example:

      ```
      Get-CsRgsWorkflow -Identity "service:ApplicationServer: prim
      ```

    - Display all the queues in the primary pool, and verify that all the imported queues are included. At the command line, type:

      ```
      Get-CsRgsQueue -Identity "service:ApplicationServer:<primary
      ```

      For example:

      ```
      Get-CsRgsQueue -Identity "service:ApplicationServer:primary.
      ```

    - Display all the agent groups in the primary pool, and verify that all the imported agent groups are included. At the command line, type:

      ```
      Get-CsRgsAgentGroup -Identity "service:ApplicationServer: <p
      ```

      For example:

      ```
      Get-CsRgsAgentGroup -Identity "service:ApplicationServer:pri
      ```

    - Display all the hours of business in the primary pool, and verify that all the imported hours of business are included. At the command line, type:

      ```
      Get-CsRgsHoursOfBusiness -Identity "service:ApplicationServe
      ```

      For example:

      ```
      Get-CsRgsHoursOfBusiness -Identity "service:ApplicationServe
      ```

    - Display all the holiday sets in the primary pool, and verify that all the imported holiday sets are included. At the command line, type:

      ```
      Get-CsRgsHolidaySet -Identity "service:ApplicationServer:<p
      ```

      For example:

      ```
      Get-CsRgsHolidaySet -Identity "service:ApplicationServer:pri
      ```

11. Verify that the import was successful by placing a call to an imported response group and verifying that the call is handled correctly.
12. Optionally, remove the response groups owned by the primary pool from the backup pool. At the command line, type:

```
Export-CsRgsConfiguration -Source "service:ApplicationServer:<backup p
```

For example:

```
Export-CsRgsConfiguration -Source "service:ApplicationServer:backup.co
```

Note:
This step creates a new file with the exported configuration, and then removes it from the backup pool.

1.7.8.4 Managing Calls to Unassigned Numbers

Managing Calls to Unassigned Numbers

Microsoft Lync Server 2013 > Operations > Managing Call Management Features >

Topic Last Modified: *2012-11-01*

Lync Server lets you configure the handling of incoming phone calls when the dialed number is valid for your organization, but is not assigned to a user or phone. You can use the Announcement application to transfer these calls to a predetermined destination (phone number, SIP URI, or voice mail), or play an audio announcement, or both. You can also transfer these calls to an Exchange UM Auto Attendant phone number. Handling calls to unassigned numbers in one of these ways helps you avoid the situations in which a caller misdials and then hears a busy tone, or the SIP client receives an error message.

This section describes how to manage unassigned number ranges to handle calls to unassigned phone numbers. The section also describes how to manage Announcements during disaster recovery if you want this functionality during an outage.

Note:
Using unassigned number handling during an outage is optional.

- Create an Announcement
- Configure Unassigned Phone Numbers
- Manage Announcements During Disaster Recovery

1.7.8.4.1 Configure Announcements

Configure Announcements

Operations > Managing Call Management Features > Managing Calls to Unassigned Numbers >

Topic Last Modified: *2012-09-12*

When you configure announcements, you are really configuring how you want calls to unassigned numbers to be handled. You can play a prompt, which can be an audio file or a text-to-speech (TTS) file, or you can just transfer the call to a specified destination without playing a prompt.

You need to create announcements before you define the unassigned number table. You need to perform this step for all announcements that use an audio prompt, a TTS prompt, or no prompt.

- Create an Announcement
- Delete an Announcement

1.7.8.4.1.1 Create an Announcement

Create an Announcement

See Also

Deploying Enterprise Voice > Deploying Call Management Features > Configuring Announcements for Unassigned Numbers >

Topic Last Modified: *2012-11-01*

To create a new announcement, you need to perform the following steps:

1. For audio prompts, record the audio file by using your favorite audio recording application.
2. For audio prompts, run the **Import-CsAnnouncementFile** cmdlet to import the contents of the audio file to File Store.
3. Run the **New-CsAnnouncement** cmdlet to create and name the announcement. Perform this step to create announcements with an audio prompt, a text-to-speech (TTS) prompt, or no prompt.

   > **Tip:**
   > You might want to create an announcement with no prompt (for example, if you want to transfer calls to a specific destination without playing a message).

4. Assign the new announcement to a number range in the unassigned number table.

This topic describes how to import and create announcements. For details about assigning announcements in the unassigned number table, see Configure the Unassigned Number Table.

To create a new announcement

1. For audio prompts, create the audio file.
2. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
3. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
4. For audio prompts, run:

   ```
   Import-CsAnnouncementFile -Parent <service of the Application Server r
   ```

5. Run:

   ```
   New-CsAnnouncement -Parent <service of Application Server running the
   ```

   For transferring calls to voice mail, type SIPAddress in the format sip:username@domainname;opaque=app:voicemail (for example, sip:bob@contoso.com;opaque=app:voicemail). For transferring calls to a phone number, type SIPAddress in the format sip:number@domainname;user=phone (for example, sip:+14255550121@contoso.com;user=phone).

   For example, to specify an audio prompt:

   ```
   $a = Get-Content ".\PromptFile.wav" -ReadCount 0 -Encoding Byte
   Import-CsAnnouncementFile -Parent service:ApplicationServer:pool0@cont
   New-CsAnnouncement -Parent service:ApplicationServer:pool0.contoso.com
   ```

   For example, to specify a TTS prompt:

   ```
   New-CsAnnouncement -Parent service:ApplicationServer:pool0.contoso.com
   ```

   For more detail about these cmdlets, and to see a list of the language codes to use in the **TextToSpeechPrompt** parameter, see New-CsAnnouncement.

Other Resources

Import-CsAnnouncementFile
New-CsAnnouncement
Configure the Unassigned Number Table

1.7.8.4.1.2 Delete an Announcement

Delete an Announcement

See Also

Managing Call Management Features > Managing Calls to Unassigned Numbers > Configure Announcements >

Topic Last Modified: *2012-11-01*

Use the following procedure to delete an announcement that is used for calls to unassigned numbers.

To delete an announcement

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. List all the announcements in your organization. At the command line, run:

   ```
   Get-CsAnnouncement
   ```

4. In the resulting list, locate the announcement you want to delete, and copy the GUID. Then, at the command line, run:

   ```
   Remove-CsAnnouncement -Identity "<Service:service ID/guid>"
   ```

   For example:

   ```
   Remove-CsAnnouncement -Identity "ApplicationServer:Redmond.contoso.com
   ```

   Note:
   For details about more options, see Get-CsAnnouncement and Remove-CsAnnouncement.

Tasks

Create an Announcement

Other Resources

Remove-CsAnnouncement
Get-CsAnnouncement

1.7.8.4.2 Configure Unassigned Phone Numbers

Configure Unassigned Phone Numbers

Operations > Managing Call Management Features > Managing Calls to Unassigned Numbers >

Topic Last Modified: *2012-11-01*

Lync Server lets you configure what happens to incoming calls to phone numbers that are valid for your organization, but are not assigned to a user or a phone. To configure the handling of such calls, you set up an unassigned number table. You can use the table to route the calls to an Announcement application or to an Exchange UM server.

How you configure the unassigned number table depends on how you want to use it. You can configure the table with all the valid extensions for your organization, with only unassigned extensions, or with a combination of both types of numbers. The unassigned number table can include both assigned and unassigned numbers, but it is invoked only when a caller dials a number that is not currently assigned. If you include all the valid extensions in the unassigned number table, you can specify the action that occurs whenever someone leaves your organization, without needing to reconfigure the table. If you include unassigned extensions in the table, you can tailor the action that occurs for specific numbers. For example, if you change the extension for your customer service desk, you can include the old customer service number in the table and assign it to an announcement that provides the new number.

Important:

Before you configure the unassigned number table, you must already have either one or more announcements defined or an Exchange UM Auto Attendant set up. For details about creating announcements, see Create an Announcement. To see if you have configured Exchange UM settings, run the **Get-CsExUmContact** cmdlet. For details, see Get-CsExUmContact.

- Create or Modify an Unassigned Number Range
- Delete an Unassigned Number Range

1.7.8.4.2.1 Create or Modify an Unassigned Number Range

Create or Modify an Unassigned Number Range

See Also

Deploying Call Management Features > Configuring Announcements for Unassigned Numbers > Configure the Unassigned Number Table >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to configure unassigned number ranges for the Announcement application.

Important:

Before you configure the unassigned number table, you must have already defined one or more announcements or set up an Exchange Unified Messaging (UM) Auto Attendant.

To use Lync Server Control Panel to configure unassigned phone numbers

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Features**, and then click **Unassigned Number**.
4. On the **Unassigned Number** page, do one of the following:
   - To create a new number range, click **New**. In **Name**, type an identifying name for this range of numbers.

     Note:

     After you commit the new unassigned number range to the database, you cannot change this name.
   - To modify an existing number range, type all or part of the name of the number range in the search field. In the resulting list of number ranges, click the name you want, click **Edit**, and then click **Show details**.

5. In the first **Number range** field, type the beginning number of the range, and in the second **Number range** field, type the ending number of the range.

Note:

- The beginning number of the range must be less than or equal to the ending number of the range.
- If the beginning number of the range or the ending number of the range includes an extension number, both the beginning number and the ending number of the range must include an extension, and the extension number must be the same for both the beginning number and the ending number.
- The number must match the regular expression (tel:)?(\+)?[1-9]\d{0,17}(;ext=[1-9]\d{0,9})?. This means the number may begin with the string tel: (if you don't specify that string, it will be automatically added for you), a plus sign (+), and a digit 1 through 9. The phone number can be up to 17 digits and may be followed by an extension in the format ;ext= followed by the extension number.

1. In **Announcement service**, do one of the following:
   - Click **Announcement**.
   - Click **Exchange UM**.
2. If, in the previous step, you clicked **Announcement**, do the following:
   - Under **FQDN of destination server**, click **Select**, click the service ID of the Application service that runs the Announcement application that will handle incoming calls to this range of unassigned numbers, and then click **OK**.
   - In **Announcement**, click the announcement to be played for this range of unassigned numbers.
3. If, in the previous step, you clicked **Exchange UM**, under **Auto Attendant phone number**, click **Select**, click the phone number to be used for this range of unassigned numbers, and then click **OK**.
4. Click **OK**.
5. On the **Unassigned Number** page, be sure that the unassigned number ranges are arranged in the order that you want. To change a range's position in the table, click one or more consecutive names in the list of ranges, and then click the up arrow or the down arrow.

Tip:

Lync Server searches the unassigned number table from top to bottom and uses the first range that matches the unassigned number. If you have overlapping ranges and one range specifies a last resort action, make sure that range is at the bottom of the list.

6. When you have the unassigned number ranges in the order that you want, click **Commit all**.

To use Windows PowerShell to configure unassigned phone numbers

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Use **New-CsUnassignedNumber** to create a new unassigned number range. Use **Set-CsUnassignedNumber** to modify an existing unassigned number range.

Tip:

If you have overlapping ranges and want the ranges to be applied in a specific order, include the Priority parameter. The range with the highest priority will be applied to the call.

At the command line, do one of the following:

- To create a number range for an Announcement service, run:

```
New-CsUnassignedNumber -Identity <unique identifier for unas
```

- Or, to create a number range for Exchange UM Auto Attendant, run:

```
New-CsUnassignedNumber -ExUmAutoAttendantPhoneNumber <phone
```

For example:

```
New-CsUnassignedNumber -Identity "Unassigned range 1" -NumberRangeStar
```

Or

```
New-CsUnassignedNumber -ExUmAutoAttendantPhoneNumber "+12065551234" -I
```

The following example shows how to modify the numbers in an existing unassigned number range:

```
Set-CsUnassignedNumber -Identity "Unassigned range 1" -NumberRangeStar
```

Tasks

Delete an Unassigned Number Range

Other Resources

New-CsUnassignedNumber
Set-CsUnassignedNumber
Get-CsUnassignedNumber

1.7.8.4.2.2 Delete an Unassigned Number Range

Delete an Unassigned Number Range

See Also

Managing Call Management Features > Managing Calls to Unassigned Numbers > Configure Unassigned Phone Numbers >

Topic Last Modified: *2012-11-01*

Use one of the following procedures to delete an unassigned number range for Announcements.

⊟To use Lync Server Control Panel to delete an unassigned number range

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Voice Features** and then click **Unassigned Number**.
4. On the **Unassigned Number** page, in the search field, type all or part of the name of the unassigned number range you want to delete.
5. In the resulting list of number ranges, click the name, click **Edit**, and then click **Delete**.
6. Click **Commit all**.

⊟To use Windows PowerShell to delete an unassigned number range

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click

Microsoft Lync Server 2013, and then click **Lync Server Management Shell**.

3. At the command line, type:

```
Remove-CsUnassignedNumber -Identity "<name of unassigned number range>
```

For example:

```
Remove-CsUnassignedNumber -Identity "Unassigned range 1"
```

> **Note:**
> For details about more options, see Remove-CsCallParkOrbit.

Tasks

Create or Modify an Unassigned Number Range

Other Resources

Remove-CsUnassignedNumber
Get-CsUnassignedNumber

1.7.8.4.3 Manage Announcements During Disaster Recovery

Manage Announcements During Disaster Recovery

Planning > Planning for High Availability and Disaster Recovery > Call Management Features for High Availability and Disaster Recovery >

Topic Last Modified: *2013-02-23*

Lync Server 2013 supports announcements for calls to unassigned numbers during outages. Restoring announcement functionality during an outage is optional. If you choose to restore announcements during an outage, you need recreate your announcement configuration in the backup pool. This section describes what you need to do if you choose to restore announcements during disaster recovery.

This section applies to unassigned number ranges that use the Announcement application. This section does not apply to unassigned number ranges that use Exchange Unified Messaging (UM) Auto Attendant.

Before an Outage

Regardless of whether you choose to use announcements during outages, you should take separate backups of any customized audio files that you configured for the Announcement application. Customized announcements are not backed up as part of the Lync Server disaster recovery process. If you do not take separate backups of the files and the files that you uploaded to the server or pool are damaged, corrupted, or erased, the files will be lost.

If you do not have backup copies of customized audio files, and the original audio files are no longer available, you can find the audio files that you configured for an Announcement application by looking in the File Store for the server or pool where you originally imported the files. You can copy all the audio files that you configured for the Announcement application from the File Store.

To copy audio files from the file store

1. At the command line, run:

```
Xcopy <Source: Pool Announcement Service File Store path> <Destination
```

For example:

```
Xcopy "<Pool File Store Path>\X-ApplicationServer-X\AppServerFiles\RGS
```

Where X-ApplicationServer-X refers to the service ID of the Application Server of the pool (for example, 1-ApplicationServer-1")

During an Outage

To use the Announcement application during an outage, you need to recreate the announcement configuration in the backup pool by performing the tasks described in this section.

> **Note:**
> We recommend that you perform these tasks after you fail over to the backup pool, because as soon as you perform step 2, the backup pool takes ownership of the unassigned number ranges.

> **Note:**
> These steps are not required for number ranges that use an Exchange UM Auto Attendant phone number.

To recreate the announcement configuration in the backup pool

1. Recreate the announcements that you deployed in the primary pool in the backup pool by doing the following:
   1.a. Import any audio files used in the primary pool to the backup pool by using the **Import-CsAnnouncementFile** cmdlet and specifying the backup pool for the Parent parameter.
   1.b. Recreate each announcement by using the **New-CsAnnouncement** cmdlet and specifying the backup pool for the Parent parameter.

   > **Note:**
   > For details about using these parameters to create announcements in the backup pool, see Create an Announcement.

2. After all announcements are recreated in the backup pool, redirect all the unassigned number ranges that use announcements in the primary pool to the recreated announcements in the backup pool.

   For each unassigned number range that uses an announcement in the primary pool, run the following:

   ```
   Set-CsUnassignedNumber -Identity "<name of number range>" -Announcemen
   ```

After the Outage

When the primary pool becomes available, you need to redirect the unassigned number ranges that you changed for the outage back to the primary pool.

> **Note:**
> These steps are not required for number ranges that use an Exchange UM Auto Attendant phone number.

To restore announcements in the primary pool

1. If you had to rebuild the primary pool during the recovery, you need to recreate the announcements in the primary pool by importing the audio files and creating announcements, just as you did in the backup pool, except that you specify the primary pool for the Parent parameter. For details, see "During an Outage" earlier in this topic.
2. For each unassigned number range that you changed for the outage, run the following:

   ```
   Set-CsUnassignedNumber [-Identity "<name of number range>"] -Announcem
   ```

3. Optionally, remove the announcements that you recreated in the backup pool. Get a list of announcements for the backup pool Announcement application. At the command line, run:

   ```
   Get-CsAnnouncement -Identity "<Service:service ID>"
   ```

For example:

```
Get-CsAnnouncement -Identity "ApplicationServer:redmond.contoso.com
```

In the resulting list, locate the announcements you want to remove and copy the GUIDs. For each announcement you want to remove, run:

```
Remove-CsAnnouncement -Identity "<Service:service ID/guid>"
```

For example:

```
Remove-CsAnnouncement -Identity "ApplicationServer:redmond.contoso.com
```

1.7.9 Managing Meetings and Conferences

Managing Meetings and Conferences

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-11-01*

Topics in this section provide step-by-step procedures for tasks you can perform using the pages in the **Conferencing** group in Lync Server Control Panel.

- Meeting Configuration Settings
- Conferencing Policies
- Dial-In Conferencing (Configuration/Access Numbers)

1.7.9.1 Meeting Configuration Settings

Meeting Configuration Settings

Microsoft Lync Server 2013 > Operations > Managing Meetings and Conferences >

Topic Last Modified: *2012-11-01*

In Lync Server 2013, conferencing policy defines the user scheduling and participation experience, and meeting join settings located on the meeting configuration page define the following:

- Whether users dialing in from the public switched telephone network (PSTN) go to the lobby
- Who can be a presenter
- Whether conference type is assigned by default
- Whether anonymous (unauthenticated) users are admitted by default

The topics in this section describe how to configure meeting join settings.

- View Meeting Configuration Settings
- Create or Modify a Collection of Meeting Configuration Settings
- Delete an Existing Collection of Meeting Configuration Settings

1.7.9.1.1 View Meeting Configuration Settings

View Meeting Configuration Settings

Operations > Managing Meetings and Conferences > Meeting Configuration Settings >

Topic Last Modified: *2013-02-23*

In Lync Server 2013 Control Panel, you use meeting configuration setting to control how meetings are implemented in your deployment. This includes the following meeting configurations:

- A global configuration that is created by default when you deploy Lync Server 2013.
- Optional site-level and user-level configurations that you can create and use to specify how meetings are implemented for specific sites or users.

To view meeting configuration settings

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Meeting Configuration**.
4. On the **Meeting Configuration** page, click the meeting configuration that you would like to view.
5. In **Edit File Filter**, select the **Show Details...** check box.

   Edit Meeting Configuration - <policy> opens displaying the settings for the selected policy. For details about configuring the settings, see Create or Modify a Collection of Meeting Configuration Settings.

Viewing Meeting Configuration Information by Using Windows PowerShell Cmdlets

Meeting configuration settings can be viewed by using Windows PowerShell and the Get-CsMeetingConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view meeting configuration information

- To view information about all your meeting configuration settings, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsMeetingConfiguration
  ```

  That will return information similar to this:

  ```
  Identity                         : Global
  PstnCallersBypassLobby           : True
  EnableAssignedConferenceType     : True
  DesignateAsPresenter             : Company
  AssignedConferenceTypeByDefault  : True
  AdmitAnonymousUsersByDefault     : True
  RequireRoomSystemsAuthorization  : False
  LogoURL                          :
  LegalURL                         :
  HelpURL                          :
  CustomFooterText                 :
  AllowConferenceRecording         : True
  ```

For more information, see the help topic for the Get-CsMeetingConfiguration cmdlet.

1.7.9.1.2 Create or Modify a Collection of Meeting Configuration Settings

Create or Modify a Collection of Meeting Configuration Settings

Operations > Managing Meetings and Conferences > Meeting Configuration Settings >

Topic Last Modified: *2013-02-23*

You can use the settings on the Meeting Configuration page to define various characteristics of the meeting join experience. By default, the global settings define the join experience. You can also create site-level and pool-level meeting join settings. If you create pool-level settings, those settings apply to all meetings hosted by that pool. If you do not create pool-level settings, site-level settings apply, if they exist. If you do not define site-level settings, the global settings apply to all meetings.

⊟To create new meeting join settings

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Meeting Configuration**.
4. On the **Meeting Configuration** page, click **New**, and then do one of the following:
   - To create a site-level policy, click **Site configuration**. In the **Select a Site** search field, type all or part of the name of the site for which you want to define meeting join settings. In the resulting list of sites, click the site you want, and then click **OK**.
   - To create a pool-level policy, click **Pool configuration**. In the **Select a Service** search field, type all or part of the name of the pool service for which you want to define meeting join settings. In the resulting list of services, click the pool you want, and then click **OK**.
5. To route participants who dial in from the public switched telephone network (PSTN) through the lobby, clear the **PSTN callers bypass lobby** check box. By default, participants dialing in from the PSTN go directly to the meeting.
6. To configure who can be a presenter in the meeting, in **Designate as presenter**, do one of the following:
   - To not allow anyone other than the organizer to be a presenter, click **None**.
   - To allow only participants who are members of your organization to be a presenter, click **Company**. This is the default setting.
   - To allow any participants to be a presenter, click **Everyone**.
7. To have the organizer select a conference type when scheduling a meeting, clear the **Assigned conference type by default** check box. By default, the conference type is automatically assigned.
8. To prevent anonymous (unauthenticated) users from being automatically admitted, clear the **Admit anonymous users by default** check box. By default, anonymous users are automatically admitted to meetings.
9. To customize the meeting invite that is sent out to participants, do the following. Note that the maximum length for URLs and custom footer text is 1KB. Except for **Help URL**, if you do not specify a value for the customizations, they will not be included in the meeting. If you do not include a custom help URL, the default help URL for Lync will be displayed in the invite.
   - To customize the logo that appears in the meeting invite, in **Logo URL**, enter the location of the logo.

Note:

> The logo must be a GIF or JPG image with a size of 188 by 30 pixels.

- To customize the help text that appears in the meeting invite, in **Help URL**, enter the location of the help text.
- To customize the legal text that appears in the meeting invite, in **Legal text URL**, enter the location of the legal text.
- To customize the footer text that appears in the meeting invite, in **Custom footer text**, enter text.

10. Click **Commit**.

To modify an existing collection of meeting configurations

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Meeting Configuration**.
4. In the list of meeting configurations, click the configuration that you want to change, click **Edit**, and then click **Show details**.
5. In **Edit Meeting Configuration**, modify any of the configuration settings, except for the configuration name, which cannot be modified.
6. Click **Commit**.

Creating New Meeting Configuration Settings by Using Windows PowerShell Cmdlets

Meeting configuration settings can be created (at the site scope only) by using Windows PowerShell and the New-CsMeetingConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To create meeting configuration settings that use the default values

- This command creates a new set of meeting configuration settings for the Redmond site:

  ```
  New-CsMeetingConfiguration -Identity "site:Redmond"
  ```

  Because no parameters (other than the mandatory Identity parameter) were specified in the preceding command, the new meeting configuration settings will use the default values for all its properties.

To change a property value when creating meeting configuration settings

- To create settings that use different property values, simply include the appropriate parameter and parameter value. For example, to create a collection of meeting configuration settings that, by default, admit everyone to a meeting as a presenter use a command like this:

  ```
  New-CsMeetingConfiguration -Identity "site:Redmond" -DesignateAsPresent
  ```

To change multiple property values when creating meeting configuration settings

- Multiple property values can be modified by including multiple parameters. For example, this command admits everyone to a meeting as a presenter and also forces PSTN users to wait in the lobby until they are formally admitted to the meeting:

  ```
  New-CsMeetingConfiguration -Identity "site:Redmond" -DesignateAsPresent
  ```

For more information, see the help topic for the New-CsMeetingConfiguration cmdlet.

1.7.9.1.3 Delete an Existing Collection of Meeting Configuration Settings

Delete an Existing Collection of Meeting Configuration Settings

Operations > Managing Meetings and Conferences > Meeting Configuration Settings >

Topic Last Modified: *2013-02-23*

You can delete a site or user configuration. The global configuration cannot be removed. If you delete the global configuration, it is automatically reset to the default values.

⊟To delete a site or user meeting configuration

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Meeting Configuration**.
4. In the list of meeting configurations, click the site or pool configuration that you want to delete, click **Edit**, and then click **Delete**.

Removing Meeting Configuration Settings by Using Windows PowerShell Cmdlets

Meeting settings can be deleted by using Windows PowerShell and the Remove-CsMeetingConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To remove a specified collection of meeting configuration settings

- This command removes the meeting configuration settings applied to the Redmond site:

  ```
  Remove-CsMeetingConfiguration -Identity "site:Redmond"
  ```

⊟To remove all the meeting configuration settings applied to the site scope

- This command removes all the meeting configuration settings applied to the site scope:

  ```
  Get-CsMeetingConfiguration -Filter "site:*" | Remove-CsMeetingConfigura
  ```

⊟To remove all the meeting configuration settings that admit anonymous users by default

- And this one removes all the settings that allow anonymous users to be admitted by default:
```
Get-CsMeetingConfiguration | Where-Object {$_.AdmitAnonymousUsersByDefa
```

For more information, see the help topic for the Remove-CsMeetingConfiguration cmdlet.

1.7.9.2 Conferencing Policies

Conferencing Policies

Microsoft Lync Server 2013 > Operations > Managing Meetings and Conferences >

Topic Last Modified: *2012-09-18*

Conferencing policy defines the features and capabilities that users have available during a conference (also known as a meeting). Conferencing policy settings encompass a wide variety of scheduling and participation options, ranging from whether a meeting can include IP audio and video to the maximum number of people who can attend. Administrators can use conferencing policy to manage security, bandwidth, and legal aspects of meetings.

You can define conferencing policy on three levels: global scope, site scope, and user scope. Settings apply to a specific user from the narrowest scope to the widest scope. If you assign a user policy to a user, those settings take precedence. If you do not assign a user policy, site settings apply. If no user or site policies apply, global policy provides the default settings.

A global policy exists by default, so you cannot create a new global policy. You also cannot delete the existing global policy, but you can change the existing global policy to customize your default settings.

- View Conferencing Policy Information
- Create or Modify a Conferencing Policy
- Delete an Existing Conferencing Policy
- Conferencing Policy Settings Reference

1.7.9.2.1 View Conferencing Policy Information

View Conferencing Policy Information

Operations > Managing Meetings and Conferences > Conferencing Policies >

Topic Last Modified: *2013-02-23*

In Lync Server 2013 Control Panel, you use conferencing policies to control how conferencing is implemented in your deployment. This includes the following conferencing policies:

- A global policy that is created by default when you deploy Lync Server 2013.
- Optional site-level and user-level policy that you can create and use to specify how conferencing is implemented for specific sites or users.

To view conferencing policy settings

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Conferencing** and then click **Conferencing Policy**.
4. On the **Conferencing Policy** page, double-click the conferencing policy that you would like to view.
5. In **Edit File Filter**, select the **Show Details...** check box.

   Edit Conferencing Policy - <policy> opens displaying the settings for the selected policy. For details about configuring the settings, see Create or Modify a Conferencing Policy.

Viewing Conferencing Policies by Using Windows PowerShell Cmdlets

Conferencing policies can be viewed by using Windows PowerShell and the Get-CsConferencingPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view conferencing policies

- To view information about all your conferencing policies, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsConferencingPolicy
  ```

  That will return information similar to this:

  ```
  Identity                                  : Global
  AllowIPAudio                              : True
  AllowIPVideo                              : True
  AllowMultiView                            : True
  Description                               :
  AllowParticipantControl                   : True
  AllowAnnotations                          : True
  DisablePowerPointAnnotations              : False
  AllowUserToScheduleMeetingsWithAppSharing : True
  AllowNonEnterpriseVoiceUsersToDialOut     : False
  AllowAnonymousUsersToDialOut              : False
  AllowAnonymousParticipantsInMeetings      : True
  AllowExternalUsersToSaveContent           : True
  AllowExternalUserControl                  : False
  AllowExternalUsersToRecordMeeting         : False
  AllowPolls                                : True
  AllowSharedNotes                          : True
  EnableDialInConferencing                  : True
  EnableAppDesktopSharing                   : Desktop
  AllowConferenceRecording                  : False
  EnableP2PRecording                        : False
  EnableFileTransfer                        : True
  EnableP2PFileTransfer                     : True
  EnableP2PVideo                            : True
  AllowLargeMeetings                        : False
  EnableDataCollaboration                   : True
  MaxVideoConferenceResolution              : VGA
  MaxMeetingSize                            : 250
  AudioBitRateKb                            : 200
  VideoBitRateKb                            : 50000
  AppSharingBitRateKb                       : 50000
  FileTransferBitRateKb                     : 50000
  TotalReceiveVideoBitRateKb                : 6000
  EnableMultiViewJoin                       : True
  ```

For more information, see the help topic for the Get-CsConferencingPolicy cmdlet.

Create or Modify a Conferencing Policy

Operations > Managing Meetings and Conferences > Conferencing Policies >

***Topic Last Modified:** 2013-02-07*

Follow these steps to create a user-level or a site-level conferencing policy. For details about how to assign a user-level policy to a user, see Assign a Per-User Conferencing Policy. For a list of all available conferencing policy settings, see Conferencing Policy Settings Reference.

⊟To create a new user or site policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Conferencing Policy**.
4. Click **New**, and then do one of the following:
   - To create a user-level policy, click **User policy**. In **New Conferencing Policy**, in **Name**, type a descriptive name for the policy.
   - To create a site-level policy, click **Site policy**. In the **Select a Site** search field, type all or part of the name of the site for which you want to create a policy. In the list of sites, click the site that you want, and then click **OK**.

     > **Note:**
     > The site name becomes the conferencing policy name, and it cannot be changed.
5. In **Description**, type a description for the policy.
6. Under **Organizer policy**, in **Maximum meeting size**, type the maximum number of users that you want to allow at a meeting. By default, the maximum meeting size is 250.
7. To prevent users from inviting anonymous users to meetings, clear the **Allow participants to invite anonymous users** check box. Anonymous users are users who do not have credentials in your organization’s Active Directory Domain Services (AD DS) and who, therefore, are not authenticated. By default, users can invite anonymous users to meetings.
8. In **Recording**, do one of the following:
   - To prevent participants from recording meetings, click **None**. This is the default setting.
   - To allow participants to record meetings, click **Enable recording**.
9. To allow external participants to record meetings, select the **Allow federated and anonymous participants to record** check box. The default is to prevent external participants from recording meetings.
10. In **Audio/video**, do one of the following:
    - To prevent the use of audio and video, click **None**.
    - To allow the use of audio but not video, click **Enable IP audio**.
    - To allow the use of audio and video, click **Enable IP audio/video**. This is the default setting.
11. If you chose to allow the use of audio in **Audio/video**, do the following:
    - To prevent users from joining the meeting by dialing in, clear the **Enable PSTN dial-in conferencing** check box. By default, users can dial in to meetings by using the public switched telephone network (PSTN).
    - If you allow users to dial in to meetings and you want to allow unauthenticated (anonymous) users to join a meeting by using dial out

phoning, select the **Allow anonymous participants to dial out** check box. With dial-out phoning, the conference server calls the user, and the user answers the phone to join the meeting. By default, anonymous users cannot join a meeting by using dial-out phoning.

12. If you chose to allow the use of video in **Audio/video**, check **Allow multiple video streams** .
13. In **Data collaboration**, do one of the following:
    - To prevent data collaboration, click **None**.
    - To allow data collaboration, click **Enable data collaboration**. This is the default setting.
14. If you chose to allow data collaboration in **Data collaboration**, do the following:
    - To prevent external downloads, clear the **Allow federated and anonymous participants to download content** check box. By default, external users can download content.
    - To prevent file transfers, clear the **Allow participants to transfer files** check box. By default, users can transfer files.
    - To prevent the use of annotations, clear the **Enable annotations** check box. To the use of annotations in shard PowerPoint presentations, clear the **Enable PowerPoint annotations**. By default, annotations are allowed.
    - To prevent the use of polls, clear the **Enable polls** check box. By default, polls are allowed.
15. In **Application sharing**, do one of the following:
    - To prevent the use of application sharing, click **Disable application sharing**.
    - To allow the use of application sharing, click **Enable application sharing**. This is the default setting.
16. If you chose to allow application sharing in **Application sharing**, do the following:
    - To prevent meeting participants from taking control of application sharing, clear the **Allow participants to take control** check box. By default, participants can take control of application sharing.
    - If you chose to allow meeting participants to take control of application sharing, select the **Allow federated and anonymous participants to take control** check box to allow external users to take control of application sharing. By default, external users cannot take control of application sharing.
17. Under **Participant policy**, do one of the following:
    - To prevent both application sharing and desktop sharing, click **Disable application and desktop sharing**.
    - To allow application sharing but not desktop sharing, click **Enable application sharing**.
    - To allow both application sharing and desktop sharing, click **Enable application and desktop sharing**. This is the default setting.
18. To prevent peer-to-peer file transfers, clear the **Enable peer-to-peer file transfer** check box. By default, peer-to-peer file transfers are allowed.
19. To allow peer-to-peer recording, select the **Enable peer-to-peer recording** check box. By default, peer-to-peer recording is not allowed.
20. To allow participants to join with multiple video streams, select the **Enable participants to join with multiple video streams** check box. By default, multiple video streams are allowed.
21. Click **Commit**.

⊟To modify an existing user or site policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Conferencing**

Policy.

4. In the list of conferencing policies, click the policy that you want to change, click **Edit**, and then click **Show details**.
5. In **Edit Conferencing Policy**, modify any of the policy settings, except for the policy name, which cannot be modified.

6. Click **Commit**.

1.7.9.2.3 Delete an Existing Conferencing Policy

Delete an Existing Conferencing Policy

Operations > Managing Meetings and Conferences > Conferencing Policies >

Topic Last Modified: *2013-02-23*

Follow these steps to delete a user-level or a site-level conferencing policy.

Note:

You cannot delete the global conferencing policy.

⊟To delete a site or user conferencing policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Conferencing Policy**.
4. In the list of conferencing policies, click the site or user policy that you want to delete, click **Edit**, and then click **Delete**.

Removing Conferencing Policies by Using Windows PowerShell Cmdlets

You can delete conferencing policies by using Lync Server Management Shell and the **Remove-CsConferencingPolicy** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To remove a specified conferencing policy

- The following command removes the conferencing policy with the Identity RedmondConferencingPolicy:

```
Remove-CsConferencingPolicy -Identity "RedmondConferencingPolicy"
```

⊟To remove all of the conferencing policies applied to the per-user scope

- The following command removes all the conferencing policies configured at the per-user scope:

```
Get-CsConferencingPolicy -Filter "tag:*" | Remove-CsConferencingPolicy
```

⊟To remove all of the conferencing polices that allow recording by external

users

- The following command deletes any conferencing policies that allow external users to record the conference:

```
Get-CsConferencingPolicy | Where-Object {$_.AllowExternalUsersToRecordM
```

For details, see Remove-CsConferencingPolicy.

1.7.9.2.4 Conferencing Policy Settings Reference

Conferencing Policy Settings Reference

Operations > Managing Meetings and Conferences > Conferencing Policies >

Topic Last Modified: *2012-09-30*

The tables in this topic list all the conferencing policy settings that you can specify by using Lync Server 2013 Control Panel.

Organizer Policy Settings

The following table lists all the conferencing policy settings that you can apply to conference organizers.

Organizer Policy Settings

Setting	Description
Maximum meeting size	Sets the maximum number of participants allowed in a meeting.
Allow participants to invite anonymous users	Allows meeting organizers to invite unauthenticated users to meetings.
Enable recording	Allows presenters or attendees to record the meeting.
Allow federated and anonymous participants to record	Allows external and unauthenticated participants to record the meeting.
Enable IP audio	Allows the use of audio in a meeting.
Enable IP audio/video	Allows the use of audio and video in a meeting.
Enable PSTN dial-in conferencing	Allows the user to attend a meeting by dialing in from the public switched telephone network (PSTN).
Allow anonymous participants to dial out	Allows unauthenticated users to join a meeting by using dial-out phoning. With dial-out phoning, the conference server calls the user, and the user answers the phone to join the meeting.
Maximum video resolution allowed for conferencing	Sets the maximum resolution for video conferencing. Valid values are **640*480 (VGA)** and **352*288(CIF)**.

Enable data collaboration	Enables data collaboration conferencing or web conferencing.
Allow federated and anonymous participants to download content	Allows external and unauthenticated participants to download content from the meeting.
Allow participants to transfer files	Allows meeting participants to transfer files during a meeting.
Enable annotations	Allows meeting participants to create annotations in content.
Enable polls	Allows meeting participants hold a poll during a meeting.
Enable application sharing	Allows users to schedule meetings that support application sharing.
Allow participants to take control	Allows participants to take control of another user's shared application.
Allow federated and anonymous participants to take control	Allows external and anonymous participants to take control of another user's shared application. **Note:** If this setting is set to True and **Allow participants to take control** is set to False, this setting is overridden.

Participant Policy Settings

The following table lists all the conferencing policy settings that you can apply to conference participants.

Participant Policy Settings

Setting	Description
Enable application sharing	Allows users to schedule meetings that support application sharing.
Enable application and desktop sharing	Allows users to participate in meetings that support application sharing and desktop sharing. In a conference, the value of this setting that applies to the organizer of the conference will be applied to all anonymous endpoints who also participate.
Enable peer-to-peer file transfer	Allows participants to perform peer-to-peer file transfers during a meeting. A peer-to-peer file transfer does not involve all the meeting participants.
Enable peer-to-peer recording	Allows participants to record peer-to-peer conferencing sessions.

1.7.9.3 Dial-In Conferencing (Configuration/Access Numbers)

Dial-In Conferencing (Configuration/Access Numbers)

Microsoft Lync Server 2013 > Operations > Managing Meetings and Conferences >

Topic Last Modified: *2012-09-18*

The topics in this section describe how to use Lync Server 2013 Control Panel to configure dial-in conferencing for use your Lync Server 2013 environment.

- Enable or Disable Dial-In Conferencing For Meetings
- Dial-In Conferencing Access Numbers
- Configure Dial-in Conferencing Personal Identification Number (PIN) Rules

1.7.9.3.1 Enable or Disable Dial-In Conferencing For Meetings

Enable or Disable Dial-In Conferencing For Meetings

Operations > Managing Meetings and Conferences > Dial-In Conferencing (Configuration/Access Numbers) >

Topic Last Modified: *2012-11-01*

The following procedure describes how to allow user to join a meeting using dial-in.

⊟To enable or disable dial-in conferencing

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Conferencing Policy**.
4. In the list of conferencing policies, select the policy for which you want to enable dial-in conferencing, click **Edit**, and then click **Show details**.
5. To allow users to join meeting by dialing in, check the **Enable PSTN dial-in conferencing** check box. By default, users can dial in to meetings by using the public switched telephone network (PSTN).
6. Click **Commit**.

1.7.9.3.2 Dial-In Conferencing Access Numbers

Dial-In Conferencing Access Numbers

Operations > Managing Meetings and Conferences > Dial-In Conferencing (Configuration/Access Numbers) >

Topic Last Modified: *2012-09-18*

To enable users to join the audio portion of on-premises conferences by dialing in from the public switched telephone network (PSTN), you must configure dial-in conferencing access numbers. Dial-in conferencing access numbers are the numbers that users call to join a conference.

Dial-in access numbers are displayed in meeting invitations and on the Dial-in Conferencing Settings webpage.

Note:
You cannot use a new dial-in access number until Active Directory replication of that access number is complete. Replication can take several hours.

- View Dial-In Conferencing Access Numbers
- Create or Modify a Dial-in Conferencing Access Number
- Delete a Dial-in Conferencing Access Number

1.7.9.3.2.1 View Dial-In Conferencing Access Numbers

View Dial-In Conferencing Access Numbers

Managing Meetings and Conferences > Dial-In Conferencing (Configuration/Access Numbers) > Dial-In Conferencing Access Numbers >

Topic Last Modified: *2013-02-23*

In Lync Server 2013 Control Panel, you provide dial-in access numbers to users so that they can join a meeting externally.

To view dial-in access numbers

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Dial-in Access Number**.
4. On the **Dial-in Access Number** page, click the access number that you would like to view.
5. In **Edit**, select the **Show Details...** check box.

Viewing Dial-in Conferencing Access Numbers by Using Windows PowerShell Cmdlets

Dial-in conferencing access numbers can be viewed by using Windows PowerShell and the Get-CsDialInConferencingAccessNumber cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view dial-in conferencing access numbers

- To view information about all your dial-in conferencing access numbers, type the following command in the Lync Server Management Shell and then press ENTER:

```
Get-CsDialInConferencingAccessNumber
```

That will return information similar to this:

```
Identity            : CN={20ca8dc8-5ff8-41f4-b5bb-22ba9972ae2e},
                      CN=Application Contacts,CN=RTCService=Services,
                          CN=Configuration,DC=litwareinc,DC=com
PrimaryUri              : sip:testnumber@litwareinc.com
DisplayName             : Test
DisplayNumber           : 1-425-555-1019
LineUri                 : tel:+14255551019
PrimaryLanguage         : en-US
SecondaryLanguages      : {}
Pool                    : atl-cs-001.litwareinc.com
HostingProvider         :
Regions                 : {US}
```

For more information, see the help topic for the Get-CsDialInConferencingAccessNumber cmdlet.

1.7.9.3.2.2 Create or Modify a Dial-in Conferencing Access Number

Create or Modify a Dial-in Conferencing Access Number

Deploying Conferencing > Configuring Dial-in Conferencing > Configure Dial-in Conferencing Access Numbers >

Topic Last Modified: *2012-09-17*

Follow these steps if you want to create or modify a dial-in conferencing access number.

Important:

Before you create a new dial-in access number, you must set a dial-in conferencing region in the dial plan that is associated with the new dial-in access number. Multiple dial plans can use the same region.

To create or modify a dial-in access number

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing** and then click **Dial-in Access Number**.
4. On the **Dial-in Access Number** page, do one of the following:
   - Click **New** to open **New Dial-in Access Number**.
   - Click one of the dial-in access numbers in the list, click **Edit**, and then click **Show details**.

   Note:

   Using the search field to search for the contents of a column in the list of dial-in access numbers may not yield the results you expect. Instead, sort the list by the column of interest to identify the dial-in access number you want to view or change.
5. In **Display number**, type the phone number that public switched telephone network (PSTN) phone users dial to join a conference.

   Note:

   This number is displayed in meeting invitations and on the Dial-in Conferencing Settings webpage.
6. In **Display name**, type a description for the dial-in access number. This is the name that is associated with the dial-in access number in Lync search results.

   Note:

This name is displayed in the client when a user calls the access number.

7. In **Line URI**, type the E.164 number of the dial-in access number in TEL URI format, including the + symbol before the number and excluding spaces. For example, tel:+14255550200.

> **Note:**
> The same Line URI cannot be reused by another dial-in conferencing access number.

8. In **SIP URI**, do the following:
   - In the text box, type a unique SIP URI for this dial-in conferencing access number. This SIP URI is displayed in various locations including, but not limited to, call notification messages and previous versions of Communicator clients.

     > **Note:**
     > The same SIP URI cannot be reused by another dial-in conferencing access number. The SIP URI cannot be modified after the access number is created. The only way to change the SIP URI is to delete and recreate the access number.

   - In the drop-down list box, click the domain of the Conferencing Attendant application that supports this dial-in access number.
9. In **Pool**, click the pool that is running the instance of Conferencing Attendant that supports this dial-in access number.

> **Note:**
> If you need to change the pool after you create the access number, you must use the **Move-CsApplicationEndpoint** cmdlet or delete and recreate the access number.

10. In **Primary language**, click the language in which prompts are played for this dial-in access number.

> **Note:**
> The primary language is the language that the Conferencing Attendant uses to answer the call. Supported languages are displayed alongside each access phone number on the Dial-in Conferencing Settings webpage.

11. (Optional) In **Secondary languages (maximum of four)**, click **Add**, select one or more additional languages that you want to support for callers to this dial-in access number, and then click **OK**.

> **Note:**
> You can choose up to four secondary languages for each dial-in access number. Users can select a secondary language before entering the conference ID when they dial in to a conference.

12. To add a region for the dial-in access number, under **Associated regions**, click **Add**, click one or more regions that are associated with the dial plans for this dial-in access number, and then click **OK**.
13. To delete a region from the dial-in access number, under **Associated regions**, click the region you want to delete, and then click **Remove**.

14. Click **Commit**.

1.7.9.3.2.3 Delete a Dial-in Conferencing Access Number

Delete a Dial-in Conferencing Access Number

Managing Meetings and Conferences > Dial-In Conferencing (Configuration/Access Numbers) > Dial-In Conferencing Access Numbers >

Topic Last Modified: *2013-02-23*

Follow these steps to delete a dial-in conferencing access number.

To delete a dial-in conferencing access number

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**, and then click **Dial-in Access Number**.
4. On the page, click the dial-in number you want to delete in the list, click **Edit**, and then click **Delete**.
5. Click **OK**.

Removing Dial-in Conferencing Access Numbers by Using Windows PowerShell Cmdlets

Dial-in conferencing access numbers can be deleted by using Windows PowerShell and the **Remove-CsDialInConferencingAccessNumber** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specific dial-in conferencing access number

- This command deletes the dial-in conferencing access number with Identity sip:RedmondDialInAccess@litwareinc.com:

```
Remove-CsDialInConferencingAccessNumber -Identity "sip:RedmondDialInAcc
```

To remove all the dial-in conferencing access numbers assigned to a specific region

- This command deletes all the dial-in conferencing access numbers associated with the Northwest region:

```
Get-CsDialInConferencingAccessNumber -Region "Northwest" | Remove-CsDia
```

To remove dial-in conferencing access numbers based on primary language

- This command deletes all the dial-in conferencing access numbers where Italian is the primary language:

```
Get-CsDialInConferencingAccessNumber | Where-Object {$_.PrimaryLanguage
```

For more information, see the help topic for the Remove-CsDialInConferencingAccessNumber cmdlet.

1.7.9.3.3 Configure Dial-in Conferencing Personal Identification Number (PIN) Rules

Configure Dial-in Conferencing Personal Identification Number (PIN) Rules

Operations > Managing Meetings and Conferences > Dial-In Conferencing (Configuration/Access Numbers) >

Topic Last Modified: *2012-06-19*

Lync Server 2013 users who have Active Directory Domain Services (AD DS) credentials in your organization can join dial-in conferences as authenticated users by using a personal identification number (PIN). PIN policy defines the rules for how dial-in conferencing PINs work.

You can create a new PIN policy if you want a specific policy to apply to a site or to a certain group of users. If you want to use the same PIN policy for your entire organization, you can use the global PIN policy and modify it as needed. PIN policies apply to users from the narrowest scope to the widest scope. If you assign a user-level PIN policy to a user, those settings take precedence. If you do not assign a user policy, the site-level PIN policy applies, if it exists. If no user or site policies apply, global PIN policy provides the default settings.

- Modify the Default Dial-in Conferencing PIN Settings
- Create or Modify Dial-in Conferencing PIN Settings for a Site or Group of Users
- Delete Dial-in Conferencing PIN Settings for a Site or Group of Users

1.7.9.3.3.1 Modify the Default Dial-in Conferencing PIN Settings

Modify the Default Dial-in Conferencing PIN Settings

Deploying Conferencing > Configuring Dial-in Conferencing > (Optional) Verify PIN Policy Settings >

Topic Last Modified: *2012-10-18*

The global PIN policy defines the rules for dial-in conferencing PINs at the forest level. Follow these steps to modify the global dial-in conferencing PIN policy. For details about creating or modifying a dial-in conferencing PIN policy at the site or user level, see Create or Modify Dial-in Conferencing PIN Settings for a Site or Group of Users.

⊟To modify the global PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click the **Global** policy, click **Edit**, and then click **Show details**.
5. In **Edit PIN Policy**, in **Minimum PIN length**, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
6. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum

number of attempts is automatically determined.

7. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
8. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
9. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
10. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
11. To allow common patterns of digits in PINs, such as sequential numbers and repetitive sets of numbers, select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

    Important:

    We recommend that you do not allow common patterns.

12. Click **Commit**.

1.7.9.3.3.2 Create or Modify Dial-in Conferencing PIN Settings for a Site or Group of Users

Create or Modify Dial-in Conferencing PIN Settings for a Site or Group of Users

Deploying Conferencing > Configuring Dial-in Conferencing > (Optional) Verify PIN Policy Settings >

Topic Last Modified: *2012-10-18*

Follow these steps to create or modify a user-level or a site-level dial-in conferencing personal identification number (PIN) policy. For details about how to change the global PIN policy, see Modify the Default Dial-in Conferencing PIN Settings.

⊟To create a user or site PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click **New**, and then do one of the following:
    - To create a user-level policy, click **User policy**. In **New PIN Policy**, in **Name**, type a name that describes the policy.
    - To create a site-level policy, click **Site policy**. In the **Select a Site** search field, type all or part of the name of the site for which you want to create a policy. In the list of sites, click the site you want, and then click **OK**.
5. In the **Description** field, type a description of the PIN policy.
6. In the **Minimum PIN length** field, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
7. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum number of attempts is automatically determined.

8. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
9. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
10. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
11. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
12. To allow common patterns of digits in PINs, such as sequential numbers and repetitive sets of numbers, select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

    Important:

    We recommend that you do not allow common patterns.

13. Click **Commit**.

⊟To change a user or site PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, click the PIN policy that you want to change, click **Edit**, and then click **Show details**.
5. In **Edit PIN Policy**, modify any of the policy settings (except for the policy name, which cannot be modified).
6. Click **Commit**.

1.7.9.3.3.3 Delete Dial-in Conferencing PIN Settings for a Site or Group of Users

Delete Dial-in Conferencing PIN Settings for a Site or Group of Users

Managing Meetings and Conferences > Dial-In Conferencing (Configuration/Access Numbers) > Configure Dial-in Conferencing Personal Identification Number (PIN) Rules >

Topic Last Modified: *2012-10-18*

Follow these steps to delete a user-level or a site-level PIN policy.

Note:

You cannot delete the global PIN policy.

⊟To delete a user or site PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Conferencing**, and then click **PIN Policy**.
4. On the **PIN Policy** page, in the search field, type all or part of the name of the policy you want to delete.
5. In the list of policies, click the policy that you want, click **Edit**, and then click **Delete**.

6. Click **OK**.

1.7.10 Managing Devices, Phones, and Client Applications

Managing Devices, Phones, and Client Applications

See Also

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2013-02-19*

The topics in this section provide step-by-step procedures for tasks that you can perform by using the **Clients** group in Lync Server 2013 Control Panel.

- Common Area Phones
- Conferencing Devices
- Mobile Phones (Policy/Push Notification)
- Test Devices
- Lync Phone Edition Configuration Settings
- Device Update Web Service
- Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013

⊟See Also

Concepts

Operations
Deploying Clients and Devices

1.7.10.1 Common Area Phones

Common Area Phones

Microsoft Lync Server 2013 > Operations > Managing Devices, Phones, and Client Applications >

Topic Last Modified: *2013-02-20*

Common area phones are IP phones that are not associated with an individual user. Instead of being located in someone’s office, common area phones are typically located in building lobbies, cafeterias, employee lounges, meeting rooms, and other locations where a large number of people are likely to gather. Unlike other phones in Lync Server, which are typically maintained by using voice policies and dial plans that are assigned to individual users, common area phones do not have individual users assigned to them. This means that they must be managed differently than your other phones.

To manage common area phones, you create Active Directory Domain Services (AD DS) contact objects for all your common area phones that, like user accounts, can be assigned policies and voice plans. This approach enables you to maintain control over common area phones, even though those phones are not associated with an individual user.

Use the topics in this section to learn how to create contact objects for common area phones, modify and delete them, and configure and view configuration information about the common area phones in your deployment.

Note:

You have three options for common area phones: the Aastra 6721ip common area phone, the HP 4110 IP Phone, and the Polycom CX500 IP common area phone. The Polycom CX3000 IP conferencing phone is another variant common area phone. However, it is intended for use in conference rooms. For details about common area phones, see the Common Area Phones section of Choosing New Devices.

- View Common Area Phone Information
- Create or Modify a Common Area Phone Contact Object
- Enable or Disable Hot Desking
- Delete a Common Area Phone Contact Object
- Assign Policies to a Common Area Phone

1.7.10.1.1 View Common Area Phone Information

View Common Area Phone Information

Operations > Managing Devices, Phones, and Client Applications > Common Area Phones >

Topic Last Modified: *2013-02-20*

You can view information about the common area phones configured for use in your organization by using the **Get-CsCommonAreaPhone** cmdlet. Used without any parameters, this cmdlet returns information about all your common area phones. Optional parameters provide different ways for you to filter information. For example, you can return all the common area phones that have contact objects in a specified organizational unit (OU) or all the contacts objects located in a specified building. For details about **Get-CsCommonAreaPhone** parameters, see Get-CsCommonAreaPhone.

Run **Get-CsCommonAreaPhone** either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

⊟Viewing Information about All Your Common Area Phones

- To view information about all your common area phones, type the following command in the Lync Server Management Shell, and then press Enter:

```
Get-CsCommonAreaPhone
```

You'll get information similar to this:

```
Identity            : CN=Building 14 Lobby,OU=Redmond,
                      DC=litwareinc,DC=com
RegistrarPool       : atl-cs-001.litwareinc.com
Enabled             : True
SipAddress          : sip:4714e34b-9781-421d-b07a-
                      52056b5b4a56@litwareinc.com
ClientPolicy        :
PinPolicy           :
VoicePolicy         :
MobilityPolicy      :
GroupChatPolicy     :
ConferencingPolicy  :
LineURI             : tel:+14255550712
DisplayNumber       : 1-425-555-0712
DisplayName         : Building 14 Lobby
Description         :
ExUmEnabled         : False
```

For details, see the Help topic for the Get-CsCommonAreaPhone cmdlet.

1.7.10.1.2 Create or Modify a Common Area Phone Contact Object

Create or Modify a Common Area Phone Contact Object

Operations > Managing Devices, Phones, and Client Applications > Common Area Phones >

Topic Last Modified: *2013-02-20*

To create Active Directory Domain Services (AD DS) contact objects for all your common area phones, use the **New-CsCommonAreaPhone** cmdlet. This cmdlet can either create new contact objects for use with common area phones, or it can associate existing contact objects with a new common area phone. To modify the properties of the contact objects associated with common area phones, use the **Set-CsCommonAreaPhone** cmdlet. Optional parameters for **Set-CsCommonAreaPhone** enable you to change items, such as the contact’s Active Directory display name or the line Uniform Resource Identifier (URI) associated with the phone, and enable and disable the account for use with Lync Server. For details about all the available modifications, see the Parameters section at Set-CsCommonAreaPhone. For details about **New-CsCommonAreaPhone** parameters, see New-CsCommonAreaPhone.

You can run these two cmdlets from either the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

Creating a common area phone contact object

- To create a new common area phone contact object, use the **New-CsCommonAreaPhone** cmdlet. At a minimum, you must supply the following information when creating a contact object:
  - **LineUri**: The telephone number assigned to the common area phone. Note that you must use the E.164 format when specifying the phone number.
  - **RegistrarPool**: The fully qualified domain name (FQDN) of the Registrar pool that will host the contact object.
  - **OU**: Distinguished name of the Active Directory container where the contact object will be created.

  We also recommend that you provide an Active Directory Domain Services (AD DS) display name. Otherwise, you will need to use a GUID to specify the phone Identity. For example:

  ```
  New-CsCommonAreaPhone -LineUri "tel:+12065551219" -RegistrarPool "atl-c
  ```

Modifying a common area phone contact object

- To modify the properties of an existing common area phone, contact object use the **Set-CsCommonAreaPhone** cmdlet. For example, this command configures the SIP address for the common area phone with the DisplayName Lobby:

  ```
  Set-CsCommonAreaPhone -Identity "Lobby" -SipAddress "sip:lobby@litwarei
  ```

For details, see the Help topics for the New-CsCommonAreaPhone cmdlet and the Set-CsCommonAreaPhone cmdlet.

1.7.10.1.3 Enable or Disable Hot Desking

Enable or Disable Hot Desking

Operations > Managing Devices, Phones, and Client Applications > Common Area Phones >

Topic Last Modified: *2013-02-20*

You can set up common area phones as *hot-desk phones*. With hot-desk phones, users can log on to their own user account, and, after they are logged on, use Lync Server features and their own user profile settings. Hot desking is managed by using client policies: to enable or disable hot desking, you need to modify the client policies that are used by your common area phones. For details about how to determine the conferencing policies that have been assigned to your common area phones, see View Common Area Phone Information.

You use the EnableHotdesking parameter of the **New-CSClientPolicy** cmdlet or the **Set-CSClientPolicy** cmdlet to enable or disable hot desking on a phone, as follows. Run these cmdlets from either the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

Enabling hot desking

- To enable hot desking for a common area phone, you must modify the client policy that has been assigned to that phone (or collection of phones).

  After you have identified the policy that needs to be modified, the next step is to use the **Set-CsClientPolicy** cmdlet to set the EnableHotdesking parameter to True. For example:

  ```
  Set-CsClientPolicy -Identity "CommonAreaPhonePolicy" - EnableHotdesking
  ```

- Alternatively, you can use the **New-CsClientPolicy** cmdlet to create a new client policy that enables hot desking. For example:

  ```
  New-CsClientPolicy -Identity "NewCommonAreaPhonePolicy" - EnableHotdesk
  ```

Important:

After this policy has been created, you must assign it to the appropriate common area phones. For details, see Assign Policies to a Common Area Phone.

Disabling hot desking

- To disable hot desking for a common area phone, reset the EnableHotdesking parameter of the **Set-CsClientPolicy** cmdlet to the default value of False. For example:

  ```
  Set-CsClientPolicy -Identity "CommonAreaPhonePolicy" - EnableHotdesking
  ```

For details, see the Help topics for the New-CsClientPolicy cmdlet and the Set-CsClientPolicy cmdlet.

1.7.10.1.4 Delete a Common Area Phone Contact Object

Delete a Common Area Phone Contact Object

See Also

Operations > Managing Devices, Phones, and Client Applications > Common Area Phones >

Topic Last Modified: *2013-02-20*

You might want to delete the contact object associated with a common area phone. For example, if you remove the phone from an employee lounge, there’s no need to have a contact object associated with that phone. The **Remove-CsCommonAreaPhone** cmdlet provides a way for you to delete common area phone accounts. When you run this cmdlet, the phone is deleted from the list of common area phones returned by **Get-CsCommonAreaPhone**. In addition, the contact object associated with that phone is deleted from Active Directory Domain Services (AD DS).

Use **Remove-CsCommonAreaPhone** to remove one common area phone or all common area phones that have a common element, such as a display name or country and area code. You can run this cmdlet from either the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

Removing a Specified Common Area Phone

- The following command removes the common area phone with the SIP address sip:mainlobby@litwareinc.com:

```
Remove-CsCommonAreaPhone -Identity "sip:mainlobby@litwareinc.com"
```

Removing Common Area Phones Based on Their Display Name

- This command removes all the common area phones where the display name includes the string value "Building 14":

```
Get-CsCommonAreaPhone | Where-Object {$_.DisplayName -match "Building 1
```

Removing Common Area Phones Based on Their Country and Area Codes

- This command removes all the common area phones for the United States (country code 1) and the area code 425:

```
Get-CsCommonAreaPhone | Where-Object {$_.LineUri  -match "^tel:\+1425"}
```

For details, see the Help topic for the Remove-CsCommonAreaPhone cmdlet.

See Also

Other Resources

Get-CsCommonAreaPhone

1.7.10.1.5 Assign Policies to a Common Area Phone

Assign Policies to a Common Area Phone

See Also

Operations > Managing Devices, Phones, and Client Applications > Common Area Phones >

Topic Last Modified: *2013-02-20*

After you create your policy for common area phones (for details, see Create a Voice Policy and Configure PSTN Usage Records), you can assign the policy to a common area phone by using Windows PowerShell and the appropriate **Grant-Cs** cmdlet. These cmdlets can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

Assigning a Policy to a Single Common Area Phone

- The following command assigns the per-user voice policy RedmondVoice to the common area phone that has the Identity Building 14 Lobby.

```
Grant-CsVoicePolicy -Identity "Building 14 Lobby" -PolicyName "RedmondV
```

Assigning a Policy to Multiple Common Area Phones

- In this example, the per-user voice policy RedmondVoice is assigned to all the common area phones configured for use in the organization.

```
Get-CsCommonAreaPhone | Grant-CsVoicePolicy  -PolicyName "RedmondVoiceP
```

For details, see the Help topics for the Grant-CsVoicePolicy.

See Also

Other Resources

Get-CsCommonAreaPhone

1.7.10.2 Conferencing Devices

Conferencing Devices

Microsoft Lync Server 2013 > Operations > Managing Devices, Phones, and Client Applications >

Topic Last Modified: *2013-02-20*

Conferencing devices bring Lync Phone Edition features into conference rooms, enabling people in the room to hear, and, depending on the device, see people in other locations.

Use the topics in this section to learn how to set up and manage your conferencing devices.

Note:

Lync Server provides support for two conferencing devices: the Polycom CX5000, which replaced the discontinued Microsoft RoundTable conferencing device, and the Polycom CX3000, the IP conferencing device. For details about conferencing devices, see the Conferencing Devices section of Choosing New Devices.

- View Conferencing Device Information
- Create or Modify a Conferencing Device Contact Object
- Enable or Disable a Conferencing Device
- Move a Conferencing Device to a New Registrar Pool

1.7.10.2.1 View Conferencing Device Information

View Conferencing Device Information

Operations > Managing Devices, Phones, and Client Applications > Conferencing Devices >

Topic Last Modified: *2013-02-20*

You can view information about the conferencing devices configured for use in your organization by using Windows PowerShell and the **Get-CsMeetingRoom** cmdlet. Run the

Get-CsMeetingRoom cmdlet from either the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:
For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

If you use the **Get-CsMeetingRoom** cmdlet without any parameters, it returns information about all your conferencing devices. Optional parameters provide different ways for you to filter information. For details, see the Parameters section of Get-CsMeetingRoom.

Viewing Information about All Your Conferencing Devices

- To view details about all your conferencing devices, type the following command in the Lync Server Management Shell, and then press Enter:

  ```
  Get-CsMeetingRoom
  ```

  This cmdlet returns information similar to the following for each conferencing device. Note that this example shows only some of the information that you'll see when you run this cmdlet:

  ```
  ContactOptionFlags                 : 64
  OwnerUrn                           : urn:device:roomsystem
  OriginatorSid                      :
  SamAccountName                     : room12129
  UserPrincipalName                  : room1219@litwareinc.com
  FirstName                          :
  LastName                           :
  WindowsEmailAddress                :
  Sid                                : S-1-5-21-2831376166-2963252556-2165
  LineServerURI                      :
  AudioVideoDisabled                 : False
  IPPBXSoftPhoneRoutingEnabled       : False
  RemoteCallControlTelephonyEnabled  : False
  PrivateLine                        :
  AcpInfo                            : {}
  HostedVoiceMail                    :
  DisplayName                        : Room 1219
  ```

Viewing Information about a Specific Conferencing Device

- To view information for a specific conferencing device, include the Identity parameter followed by the conferencing device identity (typically, the Active Directory display name). For example:

  ```
  Get-CsMeetingRoom -Identity "Room 1219"
  ```

For details, see the Help topic for the Get-CsMeetingRoom cmdlet.

1.7.10.2.2 Create or Modify a Conferencing Device Contact Object

Create or Modify a Conferencing Device Contact Object

Operations > Managing Devices, Phones, and Client Applications > Conferencing Devices >

Topic Last Modified: *2013-02-20*

To create a conferencing room object, first create an Active Directory user account to represent the device. Then, use the **Enable-CsMeetingRoom** cmdlet to enable that account to function as a conferencing device. If you need to change the properties of an existing conferencing device, use the **Set-CsMeetingRoom** cmdlet.

These cmdlets can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

> **Note:**
> For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

Creating a Conferencing Device

- After you create the Active Directory user account that represents the new conferencing device, enable it by using the **Enable-CsMeetingRoom** cmdlet. Be sure to include a) the conferencing device identity, b) the registrar pool where the room account will be homed, and c) the SIP address to be assigned to that account. For example:

```
Enable-CsMeetingRoom -Identity "Redmond Conferencing device" -Registrar
```

Modifying a Conferencing Device

- To modify the property values of an existing conferencing device, use the **the Set-CsMeetingRoom** cmdlet. For example, the following command updates the phone number (LineUri) associated with a conferencing device:

```
Set-CsMeetingRoom -Identity "Redmond Conferencing device" -LineUri "tel
```

For details, see the Help topics for the Enable-CsMeetingRoom cmdlet and the Set-CsMeetingRoom cmdlet.

1.7.10.2.3 Enable or Disable a Conferencing Device

Enable or Disable a Conferencing Device

Operations > Managing Devices, Phones, and Client Applications > Conferencing Devices >

Topic Last Modified: *2013-02-20*

Enable and disable a conferencing device by using the **Enable-CsMeetingRoom** cmdlet and the **Disable-CsMeetingRoom** cmdlet. These cmdlets can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

> **Note:**
> For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

Enabling a Conferencing Device

- To enable a conferencing device, use the **Enable-CsMeetingRoom** cmdlet. When enabling a conferencing device, you must include a) the conferencing device identity, b) the Registrar pool where the room account will be homed, and c) the SIP address to be assigned to that account.

```
Enable-CsMeetingRoom -Identity "Redmond Conferencing device" -Registrar
```

Disabling a Conferencing Device

- To disable a conferencing device, use the **Disable-CsMeetingRoom** cmdlet. Make sure that you specify the identity of the conferencing device to be disabled:

  ```
  Disable-CsMeetingRoom -Identity "sip:RedmondMeetingRoom@litwareinc.com"
  ```

For details, see the Help topics for the Enable-CsMeetingRoom cmdlet and the Disable-CsMeetingRoom cmdlet.

1.7.10.2.4 Move a Conferencing Device to a New Registrar Pool

Move a Conferencing Device to a New Registrar Pool

Operations > Managing Devices, Phones, and Client Applications > Conferencing Devices >

Topic Last Modified: *2013-02-20*

Move a conferencing device from one Registrar pool to another by using the **Move-CsMeetingRoom** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:

For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

Moving a Conferencing Device to a New Registrar Pool

- To move a conferencing device, you must specify the identity of the room to be moved, and then set the Target parameter to the fully qualified domain name (FQDN) of the Registrar pool the device will be moved to. For example:

  ```
  Move-CsMeetingRoom -Target "atl-cs-001.litwareinc.com" -Identity "Room
  ```

For details, see the Help topic for the Move-CsMeetingRoom cmdlet.

1.7.10.3 Mobile Phones (Policy/Push Notification)

Mobile Phones (Policy/Push Notification)

Microsoft Lync Server 2013 > Operations > Managing Devices, Phones, and Client Applications >

Topic Last Modified: *2012-10-15*

You can configure mobility policies and push notifications for Lync Server 2013 from the **Clients** section of Lync Server 2013 Control Panel. Use the procedures in this section to configure your mobile phone settings.

- Mobility Policies
- Push Notifications

1.7.10.3.1 Mobility Policies

Mobility Policies

See Also

Operations > Managing Devices, Phones, and Client Applications > Mobile Phones (Policy/Push Notification) >

Topic Last Modified: *2012-10-18*

Use the following procedures to configure mobility policies for Lync Server 2013.

- Create or Modify a Mobility Policy
- Assign a Per-User Mobility Policy
- Enforce Phone Locking

⊟See Also

Other Resources

Planning for Mobility

1.7.10.3.1.1 Create or Modify a Mobility Policy

Create or Modify a Mobility Policy

See Also

Managing Devices, Phones, and Client Applications > Mobile Phones (Policy/Push Notification) > Mobility Policies >

Topic Last Modified: *2013-02-23*

You can create or modify mobility policy to allow mobile users to use supported mobile devices for Lync functionality such as instant messaging (IM), presence, and contacts. You can create or modify mobility policies from Lync Server 2013 Control Panel or Lync Server 2013 Management Shell

⊟To create a mobility policy with Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Mobility Policy** navigation button.
4. On the **Mobility Policy** page, click **New**, and do one of the following:
   4.a. To create a site mobility policy, click **Site policy**, click a site, click **OK**, review the default settings, and, if you want to, make any changes.
   4.b. To create a user mobility policy, click **User policy**, type a name, review the default settings, and if you want to, make any changes.
5. Click **Commit**.

⊟To modify a mobility policy with Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Mobility Policy** navigation button.

4. On the **Mobility Policy** page, click one of the existing mobility policies.
5. On the **Edit** menu, click **Show details**.
6. Edit any of the settings.
7. Click **Commit**.

Creating External Access Policies by Using Windows PowerShell Cmdlets

You can create mobility policies (at the site scope or the per-user scope) by using Windows PowerShell and the **New-CsMobilityPolicy** cmdlet. Additionally, you can use the **Set-CsMobilityPolicy** cmdlet to modify any of your existing policies, including the global policy. These cmdlets can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To create a mobility policy at the site scope

- This command creates a new mobility policy for the Redmond site:

  ```
  New-CsMobilityPolicy -Identity "site:Redmond"
  ```

  Because no parameters (other than the mandatory Identity parameter) were specified in the preceding command, the policies will use the default values for all its properties.

To create a mobility policy at the per-user scope

- To create a mobility policy at the per-user scope, specify a unique Identity for the policy:

  ```
  New-CsMobilityPolicy -Identity "RedmondMobilityPolicy"
  ```

To change a single property value when creating a mobility policy

- To create policies that use different property values, include the appropriate parameter and parameter value. For example, this command creates mobility policy that disables Call via Work:

  ```
  New-CsMobilityPolicy -Identity "site:Redmond" -EnableOutsideVoice $Fals
  ```

To change multiple property values when creating a mobility policy

- Multiple property values can be modified by including multiple parameters. For example, this command creates a policy that disables both mobility and Call via Work:

  ```
  New-CsMobilityPolicy "site:Redmond" -EnableMobility $False -EnableOutsi
  ```

For details, see the Help topic for the New-CsMobilityPolicy and the Set-CsMobilityPolicy cmdlets.

See Also

Tasks

Configuring Mobility Policy

Assign a Per-User Mobility Policy

See Also

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Assigning Per-User Policies >

Topic Last Modified: *2013-02-22*

The mobility policy is one of the individual settings of a user account that you can configure in Lync Server Control Panel or Lync Server Management Shell.

⊟To assign a per-user mobility policy with Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

     > **Tip:**
     > To add additional search clauses to your query, click **Add Filter**.

   - Click **Find**.
6. Click a user in the search results, click **Action**, and then click **Assign policies**.

   > **Tip:**
   > If you want the same per-user mobility policy to apply to multiple users, select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **Mobility policy**, do one of the following:

   > **Note:**
   > Because there are multiple policies that you can configure in **Assign Policies**, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

   - Select **<Automatic>** to allow Lync Server 2013 to automatically choose either the global-level policy or, if defined, the site-level policy.
   - Click the name of a per-user mobility policy you previously defined on the **Mobility Policy** page.

Tip:
To help you decide the policy you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

Assigning a Per-User Mobility Policy by Using Windows PowerShell Cmdlets

You can assign per-user mobility policies by using Windows PowerShell and the **Grant-CsMobilityPolicy** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user mobility policy to a single user

- The following command assigns the per-user mobility policy RedmondMobilityPolicy to the user Ken Myer.

```
Grant-CsMobilityPolicy -Identity "Ken Myer" -PolicyName "RedmondMobilit
```

To assign a per-user mobility policy to multiple users

- The following command assigns the per-user mobility policy RedmondMobilityPolicy to all the users who are currently assigned the policy NorthAmericaMobilityPolicy. For details about the Filter parameter used in this command, see Get-CsUser.

```
Get-CsUser -Filter {MobilityPolicy -eq "NorthAmericaMobilityPolicy"} |
```

To unassign a per-user mobility policy

- The following command unassigns any per-user mobility policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsMobilityPolicy -Identity "Ken Myer" -PolicyName $Null
```

For details, see Grant-CsMobilityPolicy.

See Also

Tasks

Configuring Mobility Policy

1.7.10.3.1.3 Enforce Phone Locking

Enforce Phone Locking

See Also

Managing Devices, Phones, and Client Applications > Mobile Phones (Policy/Push Notification) > Mobility Policies >

Topic Last Modified: *2013-02-23*

Lync Phone Edition devices can be locked for security purposes. If you enforce phone lock, the device running Lync Phone Edition locks after a period of time that you configure.

When a phone is locked, a user can make calls but cannot access calendar and contact information, voice mail, or call logs or use search. To unlock the phone, the user enters a PIN.

To enforce phone lock, enable and configure it by using Lync Server Control Panel or Lync Server PowerShell cmdlets. You can enforce phone lock globally or only within the site for which it is configured.

To configure and enforce the phone lock

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. Click **Clients**, and then click **Device Configuration**.
4. On the **Device Configuration** tab, in the list of device configurations, double-click the configuration for which you want to change the phone lock settings.
5. In the **Edit Device Configuration** dialog box, verify that the **Enforce device locking** check box is selected.
6. In **Minimum PIN length**, accept the default value for the minimum number of digits that the unlock PIN must contain or specify a new value. The range for the PIN length is four to 15 digits, and the default is six.
7. In **Phone lock time-out**, accept the default value for the minimum length of time before the phone locks itself or specify a new value. The range for the timeout is 0 to 60 minutes, and the default is 10. Enter the value in the format HH:MM:SS.
8. Click **Commit**.

Enforcing Phone Locking by Using Windows PowerShell Cmdlets

Phone locking can be enforced by using the Set-CsUCPhoneConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable phone locking

- The following command enables phone locking for the Redmond site. To disable phone locking, set the EnforcePhoneLock property to False ($False).

```
Set-CsUCPhoneConfiguration -Identity" site:Redmond" -EnforcePhoneLock $
```

To enable phone locking and modify the phone lock timeout

- This command enables phone locking and also sets the phone lock timeout to 30 minutes.

```
Set-CsUCPhoneConfiguration -Identity" site:Redmond" -EnforcePhoneLock $
```

To enable phone locking throughout the organization

- In this example, phone locking is enabled on all the UC phone configuration settings in use in the organization.

```
Get-CsUCPhoneConfiguration | Set-CsUCPhoneConfiguration  -EnforcePhoneL
```

For more information, see the help topic for the Set-CsUCPhoneConfiguration cmdlet.

⊟See Also

Concepts

Managing Lync Server 2013 Security and Authentication

Other Resources

Managing Devices, Phones, and Client Applications

1.7.10.3.2 Push Notifications

Push Notifications

See Also

Operations > Managing Devices, Phones, and Client Applications > Mobile Phones (Policy/Push Notification) >

Topic Last Modified: *2012-10-19*

You can manage push notifications from the **Clients** section of Lync Server 2013 Control Panel.

- Enabling or Disabling Push Notifications for iPhones
- Enabling or Disabling Push Notifications for Windows Phones
- Viewing Information about Push Notification Settings

⊟See Also

Tasks

Configuring for Push Notifications

1.7.10.3.2.1 Enabling or Disabling Push Notifications for iPhones

Enabling or Disabling Push Notifications for iPhones

See Also

Managing Devices, Phones, and Client Applications > Mobile Phones (Policy/Push Notification) > Push Notifications >

Topic Last Modified: *2013-02-23*

Push notifications, in the form of badges, icons, or alerts, can be sent to an iPhone even when the mobile application is inactive. Push notifications notify a user of events such as a new or missed IM invitation and voice mail. You can enable or disable push notifications for iPhone by using either Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

⊟To enable push notifications for iPhone by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Push Notification Configuration** navigation button.
4. On the **Push Notification Configuration** page, click the site you want to edit, click the **Edit** menu, and then click **Show details**.
5. Click the **Enable Apple push notifications** checkbox.

6. Click **Commit**.

To disable push notifications for iPhone by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Push Notification Configuration** navigation button.
4. On the **Push Notification Configuration** page, click the site you want to edit, click the **Edit** menu, and then click **Show details**.
5. Clear the **Enable Apple push notifications** checkbox.
6. Click **Commit**.

Enabling or Disabling Push Notifications to iPhone by Using Windows PowerShell Cmdlets

Push notifications to Apple iPhone can be enabled or disabled by using the **Set-CsPushNotificationConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable push notifications for iPhone

- To enable push notifications for iPhone set the value of the EnableApplePushNotificationService property to True ($True). For example:

```
Set-CsPushNotificationConfiguration -Identity "site:Redmond" -EnableApp
```

To disable push notifications for iPhone

- To disable push notifications for iPhone set the value of the EnableApplePushNotificationService property to False ($False). For example:

```
Set-CsPushNotificationConfiguration -Identity "site:Redmond" -EnableApp
```

For more information, see the help topic for the Set-CsPushNotificationConfiguration cmdlet.

See Also

Tasks

Configuring for Push Notifications

1.7.10.3.2.2 Enabling or Disabling Push Notifications for Windows Phones

Enabling or Disabling Push Notifications for Windows Phones

See Also

Managing Devices, Phones, and Client Applications > Mobile Phones (Policy/Push Notification) > Push Notifications >

Topic Last Modified: *2013-02-23*

Push notifications, in the form of badges, icons, or alerts, can be sent to a Windows Phone even when the mobile application is inactive. Push notifications notify a user of events such as a new or missed IM invitation and voice mail. You can enable or disable push notifications for Windows Phone devices by using either Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

⊟To enable push notifications for Windows Phone by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Push Notification Configuration** navigation button.
4. On the **Push Notification Configuration** page, click the site you want to edit, click the **Edit** menu, and then click **Show details**.
5. Click the **Enable Microsoft push notifications** checkbox.
6. Click **Commit**.

⊟To disable push notifications for Windows Phone by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Push Notification Configuration** navigation button.
4. On the **Push Notification Configuration** page, click the site you want to edit, click the **Edit** menu, and then click **Show details**.
5. Clear the **Enable Microsoft push notifications** checkbox.
6. Click **Commit**.

Enabling or Disabling Push Notifications for Windows Phone by Using Windows PowerShell Cmdlets

You can enable or disable push notifications for Windows Phone by using the **Set-CsPushNotificationConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To enable push notifications for Windows Phone

- To enable push notifications for Windows Phone set the value of the EnableMicrosoftPushNotificationService property to True ($True). For example:

```
Set-CsPushNotificationConfiguration -Identity "site:Redmond" -EnableMic
```

⊟To disable push notifications for Windows Phone

- To disable push notifications for Windows Phone set the value of the

EnableMicrosoftPushNotificationService property to False ($False). For example:

```
Set-CsPushNotificationConfiguration -Identity "site:Redmond" -EnableMic
```

For more information, see the help topic for the Set-CsPushNotificationConfiguration cmdlet.

See Also

Tasks

Configuring for Push Notifications

1.7.10.3.2.3 Viewing Information about Push Notification Settings

Viewing Information about Push Notification Settings

See Also

Managing Devices, Phones, and Client Applications > Mobile Phones (Policy/Push Notification) > Push Notifications >

Topic Last Modified: *2013-02-23*

Push notifications, in the form of badges, icons, or alerts, can be sent to a mobile device even when the mobile application is inactive. Push notifications notify a user of events such as a new or missed IM invitation and voice mail. You can view information push notifications settings for mobile devices by using either Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

To view push notification information from Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Push Notification Configuration** navigation button.
4. On the **Push Notification Configuration** page, click the site you want to view, click the **Edit** menu, and then click **Show details**.

Viewing Push Notification Information by Using Windows PowerShell Cmdlets

You can view push notification configuration settings by using Windows PowerShell and the **Get-CsPushNotificationConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view push notification configuration information

- To view information about all your push notification configuration settings, type the following command in the Lync Server Management Shell and then press ENTER:

```
Get-CsPushNotificationConfiguration
```

That will return information similar to this:

```
Identity                                : Global
EnableApplePushNotificationService      : False
EnableMicrosoftPushNotificationService : False
```

For more information, see the help topic for the Get-CsPushNotificationConfiguration cmdlet.

See Also

Tasks

Configuring for Push Notifications

1.7.10.4 Test Devices

Test Devices

Microsoft Lync Server 2013 > Operations > Managing Devices, Phones, and Client Applications >

Topic Last Modified: *2012-10-15*

You can test devices from the **Test Device** page of the **Clients** section in Lync Server 2013 Control Panel.

- Create a Device to Test Update Functionality

1.7.10.4.1 Create a Device to Test Update Functionality

Create a Device to Test Update Functionality

Operations > Managing Devices, Phones, and Client Applications > Test Devices >

Topic Last Modified: *2013-02-23*

You can add a test device to the **Test Device** page and then use this device to verify the functionality of new updates before deploying the updates to production devices. You can test a device globally (throughout your entire Lync Server environment) or within a single site. You identify a test device by its Media Access Control (MAC) address or serial number. When you add a device, it appears in the list on the **Test Device** page of the Lync Server Control Panel.

To add a test device

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Clients**, and then click **Test Device**.
3. Click **New**, and then click either **Global test device** or **Site test device**.
4. Do one of the following:
   - If you clicked **Global test device**, skip to the next step.
   - If you clicked **Site test device**, select a site from the list of available sites, and then click **OK**.
5. In **New Test Device**, type a name for the device in **Device name**.
6. Under **Identifier type**, click either **MAC address** or **Serial number**.
7. In the **Unique identifier** box, type the MAC address or serial number of the device.
8. Click **Commit**.

Creating Test Devices by Using Windows PowerShell Cmdlets

Test devices can be created by using Windows PowerShell and the New-CsTestDevice cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

When creating test devices using this cmdlet, you must do two things:

- Specify either MACAddress or SerialNumber as the IdentifierType.
- Include the scope when specifying the device Identity. To create a new device at the global scope use syntax similar to this:

  ```
  -Identity "global/WindowsPhone"
  ```

  To create a test device at the site scope use syntax similar to this:

  ```
  -Identity "site:Redmond/WindowsPhone"
  ```

To create a test device by using the MAC address

- This command creates a test device at the global scope, and using the MAC address as the IdentifierType:

  ```
  New-CsTestDevice -Identity "global/WindowsPhone" -IdentifierType "MACAd
  ```

To create a test device by using the serial number

- This command creates a new test device at the site scope (for the Redmond site) and uses the serial number as the IdentifierType:

  ```
  New-CsTestDevice -Identity "site:Redmond/WindowsPhone" -IdentifierType
  ```

For more information, see the help topic for the New-CsTestDevice cmdlet.

1.7.10.5 Lync Phone Edition Configuration Settings

Lync Phone Edition Configuration Settings

Microsoft Lync Server 2013 > Operations > Managing Devices, Phones, and Client Applications >

Topic Last Modified: *2012-10-10*

Configuration settings for devices running Lync Phone Edition apply globally, or you can create new collections of settings that apply to a particular site. Collections include SIP security, device lock settings, and more.

- View Lync Phone Edition Configuration Settings Information
- Create or Modify a Collection of Lync Phone Edition Configuration Settings
- Delete an Existing Collection of Lync Phone Edition Configuration Settings
- Configure Security Settings for Lync Phone Edition
- Enforce Phone Locking

1.7.10.5.1 View Lync Phone Edition Configuration Settings Information

View Lync Phone Edition Configuration Settings Information

See Also

Operations > Managing Devices, Phones, and Client Applications > Lync Phone Edition Configuration Settings >

Topic Last Modified: *2013-02-23*

You can view configuration information about devices running Lync Phone Edition. The information is organized into collections. When you install Lync Server, you get a collection of Lync Phone Edition settings that apply to all the devices running Lync Phone Edition in your deployment. You can also create new collections of settings for a specific site. Site settings take precedence over global settings. Each collection of settings consists of a name, the scope (global or site), SIP security setting, logging level, voice quality of service (QoS) level, phone-lock setting, and phone-lock details, that is, the minimum length of the unlock personal identification number (PIN) and time before the phone locks itself.

⊟To view configuration information about devices running Lync Phone Edition

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Device Configuration** navigation button.
4. On the **Device Configuration** page, click the collection of settings you want to view information about. The name, scope, SIP security setting, voice quality level, and phone lock setting are listed on the main page. To view the logging level and phone lock details, click the **Edit** menu, and then click **Show details**.

Viewing Lync Phone Edition Configuration Information by Using Windows PowerShell Cmdlets

You can view Lync Phone Edition configuration settings by using Lync Server Management Shell and the **Get-CsUCPhoneConfiguration** cmdlet. You can run this cmdlet can from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To view Lync Phone Edition configuration information

- To view information about all your Lync Phone Edition configuration settings, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsUCPhoneConfiguration
  ```

  The command returns information similar to the following:

  ```
  Identity              : Global
  CalendarPollInterval  : 00:03:00
  EnforcePhoneLock      : True
  ```

```
PhoneLockTimeout      : 00:10:00
MinPhonePinLength     : 6
SIPSecurityMode       : High
VoiceDiffServTag      : 40
Voice8021p            : 0
LoggingLevel          : Off
```

For details, see Get-CsUCPhoneConfiguration.

See Also

Tasks

Create or Modify a Collection of Lync Phone Edition Configuration Settings
Delete an Existing Collection of Lync Phone Edition Configuration Settings
Configure Security Settings for Lync Phone Edition
Enforce Phone Locking

1.7.10.5.2 Create or Modify a Collection of Lync Phone Edition Configuration Settings

Create or Modify a Collection of Lync Phone Edition Configuration Settings

See Also

Operations > Managing Devices, Phones, and Client Applications > Lync Phone Edition Configuration Settings >

Topic Last Modified: *2013-02-23*

When you install Lync Server, you get a global collection of Lync Phone Edition settings. These settings apply to all devices running Lync Phone Edition in your deployment. You can change these settings at any time. You can also set up a new collection of settings that apply to the devices in a specific site. Site settings take precedence over global settings.

Configuration settings consist of the collection name, scope (global or site), SIP security setting, logging level, voice quality of service (QoS) level, phone-lock setting, and phone-lock details, that is, how long the a) unlock personal identification number (PIN) must be and b) phone stays idle before locking itself.

To create a collection of Lync Phone Edition configuration settings or edit settings for an existing collection

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Device Configuration** navigation button.
4. On the **Device Configuration** page, do one of the following:
   - To create a new collection of Lync Phone Edition configuration settings, click **New**, select a site, click **OK**, review the default settings, and, if you want to, make any changes.
   - To edit any of the settings in an existing collection, click the collection, click the **Edit** menu, click **Show details**, and then make your changes.

> **Tip:**
> To go back to using the default settings for the global collection, click the global collection, click the **Edit** menu, click **Delete**, and

then click **OK**. This will not delete the global collection; it just resets the settings to the defaults.

5. Click **Commit**.

Creating New Lync Phone Edition Configuration Settings by Using Windows PowerShell Cmdlets

You can create Lync Phone Edition configuration settings can (at the site scope only) by using Windows PowerShell and the **New-CsUCPhoneConfiguration** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To create new Lync Phone Edition configuration settings that use the default values

- This command creates a new set of UC phone configuration settings for the Redmond site:

  ```
  New-CsUCPhoneConfiguration -Identity "site:Redmond"
  ```

  Because no parameters (other than the mandatory Identity parameter) were specified in the preceding command, the new collection of configuration settings will use the default values for all its properties.

⊟To change a single property value when creating new Lync Phone Edition configuration settings

- To create settings that use different property values, simply include the appropriate parameter and parameter value. For example, to create a collection of UC phone configuration settings that, by default, require phone locking, use a command like this:

  ```
  New-CsUCPhoneConfiguration -Identity "site:Redmond" -EnforcePhoneLock $
  ```

⊟To change multiple property values when creating new Lync Phone Edition configuration settings

- Multiple property values can be modified by including multiple parameters. For example, this command enforces phone locking and also sets the minimum PIN length to 8 digits:

  ```
  New-CsUCPhoneConfiguration -Identity "site:Redmond" -EnforcePhoneLock $
  ```

For details, see New-CsUCPhoneConfiguration.

⊟See Also

Tasks

Delete an Existing Collection of Lync Phone Edition Configuration Settings
Configure Security Settings for Lync Phone Edition
Enforce Phone Locking

1.7.10.5.3 Delete an Existing Collection of Lync Phone Edition Configuration Settings

Delete an Existing Collection of Lync Phone Edition Configuration Settings

Operations > Managing Devices, Phones, and Client Applications > Lync Phone Edition Configuration Settings >

Topic Last Modified: *2013-02-23*

If you no longer want to use a collection of settings for devices running Lync Phone Edition, delete it. If you delete a collection for a site, the global settings will apply to the phones in that site. You cannot delete the global collection.

Note:

Instead of deleting a collection, you might just want to change some of the settings. For details about how to do so, see Create or Modify a Collection of Lync Phone Edition Configuration Settings.

⊟To delete a collection of Lync Phone Edition configuration settings

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Device Configuration** navigation button.
4. On the **Device Configuration** page, click the collection you want to delete, click the **Edit** menu, and then click **Delete**.

   Note:

   If you delete the global collection, the settings just revert to the default settings. The collection does not go away.
5. In the confirmation box, click **OK**.

Removing Lync Phone Edition Configuration Settings by Using Windows PowerShell Cmdlets

You can delete Lync Phone Edition configuration settings by using Windows PowerShell and the **Remove-CsUCConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To remove a specified collection of Lync Phone Edition configuration settings

- This command deletes the UC phone configuration settings applied to the Redmond site:

```
Remove-CsUCPhoneConfiguration -Identity "site:Redmond"
```

⊟To remove all of the Lync Phone Edition configuration settings applied to the site scope

- This command removes all the UC phone configuration settings applied to the service scope:

```
Get-CsUCPhoneConfiguration -Filter "site:*" | Remove-CsUCPhoneConfigura
```

⊟To remove all of the Lync Phone Edition configuration settings where phone locking is disabled

- This command deletes any collection of UC phone configuration settings where phone locking has been disabled:

```
Get-CsUCPhoneConfiguration | Where-Object {$_.EnforcePhoneLock -eq $Fal
```

For details, see Remove-CsUCPhoneConfiguration.

1.7.10.5.4 Configure Security Settings for Lync Phone Edition

Configure Security Settings for Lync Phone Edition

See Also

Operations > Managing Devices, Phones, and Client Applications > Lync Phone Edition Configuration Settings >

Topic Last Modified: *2013-02-23*

Help improve the security of devices running Lync Phone Edition via your SIP security setting and phone lock settings.

⊟To configure security settings for Lync Phone Edition

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click **Device Configuration**.
4. On the **Device Configuration** page, in the list of device configurations, double-click the configuration for which you want to change security settings.
5. In **Edit Device Configuration**, in **SIP security**, specify the SIP security level. The default level is **High**, which we recommend using.
6. In **Edit Device Configuration**, under **Phone Lock**, select or clear the **Enforce device locking** check box (selected by default) and specify the minimum PIN length (6 characters by default) and timeout period (10 minutes by default). We recommend using these defaults or increasing the PIN length and/or decreasing the timeout period.

Note:
For details, see Enforce Phone Locking.

Configuring Security Settings for Lync Phone Edition Phones by Using Windows PowerShell Cmdlets

Security settings can be managed by using Lync Server Management Shell and the **Get-CsUCPhoneConfiguration** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using

Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To modify the SIP security mode

- This command sets the SIPSecurityMode for the global collection of UC phone settings to Medium. SIP security could also be set to Low or High (the default value).

```
Set-CsUCPhoneConfiguration -Identity global -SIPSecurityMode "Medium"
```

To modify the minimum PIN length

- In this example, all the UC phone settings are modified to require a minimum PIN length of 7 digits.

```
Get-CsUCPhoneConfiguration | Set-CsUCPhoneConfiguration -MinPhonePinLen
```

For details, see Get-CsUCPhoneConfiguration.

See Also

Concepts

Managing Lync Server 2013 Security and Authentication

Other Resources

Managing Devices, Phones, and Client Applications

1.7.10.5.5 Enforce Phone Locking

Enforce Phone Locking

See Also

Managing Devices, Phones, and Client Applications > Mobile Phones (Policy/Push Notification) > Mobility Policies >

Topic Last Modified: *2013-02-23*

Lync Phone Edition devices can be locked for security purposes. If you enforce phone lock, the device running Lync Phone Edition locks after a period of time that you configure. When a phone is locked, a user can make calls but cannot access calendar and contact information, voice mail, or call logs or use search. To unlock the phone, the user enters a PIN.

To enforce phone lock, enable and configure it by using Lync Server Control Panel or Lync Server PowerShell cmdlets. You can enforce phone lock globally or only within the site for which it is configured.

To configure and enforce the phone lock

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. Click **Clients**, and then click **Device Configuration**.
4. On the **Device Configuration** tab, in the list of device configurations, double-click the configuration for which you want to change the phone lock settings.
5. In the **Edit Device Configuration** dialog box, verify that the **Enforce device locking** check box is selected.
6. In **Minimum PIN length**, accept the default value for the minimum number of digits that the unlock PIN must contain or specify a new value. The range for the PIN length is four to 15 digits, and the default is six.

7. In **Phone lock time-out**, accept the default value for the minimum length of time before the phone locks itself or specify a new value. The range for the timeout is 0 to 60 minutes, and the default is 10. Enter the value in the format HH:MM:SS.
8. Click **Commit**.

Enforcing Phone Locking by Using Windows PowerShell Cmdlets

Phone locking can be enforced by using the Set-CsUCPhoneConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable phone locking

- The following command enables phone locking for the Redmond site. To disable phone locking, set the EnforcePhoneLock property to False ($False).

```
Set-CsUCPhoneConfiguration -Identity" site:Redmond" -EnforcePhoneLock $
```

To enable phone locking and modify the phone lock timeout

- This command enables phone locking and also sets the phone lock timeout to 30 minutes.

```
Set-CsUCPhoneConfiguration -Identity" site:Redmond" -EnforcePhoneLock $
```

To enable phone locking throughout the organization

- In this example, phone locking is enabled on all the UC phone configuration settings in use in the organization.

```
Get-CsUCPhoneConfiguration | Set-CsUCPhoneConfiguration  -EnforcePhoneL
```

For more information, see the help topic for the Set-CsUCPhoneConfiguration cmdlet.

See Also

Concepts

Managing Lync Server 2013 Security and Authentication

Other Resources

Managing Devices, Phones, and Client Applications

1.7.10.6 Device Update Web Service

Device Update Web Service

See Also

Microsoft Lync Server 2013 > Operations > Managing Devices, Phones, and Client Applications >

Topic Last Modified: *2013-02-20*

Lync Server includes the Device Update Web service, which is automatically installed as part of the Web Services role. This service lets you download updates from Microsoft, test them, and then deploy the updates to IP phones in your organization. You can also use Device Update Web service to roll back devices to previous software versions.

This section provides details about how to manage the Device Update Web service and deployed updates by using device update logs, rules (Lync Phone Edition uses *rules* to associate firmware version updates with hardware devices), and configuration settings.

For details about the Device Update Web service process and features, see Updating Devices in the Lync Server 2010 TechNet Library. (Note that the Device Update Web service, like all Lync Phone Edition components, works the same way with Lync Server 2013 as it does with Lync Server 2010.)

- Device Update Logs and Files
- Device Update Rules
- Device Update Configuration Settings
- View Software Updates for Devices in Your Organization

⊟See Also

Other Resources

Tools and Services for Managing and Troubleshooting Devices

1.7.10.6.1 Device Update Logs and Files

Device Update Logs and Files

Operations > Managing Devices, Phones, and Client Applications > Device Update Web Service >

Topic Last Modified: *2013-02-20*

Device update logs contain important information that you can use to manage and troubleshoot the Device Update Web service. You can change what is logged and remove device logs and updates that you don’t want or no longer need. This section describes how you can use Lync Server Control Panel or Lync Server Management Shell to modify logging settings, clear the device update log, or remove log files from the server.

Note:
For details about device update log files, see Log File Types and Locations in the Lync Server 2010 TechNet Library. (Note that the Device Update Web service, like all Lync Phone Edition components, works the same way with Lync Server 2013 as it does with Lync Server 2010.)

⊟In This Section

- Modify Settings for Device Update Log Files
- Delete Device Update Log Files
- Remove Device Update Files Not Associated With a Device

1.7.10.6.1.1 Modify Settings for Device Update Log Files

Modify Settings for Device Update Log Files

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Logs and Files >

Topic Last Modified: *2013-02-23*

You can change settings for how device update information is logged in your organization by using Lync Server Control Panel or Lync Server Management Shell. The following table shows which settings are modifiable, and which tool(s) you use to modify the settings.

Log settings can be changed and applied globally, or per site.

To change	Use
The maximum size (in bytes) for a log file	Lync Server Control Panel -or- Lync Server Management Shell
The maximum amount of information (in bytes) that can be held in the cache	Lync Server Control Panel -or- Lync Server Management Shell
How often (in minutes) to write cached information to the log file	Lync Server Control Panel -or- Lync Server Management Shell
How long (in days) to keep log files	Lync Server Control Panel -or- Lync Server Management Shell
When (time of day) to check for expired files that should be deleted	Lync Server Management Shell
What log file extensions to permit	Lync Server Management Shell
Which log file types to retain	Lync Server Management Shell

To change logging settings by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Clients**, and then click **Device Log Configuration**.
3. On the **Device Log Configuration** page, double-click the configuration that you want to change.
4. In the **Edit Log Setting** dialog box, change any of the following settings:
   - **Maximum file size (bytes)** Specifies the maximum size a log file can become before it is purged. The default is 1,024,000 bytes (1 MB).
   - **Maximum cache size (bytes)** Specifies the maximum amount of information (in bytes) that can be held in the log file cache before that cache must be cleared and the data is written to a log file. The default is 512,000 bytes (0.5 MB).
   - **Number of minutes to flush cache (1-60)** Indicates how often information stored in the log file cache is written to the actual log file. After the data is logged, the cache is cleared. The default is five minutes.
   - **Number of days to keep log files (1-365)** Specifies the number of days the log files are kept before they are purged. The default is 10 days.
5. Click **Commit**.

Changing Logging Settings by Using Windows PowerShell Cmdlets

Device update log file settings can be modified by using Windows PowerShell and the

Set-CsDeviceUpdateConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

> **Note:**
> For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

The following examples show a couple of the ways that you can use **Set-CsDeviceUpdateConfiguration** to modify settings.

To modify the maximum log file size and the log cleanup interval

- The following command modifies the device update log settings applied to the Redmond site. In this example, the maximum log file size is set to 204800 bytes and the log cleanup interval is set to 14 days.

```
Set-CsDeviceUpdateConfiguration -Identity "site:Redmond" -MaxLogFileSiz
```

To modify the log cleanup time of day

- This command sets the log cleanup time for the Redmond site to 3:00 AM.

```
Set-CsDeviceUpdateConfiguration -Identity "site:Redmond" -LogCleanupTim
```

For details, see the Help topic for the Set-CsDeviceUpdateConfiguration cmdlet.

1.7.10.6.1.2 Delete Device Update Log Files

Delete Device Update Log Files

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Logs and Files >

Topic Last Modified: *2013-02-23*

The Device Update Web service keeps an extensive collection of log files. This collection includes both audit logs conducted by the service itself and log files uploaded from client devices. To prevent the server from filling up with Device Update Web service service logs, you'll probably want to clear it of log files that have been around for a certain number of days. Set this number of days based on update activity and the number of client devices in your organization, and by using Lync Server Control Panel or Lync Server Management Shell.

To clear the device update log by using Lync Server Control Panel

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Clients**, and then click **Device Log Configuration**.
3. On the **Device Log Configuration** page, double-click the configuration that you want to change.
4. In the **Edit Log Setting** dialog box, in **Number of days to keep log files (1-365)**, specifiy a number of days.
5. Click **Commit**. All files that have been on the server for more than the specified number of day are deleted. This setting will apply to this configuration until you change it.

Clearing the Device Update Log by Using the Windows PowerShell Cmdlets

You can clear device update logs by using Windows PowerShell and the **Clear-CsDeviceUpdateLog** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:
For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To clear device update logs on one server

- The following command clears the device update log on the Web server atl-cs-001.litwareinc.com. All log entries more than 10 days old (the value specified by the DaysBack parameter) will be removed from the log.

```
Clear-CsDeviceUpdateLog -Identity "service:WebServer:atl-cs-001.litware
```

To clear all device update logs

- This command removes outdated entries (in this example, entries more than 10 days old) from all the device update logs currently in use in your organization.

```
Get-CsService -WebServer | Foreach-Object {Clear-CsDeviceUpdateLog -Ide
```

For details, see the Help topic for the Clear-CsDeviceUpdateLog cmdlet.

1.7.10.6.1.3 Remove Device Update Files Not Associated With a Device

Remove Device Update Files Not Associated With a Device

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Logs and Files >

Topic Last Modified: *2013-02-20*

Each time new device updates are uploaded to the system, a corresponding device update rule is created. By default, these new device update rules are assigned to the Pending state. This means that the rules can be downloaded and installed on test devices, but not on production devices, which enables you to test the updates before making them available to users. Based on the tests, you either accept and deploy or reject and delete the update. When you reject an update, the device update is disassociated from its device update rule.

Device update files that are no longer associated with a device can be removed by using Windows PowerShell and the **Clear-CsDeviceUpdateFile** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:
For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

- For example, the following command removes any device update rules on the Web server atl-cs-001.litwareinc.com that are no longer associated with a device:

```
Clear-CsDeviceUpdateFile -Identity "service:WebServer:atl-cs-001.litwar
```

For details, see the Help topic for the Clear-CsDeviceUpdateFile cmdlet.

1.7.10.6.2 Device Update Rules

Device Update Rules

Operations > Managing Devices, Phones, and Client Applications > Device Update Web Service >

Topic Last Modified: *2013-02-20*

Periodically, Microsoft releases a new set of device firmware updates for Lync Phone Edition. *Device update rules* associate firmware updates with hardware devices—phones and other devices running Lync Phone Edition.

To get the latest set of device update rules, go to the Help and Support page on the Microsoft website, and search for "Phone Edition." Download the update package, and extract the files to a folder on the computer where the updates are to be uploaded. After the files have been extracted, import the device update rules found in the extracted .CAB file (which have the name UCUpdates.cab). Then, use the Lync Server Control Panel or Windows PowerShell cmdlets to view and manage these rules for your organization's devices.

The following topics tell you how to import, view, and manage device update rules.

- View Information about Device Update Rules
- Import Device Update Rules
- Approve a Device Update Rule
- Remove a Device Update Rule
- Reset a Device Update Rule
- Restore a Device Update Rule

1.7.10.6.2.1 View Information about Device Update Rules

View Information about Device Update Rules

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Rules >

Topic Last Modified: *2013-02-23*

View details about device update rules that have already been imported, including the type, model, and brand of devices the update applies to; version and type of update; and locale and pool for the update. Information is available for all imported device update rules—those that are pending approval, deployed (approved), recalled (restored), and those you've decided not to use (reset). Access this information from either Lync Server Control Panel or Windows PowerShell.

Note:

For details about how to import, approve, reset, restore, and remove rules, see the topics listed at Device Update Rules.

To view device update rules by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Device Update** navigation button. Imported rules are listed on the **Device Update** page.

Viewing Device Update Rules by Using Windows PowerShell Cmdlets

Detailed information about all your device update rules can also be viewed by using Windows PowerShell and the **Get-CsDeviceUpdateRule** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:

For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view all your device update rules

- The following command returns information about all the device updates rules configured for use in your organization:

  ```
  Get-CsDeviceUpdateRule
  ```

  The command returns information similar to the following for each of your device update rules:

  ```
  Identity        : Service:WebServer:pool0.vdomain.com/2de8cbf6-9441-4f6
  Id              : 2de8cbf6-9441-4f61-b755-1e4bef1effde
  DeviceType      : UCPhone
  Brand           : Microsoft
  Model           : CPE
  Revision        : A
  Locale          : ENU
  UpdateType      : CPE
  ApprovedVersion :
  RestoreVersion  :
  PendingVersion  : 4.0.7577.4066
  ```

To view all the device update rules on a specific web server

- To view the device update rules on a specific computer, use the Filter parameter followed by the server Identity and the wildcard character (*). For example:

  ```
  Get-CsDeviceUpdateRule -Filter "service:WebServer:atl-cs-001.litwareinc
  ```

For details, see the Help topic for the Get-CsDeviceUpdateRule cmdlet.

1.7.10.6.2.2 Import Device Update Rules

Import Device Update Rules

See Also

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Rules >

Topic Last Modified: *2013-02-23*

Device update rules can be imported only by using Windows PowerShell and the **Import-CsDeviceUpdate** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:

For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To import device update rules to a single web server

- The following command imports device update rules to the Web server atl-cs-001.litwareinc.com:

```
Import-CsDeviceUpdate -Identity "service:WebServer:atl-cs-001.litwarein
```

To import device update rules to all your web servers

- In this example, device update rules are imported to all the Web servers deployed in your organization. For this command to work, the folder \\atl-fs-001.litwareinc.com\Updates must be shared and available to all the Web servers.

```
Get-CsService -WebServer | ForEach-Object {Import-CsDeviceUpdate -Ident
```

For details, see the Help topic for the Import-CsDeviceUpdate cmdlet.

See Also

Tasks

View Information about Device Update Rules

Approve a Device Update Rule

1.7.10.6.2.3 Approve a Device Update Rule

Approve a Device Update Rule

See Also

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Rules >

Topic Last Modified: *2013-02-23*

After you import a device update rule, it’s installed on your test devices. If your testing is successful, and you want to roll out the update to your organization, approve it by using either Lync Server Control Panel or Windows PowerShell.

To approve a device update rule by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. On the **Device Update** page, do one of the following:
   - To approve one rule, select that rule.
   - To approve all rules, click **Edit**, and then click **Select All**.
4. Click **Action**, and then click **Approve**.

Approving a Device Update Rule by Using Windows PowerShell Cmdlets

Device update rules can also be approved by using Windows PowerShell and the **Approve-CsDeviceUpdateRule** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:

For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To approve a single device update rule

- The following command approves the device update rule d5ce3c10-2588-420a-82ac-dc2d9b1222ff9 found on the Web server atl-cs-001.litwareinc.com:

```
Approve-CsDeviceUpdateRule -Identity service:WebServer:atl-cs-001.litwa
```

To approve multiple device update rules

- This command approves all the device update rules for Microsoft-branded devices:

```
Get-CsDeviceUpdateRule | Where-Object {$_.Brand -eq "Microsoft"} | Appr
```

For details, see the Help topic for the Approve-CsDeviceUpdateRule cmdlet.

See Also

Tasks

Import Device Update Rules
Restore a Device Update Rule

1.7.10.6.2.4 Remove a Device Update Rule

Remove a Device Update Rule

See Also

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Rules >

***Topic Last Modified:** 2013-02-23*

Removing a device update rule takes it permanently out of the device update queue.

Removing a rule is different from uninstalling an update from the devices in your deployment or from your test devices. To uninstall an approved update from your deployment, you *restore* the device update rule. For details, see Restore a Device Update Rule. To uninstall an update you haven’t approved from your test devices, you *reset* it. For details, see Reset a Device Update Rule.

You can remove a device update rule by using either Lync Server Control Panel or Windows PowerShell.

To remove device update rules by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Device Update** navigation button.
4. On the **Device Update** page, do one of the following:
   - To remove one rule, select the rule you want to delete.
   - To remove all rules, click the **Edit** menu, and then click **Select All**.
5. Click **Edit**, and then click **Delete**.

Removing Device Update Rules by Using Windows PowerShell Cmdlets

Device update rules can also be removed by using Windows PowerShell and the **Remove-CsDeviceUpdateRule** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a single device update rule from a server

- The following command removes the device update rule d5ce3c10-2588-420a-82ac-dc2d9b1222ff9 from the Web server on atl-cs-001.litwareinc.com.

```
Remove-CsDeviceUpdateRule -Identity "service:WebServer:atl-cs-001.litwa
```

To remove all the device update rules from a server

- This command removes all the device update rules from the web server on atl-cs-001.litwareinc.com.

```
Get-CsDeviceUpdateRule -Filter "service:WebServer:atl-cs-001.litwareinc
```

For details, see the Help topic for the Remove-CsDeviceUpdateRule cmdlet.

See Also

Tasks

Approve a Device Update Rule

1.7.10.6.2.5 Reset a Device Update Rule

Reset a Device Update Rule

See Also

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Rules >

Topic Last Modified: *2013-02-23*

If you don’t like the way that an update works on your test devices, you can reset the device update rule, which removes the rule's pending status and uninstalls the update from the test devices.

You can remove a device update rule by using either Lync Server Control Panel or Windows PowerShell.

Note:
To uninstall a rule that you've already approved (that is, rolled out), restore it. For details, see Restore a Device Update Rule.

To reset a device update rule by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Device Update** navigation button.
4. On the **Device Update** page, do one of the following:
   - To reset one rule, select the rule you want to reset.
   - To reset all rules, on the **Edit** menu, click **Select All**.
   - To reset all rules for one brand, use the **Brand** column menu.
5. Click **Action**, and then click **Cancel pending updates**.

Tip:
If you're sure you'll never want to roll out the device update rule(s) that you cancelled, you might want to delete them. For details, see Remove a Device Update Rule.

Resetting a Device Update Rule by Using Windows PowerShell Cmdlets

Device update rules can also be reset by using Windows PowerShell and the **Reset-CsDeviceUpdateRule** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:
For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To reset a specific device update rule on a server

- The following command resets the device update rule d5ce3c10-2588-420a-82ac-dc2d9b1222ff9 on the Web server atl-cs-001.litwareinc.com:

```
Reset-CsDeviceUpdateRule -Identity "service:WebServer:atl-cs-001.litwar
```

To reset all the device update rules on a server

- This command resets all the device update rules on the Web server atl-cs-001.litwareinc.com:

```
Get-CsDeviceUpdateRule -Filter "service:WebServer:atl-cs-001.litwareinc
```

To reset all the device updates rules that have a specific brand

- In this example, all the device updates throughout the organization that have a Brand equal to Microsoft are reset:

```
Get-CsDeviceUpdateRule | Where-Object {$_.Brand -eq "Microsoft"} | Rese
```

For details, see the Help topic for the Reset-CsDeviceUpdateRule cmdlet.

See Also

Tasks

Approve a Device Update Rule

1.7.10.6.2.6 Restore a Device Update Rule

Restore a Device Update Rule

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Rules >

Topic Last Modified: *2013-02-23*

To uninstall a device update rule from the devices in your deployment, restore it. Restoring a device update rule both uninstalls the update and reinstalls the previous version of that rule.

You can restore a device update rule by using either Lync Server Control Panel or Windows PowerShell.

To restore device update rules by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Device Update** navigation button.
4. On the **Device Update** page, do one of the following:
   - To restore one rule, select that rule.
   - To restore all rules, click **Edit**, and then click **Select All**.
5. Click the **Action** menu, and then click **Restore**.

Restoring Device Update Rules by Using Windows PowerShell Cmdlets

Device updates rules can also be restored by using Windows PowerShell and the **Restore-CsDeviceUpdateRule** cmdlet.. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:

For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To restore a single device update rule on a server

- The following command restores the device update rule d5ce3c10-2588-420a-82ac-dc2d9b1222ff9 on the Web server atl-cs-001.litwareinc.com:

```
Restore-CsDeviceUpdateRule -Identity "service:WebServer:atl-cs-001.litw
```

To restore all the device update rules on a server

- This command restores all the device update rules on the web server atl-cs-001.litwareinc.com:

  ```
  Get-CsDeviceUpdateRule -Filter "service:WebServer:atl-cs-001.litwareinc
  ```

For details, see the Help topic for the Restore-CsDeviceUpdateRule cmdlet.

1.7.10.6.3 Device Update Configuration Settings

Device Update Configuration Settings

Operations > Managing Devices, Phones, and Client Applications > Device Update Web Service >

Topic Last Modified: *2013-02-20*

The Device Update Web service is managed by using device configuration settings. These settings can be applied at the global scope or at the site scope.

- View Device Update Configuration Settings
- Create or Modify a Collection of Device Update Configuration Settings
- Delete a Collection of Device Update Configuration Settings

1.7.10.6.3.1 View Device Update Configuration Settings

View Device Update Configuration Settings

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Configuration Settings >

Topic Last Modified: *2013-02-20*

You can view the Device Update Service configuration settings by using Lync Server Management Shell and the **Get-CsDeviceUpdateConfiguration** cmdlet, which you can run from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell

Note:

For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

- To view information about all your voice routes, type the following command in the Lync Server Management Shell and press Enter:

  ```
  Get-CsDeviceUpdateConfiguration
  ```

  This command returns information similar to the following:

  ```
  Identity               : Global
  ValidLogFileTypes      : {Watson, Config, Diaglog, CELog}
  ValidLogFileExtensions : {.dmp, .clg, .clg1, .clg2...}
  MaxLogFileSize         : 1024000
  MaxLogCacheLimit       : 512000
  LogCleanUpInterval     : 10.00:00:00
  LogFlushInterval       : 00:05:00
  LogCleanUpTimeOfDay    :
  ```

For details about this cmdlet, see Help topic at Get-CsDeviceUpdateConfiguration.

1.7.10.6.3.2 Create or Modify a Collection of Device Update Configuration Settings

Create or Modify a Collection of Device Update Configuration Settings

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Configuration Settings >

Topic Last Modified: *2013-02-23*

Device update configuration settings can be created (at the site scope only) by using Windows PowerShell and the **New-CsDeviceUpdateConfiguration** cmdlet and modified by using the **Set-CsDeviceUpdateConfiguration** cmdlet. These cmdlets can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell.

Note:
For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To create device update configuration settings that use the default values

- This command creates a new set of device update configuration settings for the Redmond site:

  ```
  New-CsDeviceUpdateConfiguration -Identity "site:Redmond"
  ```

  Because no parameters other than the mandatory Identity parameter were specified in the preceding command, the new collection of configuration settings will use the default values for all its properties.

To change a single property value when creating device update configuration settings

- To create settings that use different property values, simply include the appropriate parameter and parameter value. For example, to create a collection of device update configuration settings that, by default, deletes old log files every 21 days, use a command like this one:

  ```
  New-CsDeviceUpdateConfiguration -Identity "site:Redmond" -LogCleanupInt
  ```

To change multiple property values when creating device update configuration settings

- Multiple property values can be modified by including multiple parameters. For example, this command sets the log cleanup interval to 21 days and the log flush interval to 30 minutes:

  ```
  New-CsDeviceUpdateConfiguration -Identity "site:Redmond" -LogCleanupInt
  ```

For details about modifying existing device configuration settings, see the Help topic for the Set-CsDeviceUpdateConfiguration cmdlet. For details about creating collections of configuration settings, see the Help topic for the New-CsDeviceUpdateConfiguration cmdlet.

1.7.10.6.3.3 Delete a Collection of Device Update Configuration Settings

Delete a Collection of Device Update Configuration Settings

Managing Devices, Phones, and Client Applications > Device Update Web Service > Device Update Configuration Settings >

***Topic Last Modified:** 2013-02-20*

Device update configuration settings can also be deleted by using Windows PowerShell and the **Remove-CsdeviceUpdateConfiguration** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To remove a specific collection of device update configuration settings

- This command deletes the device update configuration settings applied to the Redmond site:

```
Remove-CsDeviceUpdateConfiguration -Identity "site:Redmond"
```

⊟To remove all the device update configuration settings applied to the site scope

- This command deletes all the device update configuration settings applied to the site scope:

```
Get-CsDeviceUpdateConfiguration -Filter "site:*" | Remove-CsDeviceUpdat
```

⊟To remove device update configuration settings based on the value of the LogCleanUpInterval property

- The following command deletes all the device update configuration settings where the log cleanup interval is greater than 10 days (10.00:00:00):

```
Get-CsDeviceUpdateConfiguration | Where-Object {$_.LogCleanUpInterval -
```

For details, see the Help topic for the Remove-CsDeviceUpdateConfiguration cmdlet.

1.7.10.6.4 View Software Updates for Devices in Your Organization

View Software Updates for Devices in Your Organization

See Also

Operations > Managing Devices, Phones, and Client Applications > Device Update Web Service >

***Topic Last Modified:** 2012-11-01*

With Lync Server 2013, you use Device Update Web service to view and manage software updates for your organization’s devices. These updates are available in .cab (cabinet) files from the Microsoft Support website at http://go.microsoft.com/fwlink/p/?linkId=204091. After you download the .cab file, run the **Import-CSDeviceUpdate** cmdlet to import the device update rules from the .cab file. For details about the **Import-CSDeviceUpdate** cmdlet, see Import-CsDeviceUpdate in the Lync Server Management Shell documentation.

Tip:

Before deploying a new update to your organization, verify that it functions correctly on a test device.

To view software updates for UC devices

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. From the Microsoft Support website at http://go.microsoft.com/fwlink/p/?linkId=204091, download the .cab file to a location on a Lync Server 2013 computer (for example, C:\Updates\UCUpdates.cab).
3. Import the device update rules from the C:\Updates\UCUpdates.cab file by running one of the following cmdlets:
   - If the .cab file is located on the same computer as the one running the service to be updated (service:Redmond-websvc-2), run the following cmdlet:

     ```
     Import-CsDeviceUpdate -Identity service:Redmond-websvc-2 -Fi
     ```

   - If the .cab file is located on a different computer than the one running the service to be updated (service:Redmond-websvc-3), run the following cmdlet:

     ```
     Import-CsDeviceUpdate -Identity service:Redmond-websvc-3 -By
     ```

4. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
5. In the left navigation bar, click **Clients**, and then click **Device Update**.
6. On the **Device Update** page, click an update in the list, and then do one of the following:
   - **Cancel a pending update.** To prevent the selected update from being deployed to your organization’s devices, click the **Action** menu, and then click **Cancel pending updates**.
   - **Approve an update.** To allow the selected update to be deployed to your organization’s devices, click the **Action** menu, and then click **Approve**.
   - **Restore an update.** To allow a previously approved update to be deployed to your organization’s devices, click the **Action** menu, and then click **Restore**.

Other Resources

Managing Devices, Phones, and Client Applications

1.7.10.7 Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013

Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013

See Also

Microsoft Lync Server 2013 > Operations > Managing Devices, Phones, and Client Applications >

Topic Last Modified: *2012-12-11*

Lync Server 2013 enables you to specify the version of clients that are supported in your environment. Using client version policies can help reduce the costs associated with supporting multiple client versions. It can also improve the overall user experience, because when earlier and later versions of clients interact, the available features can be limited by the earlier version of the client.

There are three components of client version control:

- Client version configuration settings are used to turn client version control on or off, either globally or for particular sites.

- Client version policies are used to assign a set of rules globally, or to a particular site, pool, or group of users.
- Client version policy rules make up a client version policy, and are used to define the actions that should be taken when users attempt to log on with specific clients and client versions.

Note:
Because anonymous users are not associated with a user, site, or service, anonymous users are affected by global-level policies only.

In This Section

- Client Version Configuration Settings
- Client Version Policies
- Client Version Rules

See Also

Other Resources

Managing Devices, Phones, and Client Applications

1.7.10.7.1 Client Version Configuration Settings

Client Version Configuration Settings

Operations > Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 >

Topic Last Modified: *2012-12-12*

Client version configuration settings are used to turn client version control on or off, either globally or for particular sites. Use the following procedures to configure client version configuration settings for Lync Server 2013.

- Enable or Disable Client Versioning
- Create or Modify a Collection of Client Version Configuration Settings
- Modify the Default Action for Clients Not Explicitly Supported or Restricted
- View Client Version Configuration Settings
- Delete an Existing Collection of Client Version Configuration Settings

1.7.10.7.1.1 Enable or Disable Client Versioning

Enable or Disable Client Versioning

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Configuration Settings >

Topic Last Modified: *2013-02-23*

Client version configuration settings are used to turn client version control on or off, either globally or for particular sites. The global client version configuration installs with Lync Server 2013 and is used to enable or disable client version control for the entire server deployment. When the global configuration is enabled, any client version policies you have in place will take effect when users attempt to log on. You can disable the global client version configuration if you do not want any client version control to occur. You can enable or disable client versioning from Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

Note:
Because anonymous users are not associated with a user, site, or service, anonymous users are affected by global-level policies only.

To enable or disable client versioning by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Client Version Configuration** navigation button.
4. Do the following:
   - To globally enable or disable client versioning, double-click the **Global** configuration, and then modify the settings.
   - To enable or disable client versioning for a particular site, click **New**, select the site, click **OK**, and then modify the settings for the site.

Enabling or Disabling Client Versioning by Using Windows PowerShell Cmdlets

You can enable or disable client versioning by using the **Set-CsClientVersionConfiguration** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable client versioning

- You can enable client versioning by setting the **Enabled** property to True ($True).

```
Set-CsClientVersionConfiguration -Identity "site:Redmond" -Enabled $Tru
```

To disable client versioning

- You can disable client versioning by setting the **Enabled** property to False ($False).

```
Set-CsClientVersionConfiguration -Identity "site:Redmond" -Enabled $Tru
```

For details, see the Help topic for the Set-CsClientVersionConfiguration cmdlet.

1.7.10.7.1.2 Create or Modify a Collection of Client Version Configuration Settings

Create or Modify a Collection of Client Version Configuration Settings

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Configuration Settings >

Topic Last Modified: *2013-02-23*

Client version configuration settings are used to turn client version control on or off. The global client version configuration installs with Lync Server and is used to enable or disable client version control for the entire server deployment. You can also configure client version configuration settings for individual sites. You can create or modify client version configuration settings from Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

> **Note:**
> Because anonymous users are not associated with a user, site, or service, anonymous users are affected by global-level policies only.

To create or modify client version configuration settings by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Client Version Configuration** navigation button.
4. On the **Client Version Configuration** page, do the following:
   - To create a new configuration, click **New**, select a site, click **OK** name, and update the settings.
   - To modify a configuration, select the configuration, click **Edit**, click **Show details**, and make changes to the settings.

Creating or Modifying Client Version Configuration Settings by Using Windows PowerShell Cmdlets

You can create client version configuration settings by using the **New-CsClientVersionConfiguration** cmdlet, and modify them by using the **Set-CsClientVersionConfiguration** cmdlet. These cmdlets can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To create a new collection of client version configuration settings

- The following command creates a new collection of client version configuration settings applied to the Redmond site. In this example, client versioning is disabled for the Redmond site.

```
New-CsClientVersionConfiguration -Identity "site:Redmond" -Enabled $Fal
```

To enable client versioning for a site

- This command enables client versioning for the Redmond site.

```
Set-CsClientVersionConfiguration -Identity "site:Redmond" -Enabled $Tru
```

To disable client versioning throughout the organization

- In this example, client versioning is disabled for all the client version configuration settings in use in the organization.

```
Get-CsClientVersionConfiguration | Set-CsClientVersionConfiguration  -E
```

For details, see the Help topic for the New-CsClientVersionConfiguration and Set-

CsClientVersionConfiguration cmdlets.

1.7.10.7.1.3 Modify the Default Action for Clients Not Explicitly Supported or Restricted

Modify the Default Action for Clients Not Explicitly Supported or Restricted

See Also

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Configuration Settings >

Topic Last Modified: *2013-02-23*

In addition to specifying the version of clients that you want to support in your Lync Server 2013 environment, you can also specify a default action for clients that do not already have a version policy defined. This enables you to restrict which client versions are used in your Lync Server environment, which can help you control the costs associated with supporting multiple client versions.

⊟To modify the default action for clients not explicitly supported or restricted

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click **Client Version Configuration**.
4. On the **Client Version Configuration** page, double-click the **Global** configuration in the list.
5. In the **Edit Client Version Configuration** dialog box, verify that the **Enable version control** check box is selected and then, under **Default action**, select one of the following:
   - **Allow** Allows the client to log on if the client version does not match any filter in the **Client version policies** list.
   - **Block** Prevents the client from logging on if the client version does not match any filter in the **Client version policies** list.
   - **Block with URL** Prevents the client from logging on if the client version does not match any filter in the **Client version policies** list, and include an error message containing a URL where a newer client can be downloaded.
   - **Allow with URL** Allows the client to log on if the client version does not match any filter in the **Client version policies** list, and include an error message containing a URL where a newer client can be downloaded.
6. If you selected **Block with URL**, type the client download URL to include in the error message in the **URL** box.
7. Click **Commit**.

⊟To disable client version control

- To disable version control to allow all clients to log on regardless of the client version, clear the **Enable version control** check box, and then click **Commit**.

Modifying the Default Action by Using Windows PowerShell Cmdlets

The default action to be taken when users try to sign on using clients that are not explicitly supported or restricted by a client version policy can be managed by using Windows PowerShell command-line interface and the **Set-CsClientVersionPolicy** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To configure the default action to block access

- The following command sets the default action for the Redmond site Block. This will block registration for any client for which no client version configuration rule exists.

```
Set-CsClientVersionConfiguration -Identity "site:Redmond" -DefaultActio
```

To configure the default action to allow access

- In this example, the default action for the Redmond site is set to Allow. This will allow registration for any client for which no client version configuration rule exists.

```
Set-CsClientVersionConfiguration -Identity "site:Redmond" -DefaultActio
```

For details, see the Help topic for the Set-CsClientVersionPolicy cmdlet.

See Also

Other Resources

Managing Devices, Phones, and Client Applications

1.7.10.7.1.4 View Client Version Configuration Settings

View Client Version Configuration Settings

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Configuration Settings >

Topic Last Modified: *2013-02-23*

Client version configuration settings are used to turn client version control on or off. The global client version configuration installs with Lync Server 2013 and is used to enable or disable client version control for the entire server deployment. When the Global configuration is enabled, any client version policies you have in place will take effect when users attempt to log on. You can view client version configuration settings from Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

> **Note:**
>
> Because anonymous users are not associated with a user, site, or service, anonymous users are affected by global-level policies only.

To view client version configuration settings by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Client Version Configuration** navigation button.

4. Double-click the name of the client version configuration you want to view.

Viewing Client Version Configuration Settings by Using Windows PowerShell Cmdlets

You can view client version configuration settings by using the **Get-CsClientVersionConfiguration** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view client version configuration information

- To view information about all your client version configuration settings, type the following command in the Lync Server Management Shell and then press ENTER:

```
Get-CsClientVersionConfiguration
```

That will return information similar to this:

```
Identity      : Global
DefaultAction : Allow
DefaultURL    :
Enabled       : True
```

For details, see the Help topic for the Get-CsClientVersionConfiguration cmdlet.

1.7.10.7.1.5 Delete an Existing Collection of Client Version Configuration Settings

Delete an Existing Collection of Client Version Configuration Settings

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Configuration Settings >

Topic Last Modified: *2013-02-23*

If you want to remove the client configuration settings that have been previously configured for a site, you can remove the settings from Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

To remove client configuration settings by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Client Version Configuration** navigation button.
4. Select the site, click **Edit**, click **Delete**, and then click **OK**.

Removing Client Version Configuration

Settings by Using Windows PowerShell Cmdlets

You can delete client version configuration settings by using the **Remove-CsClientVersionConfiguration** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To remove a specified collection of client version configuration settings

- The following command removes the client version configuration settings applied to the Redmond site:

```
Remove-CsClientVersionConfiguration -Identity "site:Redmond"
```

⊟To remove all the client version configuration settings applied to the site scope

- This command removes all the client version configuration settings configured at the site scope:

```
Get-CsClientVersionConfiguration -Filter site:* | Remove-CsClientVersio
```

⊟To remove all the client version configuration settings based on the value of the DefaultAction property

- And this command removes all the client version configuration settings where the default action has been set to "Block":

```
Get-CsClientVersionConfiguration | Where-Object {$_.DefaultAction -eq "
```

For details, see the Help topic for the Remove-CsClientVersionConfiguration cmdlet.

1.7.10.7.2 Client Version Policies

Client Version Policies

Operations > Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 >

Topic Last Modified: *2012-12-11*

Client version policies are used to apply a set of client versioning rules globally or to a particular site, pool, or group of users. Use the following procedures to configure client version policies for Lync Server 2013.

- View Client Version Policies
- Create or Modify a New Client Version Policy
- Delete an Existing Client Version Policy

1.7.10.7.2.1 View Client Version Policies

View Client Version Policies

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Policies >

Topic Last Modified: *2013-02-23*

Client version policies are used to apply a set of client versioning rules globally or to a particular site, pool, or group of users. You can view the client version policies that have been configured in your Lync Server 2013 environment from Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

⊟To view client version policies by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Client Version Policy** navigation button.
4. If you want to view the rules for a client version policy, on the **Client Version Policy** page, double-click the policy you want to view.

Viewing Client Version Policies by Using Windows PowerShell Cmdlets

You can view client version policies by using the **Get-CsClientVersionPolicy** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To view client version policies

- To view information about all your client version policies, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsClientVersionPolicy
  ```

  That will return information similar to this:

  ```
  Identity    : Global
  Rules       : {RuleId=2336c611-a243-4c5d-994b-eea8a524d0e4;
                Description=;Action=Block;ActionUrl=;MajorVersion=1;
                MinorVersion=3;BuildNumber=;QfeNumber=;
                UserAgent=RTC;UserAgentFullName=;Enabled=True;
                CompareOp=LEQ, RuleId=342c9b90-4cef-483a-a73a-
                4fe75c88711d;Description=;Action=Block;ActionUrl=;
                MajorVersion=5;MinorVersion=;BuildNumber=;QfeNumber=;
                UserAgent=WM;UserAgentFullName=;Enabled=True;
                CompareOp=LEQ,RuleId=ea03af61-9db5-4bf9-af3f-042
                ab8dd9994;Description=;Action=Block;ActionUrl=;
                MajorVersion=3;MinorVersion=5;BuildNumber=6907;
                QfeNumber=83;UserAgent=OC;UserAgentFullName=;
                Enabled=True;CompareOp=LEQ, RuleId=831edb68-
                e482-4431-a10e-add365ba8099;Description=;
                Action=Block;ActionUrl=;MajorVersion=2;MinorVersion=0;
                BuildNumber=5999;QfeNumber=;UserAgent=UCCP;
                UserAgentFullName=;Enabled=True;CompareOp=LEQ...}
  Description :
  ```

For details, see the Help topic for the Get-CsClientVersionPolicy cmdlet.

1.7.10.7.2.2 Create or Modify a New Client Version Policy

Create or Modify a New Client Version Policy

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Policies >

***Topic Last Modified:** 2013-02-23*

You can use client version policies to specify the versions of clients that are supported in your environment. Using client versioning can help reduce the costs associated with supporting multiple client versions. It can also improve the overall user experience, because when earlier and later versions of clients interact, the available features can be limited by the earlier version of the client. You can create or modify client version policies from Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

⊟To create or modify client version policies by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**.

   Note:
   The **Client Version Policy** tab is selected by default.

4. On the **Client Version Policy** page, do one of the following:
   - To create a client version policy, click **New**, select **Site policy**, **Pool policy**, or **User policy**, and then click **OK**.
   - To modify the global policy or another existing client version policy, select the policy, click **Edit**, and then click **Show details**.
5. On the **Edit Client Version Policy** page, create or modify rules as described in Create or Modify a New Client Version Policy Rule.

Creating or Modifying Client Version Policies by Using Windows PowerShell Cmdlets

You can create client version policies by using the **New-CsClientVersionPolicy** cmdlet, and modify them by using the **Set-CsClientVersionPolicy** cmdlet. These cmdlets can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To create a new site-scoped client version policy

- The following command creates a new client version policy applied to the Redmond site. Because no additional parameters are specified, the new policy will use the default client version settings.

```
New-CsClientVersionPolicy -Identity "site:Redmond"
```

⊟To create a new per-user client version policy

- To create a per-user policy, use a command similar to this:

```
New-CsClientVersionPolicy -Identity "RedmondClientVersionPolicy"
```

For details, see the Help topics for the New-CsClientVersionPolicy cmdlet and the Set-CsClientVersionPolicy cmdlet.

1.7.10.7.2.3 Delete an Existing Client Version Policy

Delete an Existing Client Version Policy

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Policies >

Topic Last Modified: *2013-02-23*

If you want to delete a client version policy that was previously configured, you can delete it from Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

To delete client version policies by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Client Version Policy** navigation button.
4. On the **Client Version Policy** page, select the client version policy or policies you want to delete, click **Edit**, and then click **Delete**.

Deleting Client Version Policies by Using Windows PowerShell Cmdlets

You can delete client version policies by using the **Remove-CsClientVersionPolicy** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specific client version policy

- This command deletes the client version policy applied to the Redmond site:

```
Remove-CsClientVersionPolicy -Identity site:Redmond
```

To remove all the client version policies applied to the site scope

- This command removes all the client version policies configured at the site scope:

```
Get-CsClientVersionPolicy -Fiter "site:*" | Remove-CsClientVersionPolic
```

To remove client version policies that do not include a specific user agent

- And this command removes any client version policies that do not include a rule for the Windows Phone Lync (WPLync) user agent:

```
Get-CsClientVersionPolicy | Where-Object {$_.Rules -notmatch "UserAgent
```

For details, see the Help topic for the Remove-CsClientVersionPolicy cmdlet.

1.7.10.7.3 Client Version Rules

Client Version Rules

Operations > Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 >

Topic Last Modified: *2012-12-11*

A client version policy is made up of a set of client version policy rules. These rules define the actions that should be taken when users attempt to log on with specific clients and client versions. Use the following procedures to configure client version policy rules for Lync Server 2013

- View Client Version Policy Rules
- Create or Modify a New Client Version Policy Rule
- Delete an Existing Client Version Policy Rule

1.7.10.7.3.1 View Client Version Policy Rules

View Client Version Policy Rules

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Rules >

Topic Last Modified: *2013-02-23*

A client version policy is made up of a set of client version policy rules. These rules define the actions that should be taken when users attempt to log on with specific clients and client versions. You can view client version policy rules from Lync Server 2013 Control Panel or Lync Server 2013 Management Shell.

⊟To view client version policy rules by using Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Client Version Policy** navigation button.
4. On the **Client Version Policy** page, double-click a client version policy you want to view.
5. The rules appear on the **Edit Client Version Policy** page. To view the details for a rule, select the rule, and then click **Show details**.

Viewing Client Version Policy Rules by Using Windows PowerShell Cmdlets

You can view client version policy rules by using Lync Server Management Shell and the **Get-CsClientVersionPolicyRule** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view client version policy rules

- To view the client version policy rules, type the following command in the Lync Server Management Shell and then press ENTER:

```
Get-CsClientVersionPolicyRule
```

  That will return information similar to this for each configured rule:

```
Identity          : Global/2336c611-a243-4c5d-994b-eea8a524d0e4
Priority          : 0
RuleId            : 2336c611-a243-4c5d-994b-eea8a524d0e4
Description       :
Action            : Block
ActionUrl         :
MajorVersion      : 1
MinorVersion      : 3
BuildNumber       :
QfeNumber         :
UserAgent         : RTC
UserAgentFullName :
Enabled           : True
CompareOp         : LEQ
```

For details, see the help topic for the Get-CsClientVersionPolicyRule cmdlet.

1.7.10.7.3.2 Create or Modify a New Client Version Policy Rule

Create or Modify a New Client Version Policy Rule

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Rules >

Topic Last Modified: *2013-01-21*

Client version policy rules define the actions that should be taken when users attempt to log on with specific clients and client versions. You can create or modify individual rules for a client version policy from Lync Server 2013 Control Panel.

Important:

Rules are listed in order of precedence. For example, if you have a rule that allows clients running version 1.5 to connect, followed by a rule that blocks clients running a version earlier than 2.0, the first rule takes precedence, and clients running version 1.5 are allowed to connect.

To create or modify client version policy rules with Lync Server Control Panel

1. Create or Modify a New Client Version Policy with Lync Server Control Panel.
2. On the **Edit Client Version Policy** page, do one of the following:
   - Click **New** to create a new client version rule.
   - Click one of the defined client types in the list, and then click **Show details**.

   Note:

   You can use wildcards to indicate the client type.
3. In **User agent**, select a client type.
4. Under **Version number**, do the following:
   - In **Major version**, type the number that corresponds to the major release of the client.
   - In **Minor version**, type the number that corresponds to the minor release of the client.
   - In **Build**, type the number that corresponds to the major and minor release

of the client.

- In **Update**, type the number that corresponds to the updated release of the client.

> **Note:**
> You can use wildcards to indicate the client version number.

5. To specify the matching operation for the client version you specified in the preceding steps, in **Comparison operation**, click one of the following:
   - **Same as**
   - **Is not**
   - **Newer than**
   - **Newer than or same as**
   - **Older than**
   - **Older than or same as**
6. To specify the action to perform when the criteria in the preceding steps are met, click one of the following in **Action**:
   - To allow the client to log on, click **Allow**.
   - To allow the client to log on and receive updates from Windows Server Update Service or Microsoft Update, click **Allow and Upgrade**. This action is available only when user agent **OC** is selected.

     > **Note:**
     > Selecting this action causes a notification to appear the next time users sign in to Lync 2013. The notification states that an update is available, even if updates have not yet been released to Windows Server Update Service or Microsoft Update. To avoid confusion, you should choose this action only after updates become available.

   - To allow the client to log on and display a message about where to download another client version, click **Allow with URL**. You specify the URL later in this procedure.
   - To prevent the client from logging on, click **Block**.
   - To prevent the client from logging on and allow the client to receive updates from Windows Server Update Service or Microsoft Update, click **Block and Upgrade**. This action is available only when user agent **OC** is selected.
   - To prevent the client from logging on and display a message about where to download another client version, click **Block with URL**. You specify the URL later in this procedure.
7. (Optional) If you clicked **Allow with URL** or **Block with URL** in the previous step, type the client download URL to include in the message in **URL**.
8. Click **OK**, and then click **Commit**.

1.7.10.7.3.3 Delete an Existing Client Version Policy Rule

Delete an Existing Client Version Policy Rule

Managing Devices, Phones, and Client Applications > Specifying the Client Applications That Can Be Used to Log On to Lync Server 2013 > Client Version Rules >

***Topic Last Modified:** 2013-01-21*

A client version policy is made up of a set of client version policy rules. These rules define the actions that should be taken when users attempt to log on with specific clients and client versions. You can delete individual rules from a client version policy from Lync Server 2013 Control Panel.

⊟To delete client version policy rules with Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Clients**, and then click the **Client Version Policy** navigation button.
4. On the **Client Version Policy** page, double-click the client version policy for the rule you want to delete.
5. The rules appear on the **Edit Client Version Policy** page. To delete a rule, select the rule, and then click **Remove**.

1.7.11 Managing Federation and External Access to Lync Server 2013

Managing Federation and External Access to Lync Server 2013

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2013-01-11*

Deploying an Edge Server or Edge pool is the first step to supporting external users. For details about deploying Edge Servers, see Deploying External User Access in the Deployment documentation.

After installing and configuring your internal deployment of Lync Server 2013, internal users in your organization can collaborate with other internal users who have SIP accounts in your Active Directory Domain Services (AD DS). Collaboration can include sending and receiving instant messages, and update of presence status and participating in conferences (also known as "meetings"). You enable and configure external user access to control whether supported external users can collaborate with internal Lync Server users. External users can include remote users of your deployment, federated users (including supported users of public instant messaging (IM) service providers), XMPP federation and anonymous participants in conferences.

If your deployment included the installation of a Lync Server 2013 Edge Server or an Edge pool, the scope of possible communication types is greatly expanded with a number of options for external user access, communication with members of other SIP federated domains, SIP federated providers, and XMPP federated users. After setting up the Edge Server or Edge pool, you enable the types of external user access that you want to provide, and configure the policies to control for the external access. In Lync Server 2013, you enable and configure external user access and policies using the Lync Server Control Panel, the Lync Server Management Shell or both, based on the task requirements. For details about these management tools, see Lync Server Administrative Tools in the Operations documentation, Lync Server Management Shell in the Operations documentation, and Install Lync Server Administrative Tools in the Operations documentation.

Important:

When you design your configuration and policies for external user access, you must understand the precedence of policies and how the policies are applied. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

By default, no policies are configured to support external user access, including remote user access, federated user access, even if you have already enabled external user access support for your organization. To control the use of external user access, you must configure one or more policies, specifying the type of external user access supported for each policy. This includes the following external access policies:

- **Global policy** The global policy is created when you deploy your Edge Servers. By default, no external user access options are enabled in the global policy. To support external user access at the global level, you configure the global policy to support one or more types of external user access options. The global policy applies to all users in your organization, but site policies and user policies override the global policy. If you delete the global policy, you do not remove it. Instead, you reset it to the default setting.
- **Site policy** You can create and configure one or more site policies to limit support for external user access to specific sites. The configuration in the site policy overrides the global policy, but only for the specific site covered by the site policy. For example, if you enable remote user access in the global policy, you might specify a site policy that disables remote user access for a specific site. By default, a site policy is applied to all users of that site, but you can assign a user policy to a user to override the site policy setting.
- **User policy** You can create and configure one or more user policies to limit support for remote user access to specific users. The configuration in the user policy overrides the global and site policy, but only for the specific users to whom the user policy is assigned. For example, if you enable remote user access in the global policy and site policy, you might specify a user policy that disables remote user access and then assign that user policy to specific users. If you create a user policy, you must apply it to one or more users before it takes effect.

To determine which configuration settings and which policies you need to create or edit, refer to the following decision points:

Do you want to allow internal and external users of your domain to be able to collaborate using instant messaging, Web conferencing, and Audio/Video?

Configure the settings as detailed in the topics Configure Policies to Control Remote User Access, and Enable or Disable Federation and Public IM Connectivity

Do you want to allow anonymous users to attend and be invited to conferences hosted by users in your deployment?

Configure the settings as detailed in the topic Assign Conferencing Policies to Support Anonymous Users, Create or Modify a Conferencing Policy and Conferencing Policy Settings Reference

Do you want to allow users to communicate with SIP Federated Domain contacts?

Configure the settings as detailed in the topics Configure Policies to Control Federated User Access, Enable or Disable Federation and Public IM Connectivity, and Manage SIP Federated Domains for Your Organization

If you have enabled communication with SIP Federation Domains, do you want to enable communications with XMPP Federated Partner contacts?

Configure the settings as detailed in the topic Configure Policies to Control XMPP Federated User Access and Manage XMPP Federated Partners for Your Organization.

If you have enabled communication with SIP Federated Domains, do you want to enable SIP Federation automatic discovery?

Configure the settings as detailed in the topic Enable or Disable Discovery of Federation

Partners.

If you have enabled communication with SIP Federation Domains, do you want to enable sending a disclaimer to Federated contacts notifying them that you use archiving and that communications may be archived?

Configure the settings as detailed in the topic Enable or Disable Sending an Archiving Disclaimer to Federated Partners.

Do you want to allow users to communicate with SIP Federated Providers that enable communication with public providers, such as Windows Live Messenger, AOL, and Yahoo!?

Configure the settings as detailed in the topics Configure Policies to Control Public User Access Enable or Disable Federation and Public IM Connectivity, and Create or Edit Public SIP Federated Providers.

◆Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

Do you want to allow users to communicate with SIP Federated Providers that are hosted providers running Microsoft Office 365, Microsoft Lync Online and Microsoft Lync Online 2010?

Configure the settings as detailed in the topics Create or Edit Public SIP Federated Providers, Enable or Disable Federation and Public IM Connectivity and Create or Edit Hosted SIP Federated Providers

Is your deployment configured in a split (also known as a hybrid) domain, where some users have their home server in an on-premise deployment, and other users are configured with a home server in an online environment?

Configure the settings as detailed in the topics Configure Policies to Control Federated User Access, Enable or Disable Federation and Public IM Connectivity and Create or Edit Hosted SIP Federated Providers

If you prefer a table that lists the requirements:

Tab in Federation and External Access (Across) Federation or External Access Type	External Access Policy	Access Edge Config	SIP Federated Domains	SIP Federated Providers	XMPP Federated Partner

(Down)					
Remote Users	Configure Policies to Control Remote User Access	Enable or Disable Remote User Access			
SIP Federated Contacts	Configure Policies to Control Federated User Access	Enable or Disable Federation and Public IM Connectivity Enable or Disable Discovery of Federation Partners Enable or Disable Sending an Archiving Disclaimer to Federated Partners	Manage SIP Federated Domains for Your Organization		
XMPP Federated Contacts	Configure Policies to Control Federated User Access Configure Policies to Control XMPP Federated User Access	Enable or Disable Federation and Public IM Connectivity			Manage XMPP Federated Partners for Your Organization
Split Domain / Hybrid Users	Configure Policies to Control Federated User Access	Enable or Disable Federation and Public IM Connectivity		Create or Edit Hosted SIP Federated Providers	
Public IM Service Contacts	Configure Policies to Control Public User Access	Enable or Disable Federation and Public IM Connectivity		Create or Edit Public SIP Federated Providers	
Anonymous user access to meetings and conferences		Assign Conferencing Policies to Support Anonymous Users **Note:** You must also consider the			

		following configuration settings under Conferencing policies: Create or Modify a Conferencing Policy and Conferencing Policy Settings Reference			

You can configure external user access settings, including any policies that you want to use to control external user access, even if you have not enabled external user access for your organization. However, the policies and other settings that you configure are in effect only when you have external user access enabled for your organization. External users cannot communicate with users of your organization when external user access is disabled or if no external user access policies are configured to support it.

Your edge deployment authenticates the types of external users (except for anonymous users, who are authenticated by the conference ID and a passkey that is sent to the anonymous participant when you create the conference and invite participants) and controls access based on how you configure your edge support. In order to control communications, you can configure one or more policies and configure settings that define how users inside and outside your deployment communicate with each other. The policies and settings include the default global policy for external user access, in addition to site and user policies that you can create and configure to enable one or more types of external user access for specific sites or users.

- Manage External Access Policy for Your Organization
- Manage Access Edge Configuration for Your Organization
- Manage SIP Federated Domains for Your Organization
- Manage SIP Federated Providers for Your Organization
- Manage XMPP Federated Partners for Your Organization
- Configuring Federation Support for a Lync Online Customer

1.7.11.1 Manage External Access Policy for Your Organization

Manage External Access Policy for Your Organization

Operations > Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 >

Topic Last Modified: *2013-02-22*

After deploying one or more Edge Servers, you must enable the types of external access that will be supported for your organization.

By default, there are no policies configured to support external user access, including remote user access, federated user access, even if you have already enabled external user access support for your organization. To control the use of external user access, you must configure one or more policies, specifying the type of external user access supported for each policy. The following policy scopes are available for creation and configuration. By default, the Global policy is created, but cannot be deleted.

- **Global policy** The global policy is created when you deploy your Edge Servers. By default, no external user access options are enabled in the global policy. To support external user access at the global level, you configure the global policy to support one or more types of external user access options. The global policy applies to all users in your organization, but site policies and user policies override the global policy. If you delete the global policy, you do not remove it. Instead, you reset it to the default setting.

- **Site policy** You can create and configure one or more site policies to limit support for external user access to specific sites. The configuration in the site policy overrides the global policy, but only for the specific site covered by the site policy. For example, if you enable remote user access in the global policy, you might specify a site policy that disables remote user access for a specific site. By default, a site policy is applied to all users of that site, but you can assign a user policy to a user to override the site policy setting.
- **User policy** You can create and configure one or more user policies to limit support for remote user access to specific users. The configuration in the user policy overrides the global and site policy, but only for the specific users to whom the user policy is assigned. For example, if you enable remote user access in the global policy and site policy, you might specify a user policy that disables remote user access and then assign that user policy to specific users. If you create a user policy, you must apply it to one or more users before it takes effect.

> **Important:**
>
> Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

These options include the following types of external access:

- **Enable communications with federated users** Enable this if you want to support user access to federated partner domains. This setting configures the ability for users to communicate with other SIP federated domains, as well as Hosted providers like Microsoft Office 365. Selecting this setting allows you to select the option to allow communication with XMPP federated domains.
  As an option, you can select **Enable communications with XMPP federated partners** if you first select **Enable communications with federated users**. XMPP federation is a federation with organizations that use extensible messaging and presence protocol (XMPP).

  > **Note:**
  >
  > If you enable XMPP federation, you must also select to deploy **XMPP federation** in the Edge pools configuration section of Topology Builder. Configuring for XMPP federation deploys an XMPP Proxy on the Edge Server and an XMPP gateway on the Front End Server.

- **Enable communications with remote users** Enable this option if you want users in your organization who are outside your firewall, such as telecommuters and users who are traveling, to be able to connect to Lync Server over the Internet.
- **Enable communications with public users** Enable this option if you want internal users to be able to communicate with public IM provider contacts, such as those provided by Windows Live, Yahoo!, and America Online (AOL).

  > **Important:**
  >
  > - As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License (“PIC USL”) is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
  > - The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to

> federate with Yahoo! Messenger. Microsoft’s ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
>
> - More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

> **Note:**
>
> In addition to enabling external user access support, you must also configure policies to control the use of external user access in your organization before any type of external user access is available to users. For details about creating, configuring, and applying policies for external user access see Enable or Disable Remote User Access.

To view external access policies by using Windows PowerShell cmdlets

- You can view external access policies by using Lync Server Management Shell and the **Get-CsExternalAccessPolicy** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

  To view information about all your external access policies, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsExternalAccessPolicy
  ```

  This command returns information similar to the following:

  ```
  Identity                          : Global
  Description                       :
  EnableFederationAccess            : False
  EnableXmppAccess                  : False
  EnablePublicCloudAccess           : False
  EnablePublicCloudAudioVideoAccess : False
  EnableOutsideAccess               : False
  ```

- Configure Policies to Control Federated User Access
- Configure Policies to Control XMPP Federated User Access
- Configure Policies to Control Remote User Access
- Configure Policies to Control Public User Access
- Assign an External User Access Policy to a Lync Enabled User
- Resetting or Deleting External User Access Policies

1.7.11.1.1 Configure Policies to Control Federated User Access

Configure Policies to Control Federated User Access

See Also

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up Lync Federation >

Topic Last Modified: *2012-11-01*

When you configure policies to support communications with federated partners, the policies apply to users of federated domains. You can configure one or more external user access policies to control whether users of federated domains can collaborate with your Lync Server 2013 users. To control federated user access, you can configure policies at the global, site, and user level. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

Note:

You can configure policies to control federated user access, even if you have not enabled federation for your organization. However, the policies that you configure are in effect only when you have federation enabled for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation. Additionally, if you specify a user policy to control federated user access, the policy applies only to users that are enabled for Lync Server 2013 and configured to use the policy. For details about specifying federated users that can sign in to Lync Server 2013, see Assign an External User Access Policy to a Lync Enabled User in the Deployment documentation or the Operations documentation.

⊟To configure a policy to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do one of the following:
   - To configure the global policy to support federated user access, click the global policy, click **Edit**, and then click **Show details**.
   - To create a new site policy, click **New**, and then click **Site policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
   - To create a new user policy, click **New**, and then click **User policy**. In **New External Access Policy**, create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnableFederatedUsers** for a user policy that enables communications for federated domain users).
   - To change an existing policy, click the appropriate policy listed in the table, click **Edit**, and then click **Show details**.
5. (Optional) If you want to add or edit a description, specify the information for the policy in **Description**.
6. Do one of the following:
   - To enable federated user access for the policy, select the **Enable communications with federated users** check box.
   - To disable federated user access for the policy, clear the **Enable communications with federated users** check box.
7. Click **Commit**.

To enable federated user access, you must also enable support for federation in your organization. For details, see Enable or Disable Federation and Public IM Connectivity.

If this is a user policy, you must also apply the policy to users that you want to be able to collaborate with federated users. For details, see Assign an External User Access Policy to a Lync Enabled User.

⊟To configure an existing policy using Windows PowerShell to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click

Microsoft Lync Server 2013, and then click **Lync Server Management Shell**.

3. Type the following in the Lync Server Management Shell:

```
Set-CsExternalAccessPolicy -Identity <name of global, site or user pol
```

An example command that will set the global policy for Federated user access to enabled, XMPP domain access to enabled, Remote user access to enabled, Public provider access to enabled, and grant the ability to use audio and video for public providers that support it:

```
Set-CsExternalAccessPolicy -Identity global -EnableFederationAccess $t
```

Tip:

The parameter "EnablePublicCloudAudioVideoAccess" does not have a corresponding selection in the Lync Server Control Panel

To create a new policy using Windows PowerShell to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

```
New-CsExtenalAccessPolicy -Identity <name of site or user policy – you
```

An example of creating a new site policy:

```
New-CsExternalAccessPolicy -Identity site:Redmond -EnableFederationAcc
```

To delete or reset a policy using Windows PowerShell to support access by users of federated domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Type the following in the Lync Server Management Shell

```
Remove-CsExternalAccessPolicy -Identity <name of global, site or user
```

An example of resetting the global policy (The global policy can only have its setting removed. The policy cannot be deleted):

```
Remove-CsExternalAccessPolicy -Identity global
```

To remove a site policy, type:

```
Remove-CsExternalAccessPolicy -Identity site:Redmond
```

Deletes the site policy Redmond. To delete a user policy named UserEAPPolicy, type:

```
Remove-CsExternalAccessPolicy -Identity UserEAPPolicy
```

Tasks

Enable or Disable Federation and Public IM Connectivity
Assign an External User Access Policy to a Lync Enabled User

Other Resources

Manage SIP Federated Domains for Your Organization
Manage SIP Federated Providers for Your Organization
Set-CsExternalAccessPolicy
New-CsExternalAccessPolicy
Get-CsExternalAccessPolicy
Remove-CsExternalAccessPolicy

Grant-CsExternalAccessPolicy

1.7.11.1.2 Configure Policies to Control XMPP Federated User Access

Configure Policies to Control XMPP Federated User Access

See Also

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up XMPP Federation >

Topic Last Modified: *2012-11-01*

This is preliminary documentation and is subject to change. Blank topics are included as placeholders.

When you configure policies for support of extensible messaging and presence protocol (XMPP) federated partners, the policies apply to users of XMPP federated domains, but not to users of session initiation protocol (SIP) instant messaging (IM) service providers (for example, Windows Live), or SIP federated domains. You configure an **XMPP Federated Partner** for each XMPP federated domain that you want to allow your users to add contacts and communicate with. XMPP federated partners policies are only available in a single scope, though it is not defined as a global policy, acts as a global policy. To define a global, site or user policy for XMPP Federation Partners, you configure the policy scope by first creating and configuring the External Access Policy for the scope you require. For details about the types of policies that you can configure for external access and federation, see Managing Federation and External Access to Lync Server 2013 in the Operations documentation.

Note:

All **Federation and External Access** policies are applied through in-band provisioning. The policies that apply to the user, belong to a site, or are global in scope are communicated to the client during login. You can configure policies to control XMPP federated partner access, even if you have not enabled XMPP federation for your organization. However, the policies that you configure take effect only when you have XMPP partner federation deployed, enabled and configured for your organization. For details about deploying and configuring XMPP partner federation, see Configuring SIP Federation, XMPP Federation and Public Instant Messaging in the Deployment documentation. Additionally, if you specify a user policy in External Access Policy to control XMPP federated partners, the policy applies only to users that are enabled for Lync Server 2013 and configured to use the policy.

⊟To edit a global policy for XMPP federated partners

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do the following for the global policy:
5. Click the global policy, click **Edit**, and then click Show details.
6. Provide a description for the Global policy (optional).
7. Select **Enable communications with federated users**.
8. Select **Enable communications with XMPP federated users**.
9. Click **Commit** to save your changes to the Global policy.

⊟To create a site or user policy for XMPP federated partners

1. Click **New**, and then click **Site policy** or **User policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
2. Provide a description for the Site policy (optional).
3. In the site or user policy, select **Enable communications with federated users**.
4. Select **Enable communications with XMPP federated users**.
5. Click **Commit** to save your changes to the site or user policy.

To edit an existing policy for XMPP federated partners

1. To change an existing policy, select the appropriate policy in the list, click **Edit**, and then click **Show details**.
2. Change or update the description for the policy (optional).
3. Select or unselect **Enable communications with federated users**.
4. Select or unselect **Enable communications with XMPP federated users**.
5. Click **Commit** to save your changes to the policy.

To edit an existing policy for XMPP federated partners by using Windows PowerShell

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   Set-CsExternalAccessPolicy -Identity <name of global, site or user pol
   ```

   An example command that will set the global policy for Federated user access to True (enabled) and XMPP domain access to True (enabled):

   ```
   Set-CsExternalAccessPolicy -Identity global -EnableFederationAccess $t
   ```

To create a site or user policy for XMPP federated partners using Windows PowerShell

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   New-CsExternalAccessPolicy -Identity <name of global, site or user pol
   ```

   An example command that will set a site policy for the Redmond site for Federated user access to enabled and XMPP domain access to enabled:

   ```
   New-CsExternalAccessPolicy -Identity site:Redmond -EnableFederationAcc
   ```

To delete an existing policy for XMPP federated partners by using Windows PowerShell

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Type the following in the Lync Server Management Shell:

   ```
   Remove-CsExternalAccessPolicy -Identity <name of global, site or user
   ```

An example command that will delete a user policy:

```
Remove-CsExternalAccessPolicy -Identity EAPUserPolicySetXMPP
```

4. An example command that will reset the global policy to defaults:

```
Remove-CsExternalAccessPolicy -Identity global
```

Tasks

Assign an External User Access Policy to a Lync Enabled User
Enable or Disable Federation and Public IM Connectivity

Other Resources

Manage XMPP Federated Partners for Your Organization
Set-CsExternalAccessPolicy
New-CsExternalAccessPolicy
Get-CsExternalAccessPolicy
Remove-CsExternalAccessPolicy
Grant-CsExternalAccessPolicy

1.7.11.1.3 Configure Policies to Control Remote User Access

Configure Policies to Control Remote User Access

Deployment > Deploying External User Access > Configuring Support for External User Access >

Topic Last Modified: *2012-10-18*

You configure one or more external user access policies to control whether remote users can collaborate with internal Lync Server users. To control remote user access, you can configure policies at the global, site, and user level. Site policies override the global policy, and user policies override site and global policies. For details about the types of policies that you can configure, see Managing Federation and External Access to Lync Server 2013. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

Note:
You can configure policies to control remote user access, even if you have not enabled remote user access for your organization. However, the policies that you configure are in effect only when you have remote user access enabled for your organization. For details about enabling remote user access, see Enable or Disable Federation and Public IM Connectivity. Additionally, if you specify a user policy to control remote user access, the policy applies only to users that are enabled for Lync Server and configured to use the policy. For details about specifying users that can sign in to Lync Server from remote locations, see Assign an External User Access Policy to a Lync Enabled User.

Use the following procedure to configure each external access policy that you want to use to control remote user access.

Note:
This procedure describes how to configure a policy only to enable communications with remote users, but each policy that you configure to support remote user access can also configure federated user access and public user access. For details about configuring policies to support federated users, see Configure Policies to Control Federated User Access. For details about configuring policies to support public users, see Create or Edit Public SIP Federated Providers.

⊟To configure an external access policy to support remote user access

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do one of the following:
   - To configure the global policy to support remote user access, click the global policy, click **Edit**, and then click **Show details**.
   - To create a new site policy, click **New**, and then click **Site policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
   - To create a new user policy, click **New**, and then click **User policy**. In **New External Access Policy**, create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnableRemoteUsers** for a user policy that enables communications for remote users).
   - To change an existing policy, click the appropriate policy listed in the table, click **Edit**, and then click **Show details**.
5. (Optional) If you want to add or edit a description, specify the information for the policy in **Description**.
6. Do one of the following:
   - To enable remote user access for the policy, select the **Enable communications with remote users** check box.
   - To disable remote user access for the policy, clear the **Enable communications with remote users** check box.
7. Click **Commit**.

To enable remote user access, you must also enable support for remote user access in your organization. For details, see Enable or Disable Federation and Public IM Connectivity in the Deployment documentation or the Operations documentation.

If this is a user policy, you must also apply the policy to users that you want to be able to connect remotely. For details, see Assign an External User Access Policy to a Lync Enabled User in the Deployment documentation or the Operations documentation.

1.7.11.1.4 Configure Policies to Control Public User Access

Configure Policies to Control Public User Access

See Also

Deploying External User Access > Configuring SIP Federation, XMPP Federation and Public Instant Messaging > Setting Up Public Instant Messaging Connectivity >

Topic Last Modified: *2013-01-11*

Public instant messaging (IM) connectivity enables users in your organization to use IM to communicate with users of IM services provided by public IM service providers, including the Windows Live network of Internet services, Yahoo!, and AOL. You configure one or more external user access policies to control whether public users can collaborate with internal Lync Server users. Public instant messaging connectivity is an added feature that relies on configuration of your deployment and users. It also depends on the provisioning of the service at the public IM provider. For information on how to provision your deployment to use the public providers, see the “Public IM Connectivity Provisioning Guide for Microsoft Lync Server, Office Communications Server, and Live Communications Server” guide: http://go.microsoft.com/fwlink/?LinkId=269821

Important:

- As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License ("PIC USL") is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013).
- The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft's ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is winding down.
- More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.

To access the Microsoft Lync Server Public IM Connectivity Provisioning site, use the following link: http://go.microsoft.com/fwlink/p/?linkId=212638

To control public user access, you can configure policies at the global, site, and user level. For details about the types of policies that you can configure, see Configuring Support for External User Access in the Deployment documentation or the Planning documentation. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object.

In the case of IM invitations, the response depends on the client software. The request is accepted unless external senders are explicitly blocked by a user-configured rule (that is, the settings in the user's client **Allow** and **Block** lists). Additionally, IM invitations can be blocked if a user elects to block all IM from users who are not on his or her **Allow** list.

Note:

You can configure policies to control public user access, even if you have not enabled federation for your organization. However, the policies that you configure are in effect only when you have federation enabled for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation. Additionally, if you specify a user policy to control public user access, the policy applies only to users that are enabled for Lync Server and configured to use the policy. For details about specifying public users that can sign in to Lync Server, see Assign an External User Access Policy to a Lync Enabled User in the Deployment documentation or the Operations documentation.

Use the following procedure to configure a policy to support access by users of one or more public IM providers.

To configure an external access policy to support public user access

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **External Access Policy**.
4. On the **External Access Policy** page, do one of the following:
   - To configure the global policy to support public user access, click the global policy, click **Edit**, and then click **Show details**.

- To create a new site policy, click **New**, and then click **Site policy**. In **Select a Site**, click the appropriate site from the list and then click **OK**.
- To create a new user policy, click **New**, and then click **User policy**. In **New External Access Policy**, create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnablePublicUsers** for a user policy that enables communications for public users).
- To change an existing policy, click the appropriate policy listed in the table, click **Edit**, and then click **Show details**.

5. (Optional) If you want to add or edit a description, specify the information for the policy in **Description**.
6. Do one of the following:
   - To enable public user access for the policy, select the **Enable communications with public users** check box.
   - To disable public user access for the policy, clear the **Enable communications with public users** check box.
7. Click **Commit**.

To enable public user access, you must also enable support for federation in your organization. For details, see Configure Policies to Control Federated User Access.

If this is a user policy, you must also apply the policy to public users that you want to be able to collaborate with public users. For details, see Assigning Per-User Policies.

Tasks

Create or Edit Public SIP Federated Providers

Other Resources

Manage SIP Federated Providers for Your Organization

1.7.11.1.5 Assign an External User Access Policy to a Lync Enabled User

Assign an External User Access Policy to a Lync Enabled User

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Manage External Access Policy for Your Organization >

Topic Last Modified: *2013-02-22*

If a user has been enabled for Lync Server, you can configure SIP federation, XMPP federation, remote user access, and public instant messaging (IM) connectivity in the Lync Server Control Panel by applying the appropriate policies to specific users. For example, if you created a policy to support remote user access, you must apply it to the user before the user can connect to Lync Server from a remote location and collaborate with internal users from the remote location.

Note:
To support external user access, you must enable support for each type of external user access you want to support, and configure the appropriate policies and other options to control its use. For details, see Configuring Support for External User Access in the Deployment documentation or Managing Federation and External Access to Lync Server 2013 in the Operations documentation.

Use the procedure in this topic to apply a previously created external user access policy to one or more user accounts.

⊟To apply an external user policy to a user account

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync

Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Users**, and then search on the user account that you want to configure.
4. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
5. In **Edit Lync Server User** under **External access policy**, select the user policy that you want to apply.

Note:
The **<Automatic>** settings apply the default server or global policy settings.

Assigning Per-User External Access Policies by Using Windows PowerShell Cmdlets

Per-user external access policies can be assigned by using Windows PowerShell and the Grant-CsExternalAccessPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To assign a per-user external access policy to a single user

- This command assigns the per-user external access policy RedmondExternalAccessPolicy to the user Ken Myer.

```
Grant-CsExternalAccessPolicy -Identity "Ken Myer" -PolicyName "RedmondE
```

⊟To assign a per-user external access policy to multiple users

- This command assigns the per-user external access policy USAExternalAccessPolicy to all the users who have accounts in the UnitedStates OU in Active Directory. For more information on the OU parameter used in this command, see the documentation for the Get-CsUser cmdlet.

```
Get-CsUser -OU "ou=UnitedStates,dc=litwareinc,dc=com" | Grant-CsExterna
```

⊟To unassign a per-user external access policy

- This command unassigns any per-user external access policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsExternalAccessPolicy -Identity "Ken Myer" -PolicyName $Null
```

For more information, see the help topic for the Grant-CsExternalAccessPolicy cmdlet.

1.7.11.1.6 Resetting or Deleting External User Access Policies

Resetting or Deleting External User Access Policies

Managing Users in Lync Server 2013 > User Accounts Enabled for Lync Server 2013 > Manage External Access Policy for Your Organization >

Topic Last Modified: *2012-09-08*

If you have created or configured external user access policies that you no longer want to use, you can do the following:

- Delete any site or user policy that you created.
- Reset the global policy to the default settings. The default global policy settings deny any external user access. The global policy cannot be deleted.
- Delete a Site or User Policy for External User Access
- Reset the Global Policy for External User Access

1.7.11.1.6.1 Delete a Site or User Policy for External User Access

Delete a Site or User Policy for External User Access

User Accounts Enabled for Lync Server 2013 > Manage External Access Policy for Your Organization > Resetting or Deleting External User Access Policies >

Topic Last Modified: *2013-02-22*

You can delete any site or user policy that is listed in Lync Server Control Panel on the **External Access Policy** page. Deleting the global policy does not actually delete it, but only resets it to the default settings, which do not include support for any external user access options. For details about resetting the global policy, see Reset the Global Policy for External User Access.

To delete a site or user policy for external user access

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. Click **External User Access**, click **External Access Policy**.
4. On the **External Access Policy** tab, click the site or user policy you want to delete, click **Edit**, and then click **Delete**.
5. When prompted to confirm the deletion, click **OK**.

Removing PIN Policies by Using Windows PowerShell Cmdlets

External access policies can be deleted by using Windows PowerShell and the Remove-CsExternalAccessPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specific external access policy

- This command removes the external access policy applied to the Redmond site:

```
Remove-CsExternalAccessPolicy -Identity "site:Redmond"
```

To remove all the external access policies applied to the per-user scope

- This command removes all the external access policies configured at the per-user scope:

```
Get-CsExternalAccessPolicy -Filter "tag:*" | Remove-CsExternalAccessPol
```

To remove all the external access policies where outside user access is disabled

- This command deletes all the external access policies where outside user access has been disabled:

```
Get-CsExternalAccessPolicy | Where-Object {$_.EnableOutsideAccess -eq $
```

For more information, see the help topic for the Remove-CsExternalAccessPolicy cmdlet.

1.7.11.1.6.2 Reset the Global Policy for External User Access

Reset the Global Policy for External User Access

User Accounts Enabled for Lync Server 2013 > Manage External Access Policy for Your Organization > Resetting or Deleting External User Access Policies >

Topic Last Modified: *2013-02-22*

You cannot completely delete a global policy. Using the **Delete** option on the global policy only resets the global policy to the default settings, which do not include support for any external user access options.

To reset the global policy to the default settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, click **External Access Policy**.
4. On the **External Access Policy** tab, click the global policy, click **Edit**, and then click **Delete**.
5. When prompted to confirm the deletion, click **OK**. A message appears at the top of the page informing you that the global policy has been reset.

Resetting the Global External Access Policy by Using Windows PowerShell Cmdlets

The global external access policy can be reset by using Windows PowerShell and the Remove-CsExternalAccessPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To reset the global external access policy

- This command resets the global external access policy:

```
Remove-CsExternalAccessPolicy -Identity "global"
```

For more information, see the help topic for the Remove-CsExternalAccessPolicy cmdlet.

1.7.11.2 Manage Access Edge Configuration for Your Organization

Manage Access Edge Configuration for Your Organization

Microsoft Lync Server 2013 > Operations > Managing Federation and External Access to Lync Server 2013 >

Topic Last Modified: *2012-11-01*

This is preliminary documentation and is subject to change. Blank topics are included as placeholders.

After deploying one or more Edge Servers, you must enable the types of external domain or provider access, remote user access, and anonymous user access to conferences through the Edge Servers that will be supported for your organization.

These options include the following types of access that can be configured through the **Access Edge Configuration** page:

- **Enable federation and public IM connectivity** Enable this if you want to support user access to federated partner domains. This setting applies to both SIP federation and XMPP federation that are configured for global, site or user scopes on the **External Access Policy** page. For federation settings to apply, you must configure federation support on both pages.
  Two options exist that are optional settings for how federated partners are discovered, and whether archiving disclaimers (notification to federated contacts that you communicate with that your deployment has archiving enabled and that the communications details will be archived) will be sent to contacts
  - **Enable partner domain discovery** Selecting this option enables the automatic discovery of domains that you can federate with. Lync Server 2013 uses Domain Name System (DNS) records to try to discover domains not listed in the allowed domains list, automatically evaluating incoming traffic from discovered federated partners and limiting or blocking that traffic based on trust level, amount of traffic, and administrator settings. If you do not select this option, federated user access is enabled only for users in the domains that you include on the allowed domains list. Whether or not you select this option, you can specify that individual domains to be blocked or allowed, including restricting access to specific servers running the Access Edge service in the federated domain. For details, see Configure Support for Allowed External Domains.
  - **Send archiving disclaimer to federated partners** Selecting this option enables the sending of an archiving disclaimer message to federated partners that advises them that communications details are recorded. If you archive external communications with federated partner domains, you should enable the archiving disclaimer notification to warn partners that their messages and communications details are being archived by your deployment. For details on archiving, see Defining Your Organization's Requirements for Archiving.
- **Enable remote user access** Enable this option if you want users in your organization who are outside your firewall, such as telecommuters and users who are traveling, to be able to connect to Lync Server. For details, see Enable or Disable Remote User Access.
- **Enable anonymous users to access conferences** Enable this option if you want internal users to invite external anonymous users to conferences that

they organize. Enabling this setting only allows anonymous users for conferences. To configure the conferencing experience and options that will define how and what your users can do with conferences and for the inclusion of anonymous users, see details at **Create or Modify Conferencing User Experience for a Site or Users** and Conferencing Policy Settings Reference.

Note:

In addition to enabling external user access support, you also configure policies to control the use of remote user access in your organization before any type of external user access is available to users. For details about creating, configuring, and applying policies for external user access, see Manage External Access Policy for Your Organization.

Viewing Access Edge configuration information by using Windows PowerShell cmdlets

- Access Edge configuration information can be viewed by using Windows PowerShell and the **Get-CsAccessEdgeConfiguration** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

  To view information about all your Access Edge configuration settings, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsAccessEdgeConfiguration
  ```

  That will return information similar to this:

  ```
  Identity                                : Global
  AllowAnonymousUsers                     : False
  AllowFederatedUsers                     : False
  AllowOutsideUsers                       : True
  BeClearingHouse                         : False
  EnablePartnerDiscovery                  : False
  EnableArchivingDisclaimer               : False
  EnableUserReplicator                    : True
  KeepCrlsUpToDateForPeers                : True
  MarkSourceVerifiableOnOutgoingMessages : True
  OutgoingTlsCountForFederatedPartners    : 4
  DiscoveredPartnerStandardRate           : 20
  EnableDiscoveredPartnerContactsLimit    : True
  MaxContactsPerDiscoveredPartner         : 1000
  DiscoveredPartnerReportPeriodMinutes    : 60
  MaxAcceptedCertificatesStored           : 1000
  MaxRejectedCertificatesStored           : 500
  CertificatesDeletedPercentage           : 20
  RoutingMethod                           : UseDnsSrvRouting
  ```

- Enable or Disable Federation and Public IM Connectivity
- Enable or Disable Discovery of Federation Partners
- Enable or Disable Sending an Archiving Disclaimer to Federated Partners
- Enable or Disable Remote User Access
- Enable or Disable Anonymous User Access
- Assign Conferencing Policies to Support Anonymous Users

1.7.11.2.1 Enable or Disable Federation and Public IM Connectivity

Enable or Disable Federation and Public IM Connectivity

Operations > Managing Federation and External Access to Lync Server 2013 > Manage Access Edge Configuration for Your Organization >

Topic Last Modified: *2013-02-23*

Support for federation is required to enable users who have an account with a trusted customer or partner organization, including partner domains and users of public instant messaging (IM) provider users that you support, to collaborate with users in your organization. Federation is also required to use a hosted Exchange service provider to provide voice mail to Enterprise Voice users whose mailboxes are located on a hosted Exchange service such as Microsoft Exchange Online. When you have established a trust relationship with these external domains, you can authorize users in those domains to access your deployment and participate in Lync Server communications. This trust relationship is called a federation and it is not related to, or dependent upon, an Active Directory trust relationship.

To support access by users of federated domains, you must enable federation. If you enable federation for your organization, you must also specify whether to implement the following options:

- **Enable partner domain discovery** If you enable this option, Lync Server uses Domain Name System (DNS) records to try to discover domains not listed in the allowed domains list, automatically evaluating incoming traffic from discovered federated partners and limiting or blocking that traffic based on trust level, amount of traffic, and administrator settings. If you do not select this option, federated user access is enabled only for users in the domains that you include on the allowed domains list. Whether or not you select this option, you can specify that individual domains to be blocked or allowed, including restricting access to specific servers running the Access Edge service in the federated domain. For details about controlling access by federated domains, see Configure Support for Allowed External Domains.
- **Send an archiving disclaimer to federated partners** Disclaimer notice is sent to federated partners that archiving in your deployment is in place. If you support archiving of external communications with federated partner domains, you should enable the archiving disclaimer notification to warn partners that their messages are being archived.

If you later want to temporarily or permanently prevent access by users of federated domains, you can disable federation for your organization. Use the procedure in this section to enable or disable federated user access for your organization, including specifying the appropriate federation options to be supported for your organization.

Note:

Enabling federation for your organization only specifies that your servers running the Access Edge service support routing to federated domains. Users in federated domains cannot participate in IM or conferences in your organization until you also configure at least one policy to support federated user access. Users of public IM service providers cannot participate in IM or conferences in your organization until you also configure at least one policy to support public IM connectivity. Lync Server cannot use a hosted Exchange service to provide call answering, Outlook Voice Access (including voice mail), or auto-attendant services for users whose mailboxes are located on a hosted Exchange service until you configure a hosted voice mail policy that provides routing information. For details about configuring policies for communication with users of federated domains in other organizations, see Manage SIP Federated Domains for Your Organization in the Operations documentation. Additionally, if you want to support communication with users of IM service providers, you must configure policies to support it and also configure support for the individual service providers that you want to support. For details, see Manage SIP Federated Providers for Your Organization in the Operations documentation. For details about creating a hosted voice mail policy, see Manage Hosted Voice Mail Policies in the Deployment documentation.

⊟To enable or disable federated user access for your organization

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **Access Edge Configuration**.
4. On the **Access Edge Configuration** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, do one of the following:
   - To enable federated user access for your organization, select the **Enable communications with federated users** check box.
   - To disable federated user access for your organization, clear the **Enable communications with federated users** check box.
6. If you selected the **Enable communications with federated users** check box, do the following:
   - If you want to support automatic discovery of partner domains, select the **Enable partner domain discovery** check box.
   - If your organization supports archiving of external communications, select the **Send archiving disclaimer to federated partners** check box.
7. Click **Commit**.

To enable federated users to collaborate with users in your Lync Server 2013 deployment, you must also configure at least one external access policy to support federated user access. For details, see Configure Policies to Control Federated User Access in the Deployment documentation or the Operations documentation. To control access for specific federated domains, see Configure Support for Allowed External Domains in the Deployment documentation or Operations documentation.

Enabling or Disabling Federation and Public IM Connectivity by Using Windows PowerShell Cmdlets

Federation and public IM connectivity can also be managed by using Windows PowerShell and the Set-CsAccessEdgeConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable federation and public IM connectivity

- To enable federation and public IM connectivity, set the value of the **AllowFederatedUsers** property to True ($True):

  ```
  Set-CsAccessEdgeConfiguration -AllowFederatedUsers $True
  ```

To disable federation and public IM connectivity

- To disable federation and public IM connectivity, set the value of the **AllowFederatedUsers** property to False ($False):

  ```
  Set-CsAccessEdgeConfiguration -AllowFederatedUsers $True
  ```

1.7.11.2.2 Enable or Disable Discovery of Federation Partners

Enable or Disable Discovery of Federation Partners

Operations > Managing Federation and External Access to Lync Server 2013 > Manage Access

Edge Configuration for Your Organization >

Topic Last Modified: *2013-02-23*

At the time you deployed your Edge Servers and enabled federation for your organization, you should have specified whether to support automatic discovery of federated partner domains. Use the procedure in this topic to change that configuration.

> **Note:**
>
> The following procedure assumes that you have already enabled federation for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation.

To enable or disable automatic discovery of federated domains for your organization

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, click **Access Edge Configuration**.
4. On the **Access Edge Configuration** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, under **Enable communications with federated users**, select or clear the **Enable partner domain discovery** check box to enable or disable automatic discovery of partner domains.
6. Click **Commit**.

To enable federated users to collaborate with users in your Lync Server deployment, you must have also configured at least one external access policy to support federated user access. For details, see Enable or Disable Federation and Public IM Connectivity in the Deployment documentation or the Operations documentation. For details about controlling access for specific federated domains, see Manage SIP Federated Domains for Your Organization, Manage SIP Federated Providers for Your Organization and Manage XMPP Federated Partners for Your Organization in the Operations documentation.

Enabling or Disabling Discovery of Federation Partners by Using Windows PowerShell Cmdlets

Discovery of federation partners can be managed by using Windows PowerShell and the Set-CsAccessEdgeConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable discovery of federation partners

- To enable discovery of federation partners, set the value of the **EnablePartnerDiscovery** property to True ($True). Note that you must enable DNS SRV routing in order to change this property value.

  ```
  Set-CsAccessEdgeConfiguration -UseDnsSrvRouting -EnablePartnerDiscovery
  ```

To disable discovery of federation partners

- To disable discovery of federation partners, set the value of the **EnablePartnerDiscovery** property to False ($False):

```
Set-CsAccessEdgeConfiguration -UseDnsSrvRouting -EnablePartnerDiscovery
```

1.7.11.2.3 Enable or Disable Sending an Archiving Disclaimer to Federated Partners

Enable or Disable Sending an Archiving Disclaimer to Federated Partners

Deployment > Deploying Archiving > Configuring Support for Archiving >

Topic Last Modified: *2013-02-23*

At the time you deployed your Edge Servers and enabled federation for your organization, you should have specified whether to automatically send the archiving disclaimer to federated partners. If you archive external communications, you should enable the sending of an archiving disclaimer. Use the procedure in this topic to change that configuration.

Note:

The following procedure assumes that you have already enabled federation for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation.

To enable or disable sending of an archiving disclaimer to federated partners

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, click **Access Edge Configuration**.
4. On the **Access Edge Configuration** tab, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, under **Enable communications with federated users**, select or clear the **Send archiving disclaimer to federated partners** check box to enable or disable automatically sending the archiving disclaimer.
6. Click **Commit**.

To enable federated users to collaborate with users in your Lync Server 2013 deployment, you must have also configured at least one external access policy to support federated user access. For details, see Manage XMPP Federated Partners for Your Organization in the Deployment documentation or the Operations documentation. For details about controlling access for specific federated domains, see Configure Support for Allowed External Domains in the Deployment documentation or Operations documentation.

Enabling or Disabling the Archiving Disclaimer by Using Windows PowerShell

Cmdlets

The use of the archiving disclaimer can be managed by using Windows PowerShell and the Set-CsAccessEdgeConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To enable the archiving disclaimer

- To enable the archiving disclaimer, set the value of the **EnableArchivingDisclaimer** property to True ($True):

```
Set-CsAccessEdgeConfiguration -EnableArchivingDisclaimer $True
```

⊟To disable the archiving disclaimer

- To disable the archiving disclaimer, set the value of the **EnableArchivingDisclaimer** property to False ($False):

```
Set-CsAccessEdgeConfiguration -EnableArchivingDisclaimer $False
```

1.7.11.2.4 Enable or Disable Remote User Access

Enable or Disable Remote User Access

Deployment > Deploying External User Access > Configuring Support for External User Access >

Topic Last Modified: *2013-02-23*

Remote users are users in your organization who have a persistent Active Directory identity within the organization. Remote users often sign in to Lync Server from outside your network by using a virtual private network (VPN) when they are not connected to your organization’s network. Remote users include employees working at home or on the road and other remote workers, such as trusted vendors, who have been granted enterprise credentials. If you enable remote user access for remote users, supported remote users connect over the Internet and do not have to connect using a VPN in order to collaborate with internal users using Lync Server.

To support remote user access, you must enable remote user access. When you enable remote user access, you enable it for your entire organization. If you later want to temporarily or permanently prevent remote user access, you can disable it for your organization. Use the procedure in this section to enable or disable remote user access for your organization.

Note:

Enabling remote user access only specifies that your servers running the Access Edge service support communications with remote users, but remote users cannot participate in instant messaging (IM) or conferences in your organization until you also configure at least one policy to manage the use of remote user access. Lync Server policy settings that are applied at one policy level can override settings that are applied at another policy level. Lync Server policy precedence is: User policy (most influence) overrides a Site policy, and then a Site policy overrides a Global policy (least influence). This means that the closer the policy setting is to the object that the policy is affecting, the more influence it has on the object. For details about configuring policies for the use of remote user access, see Configure Policies to Control Remote User Access.

To enable or disable remote user access for your organization

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Federation and External Access**, and then click **Access Edge Configuration**.
4. On the **Access Edge Configuration** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, do one of the following:
    - To enable remote user access for your organization, select the **Enable remote user access** check box.
    - To disable remote user access for your organization, clear the **Enable remote user access** check box.
6. Click **Commit**.

To enable remote users to sign in to your servers running Lync Server, you must also configure at least one external access policy to support remote user access. For details, see Configure Policies to Control Remote User Access in the Deployment documentation or the Operations documentation.

Enabling or Disabling Remote User Access by Using Windows PowerShell Cmdlets

Remote user access can be managed by using Windows PowerShell and the Set-CsAccessEdgeConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable remote user access

- To enable remote user access, set the value of the **AllowOutsideUsers** property to True ($True):

```
Set-CsAccessEdgeConfiguration -AllowOutsideUsers $True
```

To disable remote user access

- To disable remote user access, set the value of the **AllowOutsideUsers** property to False ($False):

```
Set-CsAccessEdgeConfiguration -AllowOutsideUsers $False
```

1.7.11.2.5 Enable or Disable Anonymous User Access

Enable or Disable Anonymous User Access

See Also

Deployment > Deploying External User Access > Configuring Support for External User Access >

Topic Last Modified: *2013-02-23*

Anonymous users are users who do not have a user account in your organization's Active Directory Domain Services (AD DS) or in a supported federated domain, but can be invited to participate remotely in an on-premises conference. By allowing anonymous participation in meetings you enable anonymous users (that is, users whose identity is verified through the meeting or conference key only) to join meetings. Allowing anonymous participation requires enabling it for your organization.

If you later want to temporarily or permanently prevent access by anonymous users, you can disable it for your organization. Use the procedure in this section to enable or disable anonymous user access for your organization.

Note:

By enabling anonymous user access for your organization you are only specifying that your servers running the Access Edge service support access by anonymous users. Anonymous users cannot participate in any meetings in your organization until you also configure at least one conferencing policy and apply it to one or more users or user groups. The only users that can invite anonymous users to meetings are those users that are assigned a conferencing policy that is configured to support anonymous users. For details about configuring conferencing policies to support inviting anonymous users, see Conferencing Policies.

To enable or disable anonymous user access for your organization

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **Access Edge Configuration**.
4. On the **Access Edge Configuration** page, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, do one of the following:
   - To enable anonymous user access for your organization, select the **Enable communications with anonymous users** check box.
   - To disable anonymous user access for your organization, clear the **Enable communications with anonymous users** check box.
6. Click **Commit**.

Enabling or Disabling Anonymous User Access by Using Windows PowerShell Cmdlets

You can manage anonymous user access by using Windows PowerShell and the **Set-CsAccessEdgeConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable anonymous user access

- To enable anonymous user access, set the value of the **AllowAnonymousUsers** property to True ($True):

```
Set-CsAccessEdgeConfiguration -AllowAnonymousUsers $True
```

To disable anonymous user access

- To disable anonymous user access, set the value of the **AllowAnonymousUsers** property to False ($False):

```
Set-CsAccessEdgeConfiguration -AllowAnonymousUsers $False
```

See Also

Concepts

Conferencing Policy Settings Reference

1.7.11.2.6 Assign Conferencing Policies to Support Anonymous Users

Assign Conferencing Policies to Support Anonymous Users

Deployment > Deploying External User Access > Configuring Support for External User Access >

Topic Last Modified: *2012-10-19*

By default, all users are prevented from inviting anonymous users to participate in a meeting. You control who can invite anonymous users by configuring a conferencing policy to support anonymous users, and applying that conferencing policy to specific users. For details about how to configure a conferencing policies to support anonymous users, see Create or Modify a Conferencing Policy and Managing Federation and External Access to Lync Server 2013.

Use the procedure in this section to apply a conferencing policy that you have already created to one or more users or user groups.

Note:

In addition to configuring and applying a policy to enable users to invite anonymous users, you must also enable support for anonymous users for your organization. For details, see Configure Policies to Control Public User Access.

To configure a user policy for anonymous participation in meetings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Conferencing**, and then do one of the following:
   3.a.To create a new user policy, click **New**, and then click **User policy**. Create a unique name in the **Name** field that indicates what the user policy covers (for example, **EnableAnonymous** for a user policy that enables communications with anonymous users).
   3.b.To configure an existing user policy, click the appropriate policy listed in the table, click **Edit**, and then click **Show details**.
4. In the **Conferencing Policies** dialog box, select the **Allow participants to invite anonymous users** check box.
5. Click **Commit**.
6. In the left navigation bar, click **Users**, search on the user account that you want to configure.
7. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
8. In **Edit Lync Server User** under **Conferencing policy**, select the user policy with the anonymous user access configuration that you want to apply to this

user.

> **Note:**
> The **<Automatic>** settings apply the default server installation settings and are applied automatically by the server.

To enable users to invite anonymous users to conferences, you must also enable support for anonymous users in your organization. For details, see Configure Policies to Control Public User Access in the Deployment documentation or the Operations documentation.

1.7.11.3 Manage SIP Federated Domains for Your Organization

Manage SIP Federated Domains for Your Organization

See Also

Microsoft Lync Server 2013 > Operations > Managing Federation and External Access to Lync Server 2013 >

Topic Last Modified: *2012-10-19*

This is preliminary documentation and is subject to change. Blank topics are included as placeholders.

To manage and configure SIP domains that you can federate with, you can do the following:

- Create or edit an allowed domain list of SIP federated partner domains.
- Create or edit a blocked domain list of SIP federated domains.

To perform these tasks, use the procedures in this this section.

- Configure Support for Allowed External Domains
- Configure Support for Blocked External Domains

See Also

Tasks

Configure Policies to Control Federated User Access
Enable or Disable Federation and Public IM Connectivity
Enable or Disable Discovery of Federation Partners

1.7.11.3.1 Configure Support for Allowed External Domains

Configure Support for Allowed External Domains

Operations > Managing Federation and External Access to Lync Server 2013 > Manage SIP Federated Domains for Your Organization >

Topic Last Modified: *2012-10-19*

If you have configured support for federated partners, you can manage which specific domains can federate with your organization. You configure one or more specific external domains as allowed federated domains. To do this, add each domain to the list of allowed domains. Even if partner discovery is enabled for your organization, do this if the domain is a federated partner that might need to communicate with more than 1,000 of your users or might need to send more than 20 messages per second. If partner discovery is not enabled for your organization, only users of external domains that you add to the allowed domains list can participate in IM and conferencing with users in your organization. If you want to restrict access for a federated domain to a specific server running the Access Edge service of the federated partner, you can specify the domain name of the server running the Access Edge service for each domain in the list of allowed domains.

> **Note:**
>
> This procedure describes how to configure support for specific domains, but implementing support for federated users also requires that you enable support for federated users for your organization, and configure and apply policies to control which users can collaborate with federated users. For details about enabling support for federated users, see Enable or Disable Remote User Access. For details about configuring policies to control federation, see Configure Policies to Control Federated User Access.

⊟To add an external domain to the list of allowed domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, and then click **Federated Domains**.
4. On the **Federated Domains** page, click **New**, and then click **Allowed domain**.
5. In **New Federated Domains**, do the following:
   - In **Domain name (or FQDN)**, type the name of the federated partner domain.

     > **Note:**
     >
     > This name must be unique and cannot already exist as an allowed domain for this server running the Access Edge service. The name cannot exceed 256 characters in length.
     > The search on the federated partner domain name performs a suffix match. For example, if you type **contoso.com**, the search will also return the domain **it.contoso.com**.
     > A federated partner domain cannot simultaneously be blocked and allowed. Lync Server 2013 prevents this from happening so that you do not have to synch up your lists.

   - If you want to restrict access for this federated domain to users of a specific server running the Access Edge service, in **Access Edge service (FQDN)**, type the FQDN of the federated domain’s server running the Access Edge service.
   - If you want to provide additional information, in **Comment**, type information that you want to share with other system administrators about this configuration.
6. Click **Commit**.
7. Repeat steps 4 through 6 for each federated partner domain that you want to allow.

To enable federated user access, you must also enable support for federated user access in your organization. For details, see Enable or Disable Remote User Access.

Additionally, you must configure and apply the policy to users that you want to be able to collaborate with federated users. For details, see Configure Policies to Control Federated User Access.

1.7.11.3.2 Configure Support for Blocked External Domains

Configure Support for Blocked External Domains

Operations > Managing Federation and External Access to Lync Server 2013 > Manage SIP Federated Domains for Your Organization >

Topic Last Modified: *2012-09-08*

If you have configured support for federated partners, you can manage which domains will be blocked from federating with your organization. The list of blocked domains will act as a block list (listing of explicit entries that are not to be allowed) and will apply in federated domain discovery, if you have this option enabled. For details, see Enable or Disable Discovery of Federation Partners.

Block one or more external domains from connecting to your organization. To do this, add the domain to the list of blocked domains.

⊟ To add an external domain to the list of blocked domains

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**.
4. Click **Federated Domains**, click **New**, and then click **Blocked domain**.
5. In **New Federated Domains**, do the following:
   - In **Domain name (or FQDN)**, type the name of the federated partner domain that you want to block.

     > **Note:**
     > The name cannot exceed 256 characters in length.
     > The search on the federated partner domain name performs a suffix match. For example, if you type **contoso.com**, the search will also return the domain **it.contoso.com**.
     > A federated partner domain cannot simultaneously be blocked and allowed. Lync Server 2013 prevents this from happening so that you do not have to synch up your lists.

   - (Optional) In **Comment**, type information that you want to share with other system administrators about this configuration.
6. Click **Commit**.
7. Repeat steps 4 through 6 for each federated partner that you want to block.

To enable federated user access, you must also enable support for federated user access in your organization. For details, see Enable or Disable Remote User Access.

Additionally, you must configure and apply the policy to users that you want to be able to collaborate with federated users. For details, see Configure Policies to Control Federated User Access.

1.7.11.4 Manage SIP Federated Providers for Your Organization

Manage SIP Federated Providers for Your Organization

Microsoft Lync Server 2013 > Operations > Managing Federation and External Access to Lync Server 2013 >

Topic Last Modified: *2012-10-19*

This is preliminary documentation and is subject to change. Blank topics are included as placeholders.

To configure support for users of SIP federated providers, you need to do the following:

- Configure one or more external user access policies to support communicating with SIP federated provider contacts
- Specify which hosted providers you want to support
- Specify which public IM providers you want to support

To perform these tasks, use the procedures in this section.

- Create or Edit Public SIP Federated Providers
- Create or Edit Hosted SIP Federated Providers

1.7.11.4.1 Create or Edit Public SIP Federated Providers

Create or Edit Public SIP Federated Providers

See Also

Operations > Managing Federation and External Access to Lync Server 2013 > Manage SIP Federated Providers for Your Organization >

Topic Last Modified: *2012-10-19*

Public instant messaging (IM) connectivity enables users in your organization to use IM to communicate with users of IM services provided by public IM service providers, including the Windows Live Messenger, Yahoo!, and AOL.

Lync Server 2013 has public provider configurations for America Online, Windows Live and Yahoo! instant messaging. Each public provider is configured with the provider's Edge server fully qualified domain name, and the default verification level **Allow users to communicate only with people on their Contacts list who use this provider**.

As a default setting, none of the public providers are enabled. You should complete license agreement and provisioning work before enabling the public providers. You can enable the provider before completing the licensing and provisioning work. Users will not be able to communicate with contacts on those providers until the pre-requisite work is completed. For details on licensing and provisioning of public providers, see Configure Policies to Control Public User Access.

Use the following procedure to create or edit Public providers:

⊟To create or edit public providers

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Federation and External Access**, and then click **SIP Federated Providers**.
4. If you need to create a new Public provider, click **New** and then click **Public provider**.
5. If you need to edit an entry from the list of Public providers, select a public provider, click **Edit**, then click **Show details**.
6. On the **Edit SIP Federated Provider** page, you can type or edit the following

settings:

- **Enable communications with this provider** Selecting this setting enables IM with this provider's users.
- **Provider name:** A required property, type the name of the provider as it will be reflected in the listing of SIP Federated Providers.
- **Access Edge service (FQDN):** A required property, type the fully qualified domain name of the Access Edge service of the provider that you are configuring. This information is provided as a default item, and should only be changed if the public provider makes a change to the FQDN of the Access Edge service at the public provider.
- **Default verification level:** The default setting, **Allow users to communicate with people on their Contacts list who use this provider** will limit communication to contacts that you have accepted and are in your contact list.

  Selecting **Allow users to communicate with everyone using this provider** removes the restriction that you must have received and accepted a contact invite. This setting does not limit who can contact you from the public provider's network.

7. When you are done configuring the settings, click **Commit** to save, or click **Cancel** to discard your changes.

Tasks

Configure Policies to Control Public User Access
Enable or Disable Federation and Public IM Connectivity

1.7.11.4.2 Create or Edit Hosted SIP Federated Providers

Create or Edit Hosted SIP Federated Providers

See Also

Operations > Managing Federation and External Access to Lync Server 2013 > Manage SIP Federated Providers for Your Organization >

Topic Last Modified: *2012-10-19*

Hosted provider instant messaging (IM) connectivity enables users in your organization to use IM to communicate with users of IM services provided by hosted providers, including the Microsoft Office 365 and Lync Online.

Each hosted provider is configured with the provider's Edge server fully qualified domain name, and the default verification level **Allow users to communicate only with people on their Contacts list who use this provider**.

Use the following procedure to create or edit Hosted providers:

⊟To create or edit hosted providers

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Federation and External Access**, and then click **SIP Federated Providers**.
4. If you need to create a new Hosted provider, click **New** and then click **Hosted provider**.
5. If you need to edit an entry from the list of Hosted providers, select a hosted provider, click **Edit**, then click **Show details**.

6. On the **Edit SIP Federated Provider** page, you can type or edit the following settings:
   - **Enable communications with this provider** Selecting this setting enables communications with this provider's users.
   - **Provider name:** A required property, type the name of the provider as it will be reflected in the listing of SIP Federated Providers.
   - **Access Edge service (FQDN):** A required property, type the fully qualified domain name of the Access Edge service of the hosted provider that you are configuring. This information should be provided by the hosted provider, and should only be changed if the hosted provider makes a change to the FQDN of the Access Edge service at the hosted provider.
   - **Default verification level:** The default setting, **Allow users to communicate with people on their Contacts list who use this provider** will limit communication to contacts that you have accepted and are in your contact list.

     Selecting **Allow users to communicate with everyone using this provider** removes the restriction that you must have received and accepted a contact invite. This setting does not limit who can contact you from the hosted provider's network.
7. When you are done configuring the settings, click **Commit** to save, or click **Cancel** to discard your changes.

Tasks

Configure Policies to Control Public User Access
Enable or Disable Federation and Public IM Connectivity

1.7.11.5 Manage XMPP Federated Partners for Your Organization

Manage XMPP Federated Partners for Your Organization

Microsoft Lync Server 2013 > Operations > Managing Federation and External Access to Lync Server 2013 >

Topic Last Modified: *2012-10-19*

This is preliminary documentation and is subject to change. Blank topics are included as placeholders.

To manage support for users of XMPP federated domains, you need to do the following:

- Configure one or more external access policies to support users of XMPP federated domains.
- Configure Access Edge Configuration policy to support federation.
- Create XMPP Federated Partners definitions.
- Understand negotiation settings available for XMPP federation.

To perform these tasks, use the procedures in this this section.

- Create or Edit XMPP Partner Configuration
- Negotiation Settings for XMPP Federated Partners
- Example XMPP Configuration – XMPP Federation with Google Talk

1.7.11.5.1 Create or Edit XMPP Partner Configuration

Create or Edit XMPP Partner Configuration

Operations > Managing Federation and External Access to Lync Server 2013 > Manage XMPP Federated Partners for Your Organization >

Topic Last Modified: *2012-11-01*

Microsoft Lync Server 2013 integrates an Extensible Messaging and Presence Protocol (XMPP) proxy on the Edge Server and an XMPP Gateway on the Front End Server or Front End pool. To allow connections from other XMPP deployments, you must configure XMPP in the Lync Server Control Panel. You configure settings on an XMPP domain basis. To create a new partner association, you do the following:

⊟To create a new federated partner or edit an existing configuration

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Federation and External Access**, and then click **XMPP Federated Partners**.
4. To create a new configuration, click **New**
5. To edit an existing configuration, select the configuration and click **Edit**
6. To create or edit configurations for **XMPP Federated Partners**, you define the following settings:
7. **Primary domain** (Required). The primary domain is the base domain of the XMPP partner. For example, you would enter **fabrikam.com** for the XMPP partner domain name. This is a required entry.
8. **Description** The description is for notes or other identifying information for this particular configuration. This entry is optional.
9. **Additional domains** Additional domains are domains that are a part of your XMPP partner's domain that should be included as part of the allowed XMPP communication. For example, if the primary domain is **fabrikam.com**, then you would list all other domains that are under fabrikam.com that you will communicate with by way of XMPP. For example, you might enter **corp.fabrikam.com** and **it.fabrikam.com** for the Corporate XMPP domain and the Information Technologies XMPP domain under fabrikam.com's main XMPP domain.
10. **Partner type** The **Partner type** is a required setting and gives you a selection of three choices in a drop-down menu. You must choose one of the following to describe and enforce what contacts can be added. You can select from:
    - **Federated** A **Federated** partner type is a trusted connection between a Lync Server or Office Communications Server 2007 R2 partner deployment.
    - **Public verified** A **Public verified** partner is when contacts that are part of a deployment that are verified by the provider can be added to your user's list of contacts. Invites can be sent from the Lync user or the Lync user can accept invites from the partner contact.
    - **Public unverified** A **Public unverified** relationship implies that there is no established and verifiable status between the two deployments. A Lync user must invite the unverified contact for that contact to be able to add the Lync user to his contact list. For example, Google GTalk is not a public verified XMPP service as it relates to Lync Server. A GTalk user will not be able to add the Lync user as a contact unless there is an explicit invite sent from the Lync user.
11. Notes on stream negotiation and the security methods Transport Layer Security (TLS) and Software Authentication and Security Layer (SASL):

    The **XMPP Standards Foundation** (XSF) and the **Internet Engineering Task Force** (IETF) define a set of rules and standards for using and managing TLS client certificates, TLS server certificates, and the SASL mechanism. Using TLS and SASL is the required process for securing the XMPP stream. From the XMPP Standards document **XEP-0178**, "specifies a recommended protocol flow for use of the SASL EXTERNAL mechanism with PKIX certificates, especially when an XMPP service indicates that TLS is mandatory-to-negotiate." PKIX, as stated in the XSF documentation, refers to public key infrastructure, also known as PKI.

Refer to the XSF document XEP-0178 for more details on the XMPP requirements. For details, refer to "XEP-0178: Best Practices for Use of SASL EXTERNAL with Certificates". http://xmpp.org/extensions/xep-0178.html

Refer to the IETF document "Extensible Messaging and Presence Protocol (XMPP): Core", Section 5.0, STARTTLS Negotiation http://tools.ietf.org/html/rfc6120.

- **TLS Negotiation** Defines the TLS negotiation rules. An XMPP service can require TLS, can make TLS optional, or you define that TLS is not supported. Choosing Optional leaves the requirement up to the XMPP service for a mandatory-to-negotiate decision. To view all possible settings and details for SASL, TLS and Dialback negotiation –including not valid and known error configurations - see Negotiation Settings for XMPP Federated Partners.
  - **Required** The XMPP service requires TLS negotiation.
  - **Optional** The XMPP service indicates that TLS is mandatory-to-negotiate.
  - **Not Supported** The XMPP service does not support TLS.
- **SASL negotiation** Defines the SASL negotiation rules. An XMPP service can require SASL, can make SASL optional, or you define that SASL is not supported. Choosing Optional leaves the requirement up to the partner XMPP service for a mandatory-to-negotiate decision.

  > ⚠**Warning:**
  >
  > SASL requires TLS. To use SASL, TLS must either be required or optional. Any configuration that defines SASL as either required or optional must have TLS support. When clicking **Commit** to save your changes, if you have not set TLS to required or optional, you will be warned that SASL must have TLS support and your changes are not saved. To resolve the error, set TLS to **Required** or **Optional**. If use of SASL is optional and TLS negotiation support is not possible, you must set SASL negotiation to **Not Supported**. Confirm with the XMPP service what the proper negotiation streams must be for TLS and SASL or service interruption will occur.

  - **Required** The XMPP service requires SASL negotiation.
  - **Optional** The XMPP service indicates that SASL is mandatory-to-negotiate.
  - **Not Supported** The XMPP service does not support SASL.
- **Dialback negotiation** Dialback negotiation is defined by the XSF in document **XEP-220 : Server Dialback** http://xmpp.org/extensions/xep-0220.html. The server dialback process uses the domain name system (DNS) and an authoritative server to verify that the request came from a valid XMPP partner. To do this, the originating server creates a message of a specific type with a generated dialback key and looks up the receiving server in DNS. The originating server sends the key in an XML stream to the resulting DNS lookup, presumably the receiving server. On receipt of the key over the XML stream, the receiving server does not respond to the originating server, but sends the key to a known authoritative server. The authoritative server verifies that the key is either valid or not valid. If not valid, the receiving server does not respond to the originating server. If the key is valid, the receiving server informs the originating server that the identity and key is valid and the conversation can commence.

  There are two valid states for **Dialback negotiation**:

  - **True** The XMPP server is configured to use Dialback negotiation if a request should be received from an originating server

- **False** The XMPP server is not configured to use Dialback negotiation and if a request should be received from an originating server, it will be ignored

1.7.11.5.2 Negotiation Settings for XMPP Federated Partners

Negotiation Settings for XMPP Federated Partners

Operations > Managing Federation and External Access to Lync Server 2013 > Manage XMPP Federated Partners for Your Organization >

Topic Last Modified: *2012-10-21*

The settings for the negotiation types in the configuration of an XMPP Partner have a wide variety of possible combinations. Not all of these combinations are valid. The table detailed in this topic will define the valid and not valid settings. Common configurations are presented in the first table, the second table detailing all possible combinations. Note that you cannot have *Simple Authentication and Security Layer* (SASL) **unless** *Transport Layer Security* (TLS) is also available. SASL is sent in an unencrypted (readable) format and should never be transmitted unless protected by another means, such as TLS.

Common XMPP Federation Negotiation Methods

Transport Layer Security (TLS)	Simple Authentication and Security Layer (SASL)	Dialback Authentication	Expected Authentication Method(s)	Notes
Required	Required	False	SASL over TLS	TLS and SASL required helps to ensure that the SASL message stream is secure. Dialback is not available and cannot be used for a fallback method if the XMPP federated partner has not set TLS to required or optional.
Required	Optional	True	SASL over TLS, TLS Dialback, TCP Dialback	By requiring TLS, if the XMPP federated partner has set SASL to optional or required SASL is used. If SASL is not available, Dialback over TLS will be used.
Optional	Optional	True	SASL over TLS, TLS Dialback, TCP Dialback	While very flexible in the negotiation methods offered, these settings

				rely on the XMPP federation partner’s settings. If the partner has TLS optional or required but SASL is not supported, TLS Dialback will be available. If the partner has TLS and SASL set to optional or required, the optimal selection of TLS over SASL is used.
Not Supported	Not Supported	True	TCP Dialback	In many cases, TCP Dialback is the only possible solution. Less desirable than other options, it does provide some level of trust.

XMPP Federation Negotiation Methods Matrix - Complete

Transport Layer Security (TLS)	**Simple Authentication and Security Layer (SASL)**	**Dialback Authentication**	**Expected Authentication Method**	**Notes, Warning or Error for Not Valid Configuration**
Required	Required	True	SASL over TLS	⚠**Warning:** Dialback will not operate if both SASL and TLS are required.
Required	Required	False	SASL over TLS	
Optional	Required	True	SASL over TLS, TLS Dialback, TCP Dialback	⚠**Warning:** SASL requires TLS. Allowing TLS to be optional may result in failed session negotiations.
Optional	Required	False	SASL over TLS	⚠**Warning:** SASL requires TLS. Allowing TLS to be optional may result in failed session negotiations.

Not Supported	Required	True	TCP Dialback	⚠ **Warning:** SASL requires TLS. Allowing TLS to be optional may result in failed session negotiations.
Not Supported	Required	False	⚠ **Warning:** Not Valid Configuration	⚠ **Warning:** Because SASL requires TLS, and TLS is not available, SASL/ TLS cannot succeed. TCP Dialback is set to false, and cannot be used.
Required	Optional	True	SASL over TLS, TLS Dialback	
Required	Optional	False	SASL over TLS	
Optional	Optional	True	SASL over TLS, TLS Dialback, TCP Dialback	⚠ **Warning:** SASL requires TLS. Allowing TLS to be optional may result in failed session negotiations.
Optional	Optional	False	SASL over TLS	⚠ **Warning:** SASL requires TLS. Allowing TLS to be optional may result in failed session negotiations.
Not Supported	Optional	True	TCP Dialback	⚠ **Warning:** SASL requires TLS. Allowing TLS to be optional may result in failed session negotiations.
Not Supported	Optional	False	⚠ **Warning:** Not Valid Configuration	⚠ **Warning:** SASL requires TLS. Allowing TLS to be optional may result in failed session negotiations.
Required	Not Supported	True	TLS Dialback	Configuration

				allows for TLS Dialback.
Required	Not Supported	False	Not Valid Configuration	⚠**Warning:** SASL or Dialback must be enabled.
Optional	Not Supported	True	TLS Dialback, TCP Dialback	Based on negotiation choices of the other end point, TCP or TLS Dialback will be accepted.
Optional	Not Supported	False	Not Valid Configuration	⚠**Warning:** SASL or Dialback must be enabled.
Not Supported	Not Supported	True	TCP Dialback	TCP Dialback is the only negotiation method available
Not Supported	Not Supported	False	Not Valid Configuration	⚠**Warning:** SASL or Dialback must be enabled.

1.7.11.5.3 Example XMPP Configuration â€“ XMPP Federation with Google Talk

Example XMPP Configuration – XMPP Federation with Google Talk

Operations > Managing Federation and External Access to Lync Server 2013 > Manage XMPP Federated Partners for Your Organization >

Topic Last Modified: *2012-11-01*

An example configuration for deploying the XMPP Proxy defines a federation with Google Talk.

⊟Example XMPP configuration – XMPP federation with Google Talk

1. On the Front End Server, open the Lync Server Deployment Wizard. Click **Install** or **Update Lync Server System**, then click **Setup** or **Remove Lync Server Components**. Click **Run Again**.
2. At **Setup Lync Server components**, click **Next**. The summary screen will show actions as they are executed. After the deployment is complete, click **View Log** to view available log files. Click **Finish** to complete the deployment.
3. On the Edge Server, open the Lync Server Deployment Wizard. Click **Install** or **Update Lync Server System**, then click **Setup** or **Remove Lync Server Components**. Click **Run Again**.
4. Add Google Talk as an XMPP allowed partner. Google Talk currently only supports unencrypted, TCP connections for server-to-server XMPP federation and only supports Server Dialback for identity verification. (See http://xmpp.org/extensions/xep-0220.html).

```
New-CsXmppAllowedPartner gmail.com -TlsNegotiation NotSupported -SaslN
```

5. To enable Edge Federation, type the following:

```
Set-CsAccessEdgeConfiguration -AllowFederatedUsers $true
```

6. At **Setup Lync Server components**, click **Next**. The summary screen will show actions as they are executed. After the deployment is done, click **View Log** to view available log files. Click **Finish** to complete the deployment.
7. On the Edge Server, in the Lync Server Deployment Wizard, next to **Step 3: Request, Install, or Assign Certificates**, click **Run again**.

> **Tip:**
>
> If you are deploying the Edge Server for the first time, you will see Run instead of Run Again.

8. On the **Available Certificate Tasks** page, click **Create a new certificate request**.
9. On the **Certificate Request** page, click **External Edge Certificate**.
10. On the **Delayed or Immediate Request** page, select the **Prepare the request now, but send it later** check box.
11. On the **Certificate Request File** page, type the full path and file name of the file to which the request is to be saved (for example, c:\cert_exernal_edge.cer).
12. On the **Specify Alternate Certificate Template** page, to use a template other than the default WebServer template, select the **Use alternative certificate template for the selected certification authority** check box.
13. On the **Name and Security Settings** page, do the following:
    13.a. In **Friendly name**, type a display name for the certificate
    13.b. In **Bit length**, specify the bit length (typically, the default of **2048**)
    13.c. Verify that the **Mark certificate private key as exportable** check box is selected
14. On the **Organization Information** page, type the name for the organization and the organizational unit (for example, a division or department)
15. On the **Geographical Information** page, specify the location information
16. On the **Subject Name/Subject Alternate Names** page, the information to be automatically populated by the wizard is displayed. If additional subject alternative names are needed, you specify them in the next two steps
17. On the **SIP Domain Setting on Subject Alternate Names (SANs)** page, select the domain check box to add a sip. <*sipdomain*> entry to the subject alternative names list.
18. On the **Configure Additional Subject Alternate Names** page, specify any additional subject alternative names that are required.

> **Tip:**
>
> If the XMPP proxy is installed, by default the domain name (such as contoso.com) is populated in the SAN entries. If you require more entries, add them in this step.

19. On the **Request Summary** page, review the certificate information to be used to generate the request.
20. After the commands finish running, you can **View Log**, or click **Next** to continue.
21. On the **Certificate Request File** page, you can view the generated certificate signing request (CSR) file by clicking **View** or exit the Certificate Wizard by clicking **Finish**.
22. Copy the request file and submit to your public certification authority.
23. After receiving, importing and assigning the public certificate, you must stop and restart the Edge Server services. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.. In the Lync Server Management Shell, type:

```
Stop-CsWindowsService
```

```
Start-CsWindowsService
```

24.To configure DNS for XMPP federation, you add the following SRV record to external DNS:_xmpp-server._tcp.<*domain name*> The SRV record will resolve to the access edge FQDN of the Edge server, with a port value of 5269

25.Configure a new External Access Policy to enable all users by opening the Lync Server Management Shell on a Front End Server and typing:

```
New-CsExternalAccessPolicy -Identity FedPic -EnableFederationAcces $tr
Get-CsUser | Grant-CsExternalAccessPolicy -PolicyName FedPic
```

1.7.11.6 Configuring Federation Support for a Lync Online Customer

Configuring Federation Support for a Lync Online Customer

Microsoft Lync Server 2013 > Operations > Managing Federation and External Access to Lync Server 2013 >

Topic Last Modified: *2012-11-01*

You can provide communications services to users in your organization in any of the following ways:

- Deploying Lync Server 2013 in your organization (known as *on-premises services*) and setting up Lync 2013 user accounts in your organization.
- Setting up a Microsoft Lync Online 2010 customer account with a Hosting Provider and setting up user accounts with the Hosting Provider (known as *online services*).

If you deploy Lync 2013 in your organization, you can federate with the domains of one or more Microsoft Lync Online 2010 customers. To enable federation between users of your on-premises Lync 2013 deployment and users of a Lync Online 2010 customer, you must configure support for the domain and users of the Lync Online customer.

Note:

This documentation describes only the procedures for configuring your organization to support federation with an Lync Online 2010 customer. This documentation does not describe the procedures for configuring the Lync Online 2010 customer to support federation. For details about Lync Online services, see Lync Online at http://go.microsoft.com/fwlink/p/?linkId=218941.

- Prerequisites for Federating with a Lync Online Customer
- Configure Federation Support for a Lync Online Domain
- Configure User Access for Federation with a Lync Online Customer
- Verify Communications with a Lync Online Customer

1.7.11.6.1 Prerequisites for Federating with a Lync Online Customer

Prerequisites for Federating with a Lync Online Customer

Operations > Managing Federation and External Access to Lync Server 2013 > Configuring Federation Support for a Lync Online Customer >

Topic Last Modified: *2012-10-19*

To federate with a Lync Online 2010 customer, you should have already completed initial deployment and configuration of Lync Server 2013 in your organization. This includes the following:

- Deploying at least one Standard Edition server or one Enterprise Edition Front End pool in your organization. For details about deploying internal servers, see Deploying Lync Server 2013 in the Deployment documentation.

- Enabling internal user accounts for Lync Server 2013. For details, see Disable or Re-Enable User Account for Lync Server in the Deployment documentation or the Operations documentation.
- Deploying at least one Edge Server and the other components required to support external user access. For details, see Managing Federation and External Access to Lync Server 2013 in the Deployment documentation.
- Enabling federation support within your organization and configuring the appropriate method for controlling access by federated domains. For details, see Enable or Disable Remote User Access and Manage SIP Federated Providers for Your Organization in the Operations documentation.
- Enabling external user access for users in your organization. For details, see Assign an External User Access Policy to a Lync Enabled User and in the Deployment documentation or Operations documentation.

1.7.11.6.2 Configure Federation Support for a Lync Online Domain

Configure Federation Support for a Lync Online Domain

Operations > Managing Federation and External Access to Lync Server 2013 > Configuring Federation Support for a Lync Online Customer >

Topic Last Modified: *2012-11-01*

Federating with a Microsoft Lync Online 2010 customer requires you to complete the following steps:

- Configure support for the domain of the Lync Online 2010 customer (for example, contoso.onmicrosoft.com). As specified in the Prerequisites for Federating with a Lync Online Customer section of this documentation, you should have already enabled federation for your organization. Enabling federation requires specifying the method to be used to control access by federated domains. If you configured your organization to use discovery, adding the domain to your organization’s allowed list is optional. If you did not enable domain discovery, then you must add the domain name of the Lync Online customer to your allowed domains list. You can add a domain name either by using Lync Server Control Panel or by running the **New-CSAllowedDomain** cmdlet. For details about using Lync Server Control Panel, including enabling discovery of domains, see Manage SIP Federated Providers for Your Organization in the Operations documentation. For details about using the **New-CSAllowedDomain** cmdlet to add a domain, see New-CsAllowedDomain in the Operations documentation.

Note:
A Lync Online customer can have multiple domains. If you want to federate with more than one of the domains, you must configure support for each individual domain with which you want to support federation, and the administrator of the Lync Online customer must enable federation for each of the domains to be federated.

- Configure support for the hosting provider of the Lync Online 2010 customer domain with which you want to federate. Use the procedure in this section to configure support for hosting provider.

Note:
This step is required only for federation with a domain of a Lync Online customer, not for federation with any domain that is deployed on-premises at a federated partner’s location.

⊟To configure support for a hosting provider

1. From a Front End Server, Start the Lync Server Management Shell: Click

Start, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.

2. Run the **New-CsHostingProvider** cmdlet to create and configure the hosting provider. For example, run:

```
New-CsHostingProvider -Identity LyncOnline -ProxyFqdn "sipfed.online.l
```

The preceding example sets the following parameters:

- **Identity** specifies a unique string value identifier for the hosting provider that you are creating. Note that the command will fail if an existing provider has already been configured with that Identity.
- **ProxyFQDN** specifies the fully qualified domain name (FQDN) for the proxy server used by the hosting provider. This value cannot be modified. If the hosting provider changes its proxy server you will need to delete and then recreate the entry for that provider.
- **VerificationLevel** specifies how (or if) messages sent from a hosting provider are verified to ensure that they were sent from that provider.
- **Enabled** indicates whether the network connection between your domain and the hosting provider is enabled. Messages cannot be exchanged between the two organizations until this value is set to **True**.
- **EnabledSharedAddressSpace** indicates whether the hosting provider is being used in a shared SIP address space (split domain) scenario.
- **HostsOCSUsers** indicates whether the hosting provider is used to host Lync Server accounts. If **False**, the provider hosts other account types, such as Microsoft Exchange accounts.
- **IsLocal** indicates whether the proxy server used by the hosting provider is contained within your Lync Server topology.

For details about using this cmdlet, see New-CsHostingProvider in the Operations documentation.

1.7.11.6.3 Configure User Access for Federation with a Lync Online Customer

Configure User Access for Federation with a Lync Online Customer

Operations > Managing Federation and External Access to Lync Server 2013 > Configuring Federation Support for a Lync Online Customer >

Topic Last Modified: *2012-11-01*

You must configure the user accounts of all the users in your organization in order for them be allowed to communicate with federated partners. This configuration is applied for all federated partners, including any Microsoft Lync Online 2010 customer domains with which you support federation. For details about configuring federation support for user accounts, see Configure Policies to Control Federated User Access and Assign an External User Access Policy to a Lync Enabled User in the Operations documentation.

1.7.11.6.4 Verify Communications with a Lync Online Customer

Verify Communications with a Lync Online Customer

Operations > Managing Federation and External Access to Lync Server 2013 > Configuring Federation Support for a Lync Online Customer >

Topic Last Modified: *2012-10-08*

To enable Lync users in your organization to communicate with users of a Microsoft Lync

Online 2010 customer, you must have completed the following steps:

- Met all prerequisites. This includes deploying your internal and edge servers, enabling federation support for your organization, and setting up user accounts. For details, see Prerequisites for Federating with a Lync Online Customer.
- Configured domain access support in your internal deployment. This includes creating a host provider entry and configuring your deployment to allow access from the Lync Online customer's domain. For details, see Configure Federation Support for a Lync Online Domain.
- Configured your user accounts to support federation. For details, see Configure User Access for Federation with a Lync Online Customer.

After you complete all of these steps and the administrator of the Lync Online 2010 customer completes all configuration of their online services to support federation with your organization, verify communications by testing communications between an internal user in your organization and a user of the Lync Online customer. If communication is not successful, use the Logging Tool from your Edge Server to capture log and trace files in order to troubleshoot the problem. For details about using the Logging Tool, see Open Lync Server Administrative Tools in the Operations documentation. For details about the Logging Tool, see the Lync Server 2010 Logging Tool documentation on the TechNet Library at http://go.microsoft.com/fwlink/p/?linkId=199265.

1.7.12 Managing Lync Server 2013 Archiving

Managing Lync Server 2013 Archiving

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-10-10*

When you deploy Archiving for your organization, you specify the initial configuration during deployment. However, there may be times when you want to change how you implement archiving support for day-to-day management or to meet new requirements in your organization. For example, you may need to set up archiving support differently for a specific site, pool, or users within your organization. For users homed on Lync Server 2013, you do this be creating and customizing archiving policies and configurations. If you use Microsoft Exchange integration, you must also configure Exchange 2013 settings. This section provides information and procedures to enable you to make changes to your Archiving deployment.

- How Archiving Works
- Managing the Archiving of Internal and External Communications
- Managing Archiving Configuration Options for Your Organization, Sites, and Pools
- Changing Archiving Database Options
- Exporting Archived Data

1.7.12.1 How Archiving Works

How Archiving Works

Microsoft Lync Server 2013 > Planning > Planning for Archiving >

Topic Last Modified: *2013-01-22*

Lync Server 2013 Archiving provides options to help you meet your compliance needs. To implement and maintain it in a way that most effectively meets your organization's requirements, you should understand:

- What information can be archived.
- How to enable and disable Archiving in your deployment.
- The archiving options that you can configure to control how Archiving is implemented.

What Information Can Be Archived?

The following types of content can be archived:

- Peer-to-peer instant messages
- Conferences (meetings), which are multiparty instant messages
- Conference content, including uploaded content (for example, handouts) and event-related content (for example, joining, leaving, uploading sharing, and changes in visibility)
- Whiteboards and polls shared during a conference

The following types of content are not archived:

- Peer-to-peer file transfers
- Audio/video for peer-to-peer instant messages and conferences
- Desktop and application sharing for peer-to-peer instant messages and conferences

Lync Server also does not archive Persistent Chat conversations. To archive Persistent Chat conversations, you must enable and configure the compliance service, which is a component that can be deployed with Microsoft Lync Server 2013, Persistent Chat Server. For details, see Planning for Persistent Chat Server in the Planning documentation.

How Do I Start Using Archiving?

Archiving is automatically installed on each Front End Server when you deploy the server, but Archiving is not enabled until you configure it. How you configure it is determined by how you deploy Archiving:

- **Archiving using Microsoft Exchange integration.** If you have users who are homed on Exchange 2013 and their mailboxes have been put on In-Place Hold, you can select the option to integrate Lync Server 2013 storage with Exchange storage. If you choose the Microsoft Exchange integration option, you use Exchange 2013 policies and configurations to control the archiving of Lync Server 2013 data for those users.
- **Archiving using Lync Server Archiving databases.** If you have users who are not homed on Exchange 2013 or who have not had their mailboxes put on In-Place Hold, or if you don’t want to use Microsoft Exchange integration for any or all users in your deployment, you can deploy Lync Server Archiving databases using SQL Server to store Archiving data for those users. In this case, Lync Server 2013 Archiving policies and configurations determine whether Archiving is enabled and how it is implemented. To use Lync Server 2013, you must add the appropriate SQL Server databases to your topology and publish the topology.

Archiving Setup When Using Microsoft Exchange Integration

If your users are homed on Exchange 2013 and their mailboxes have been put on In-Place Hold, you can choose the **Microsoft Exchange integration** option (as described later in this section) to archive Lync Server 2013 for those users, and then you control archiving for those users by specifying Exchange In-Place Hold policies and settings, as well as Lync Server configurations to control the following:

- Whether to archive IM, conferencing, or both.
- Whether to implement critical mode for your Lync Server deployment.
- Selection of the Microsoft Exchange integration option to use Exchange 2013

for storage of archived data.

These Lync Server 2013 Archiving configuration options are described later in this section. For information about how to configure Exchange In-Place Hold policies and settings to support archiving, see the Exchange 2013 product documentation.

Archiving Setup When Using Lync Server Archiving Database Storage

If you want to use Lync Server Archiving databases (using SQL Server databases) to archive data for any users in your deployment, you can configure Lync Server Archiving policies to control whether Archiving is enabled for those users. In each Archiving policy, you can enable or disable Archiving for either or both of the following:

- Internal communications
- External communications

By default, archiving is not enabled for internal communications or external communications in any Lync Server Archiving policy. You enable and disable communications using Lync Server 2013 Control Panel or using cmdlets in the Lync Server 2013 Management Shell.

Lync Server 2013 Archiving policies include the following:

- **Global Archiving policy**. This is the default Archiving policy and applies to your entire deployment. It is created when you deploy Lync Server 2013 and, by default, disables Archiving for both internal and external communications. You cannot delete this policy. If you choose the delete option, the global policy is reset to the default settings.
- **Site Archiving policy**. Optionally, you can enable or disable Archiving for one or more specific sites by creating and configuring a site-level Archiving policy for the site. When you create a site-level Archiving policy, by default, archiving is not enabled. You can delete any site-level Archiving policy that you create. A site-level Archiving policy overrides the global policy, but only for the site specified in the policy. For example, if you enable Archiving for internal and external communications in your global policy and create a site policy in which you disable Archiving for external communications, only internal communications would be archived for that site.
- **User Archiving policy**. Optionally, you can enable or disable Archiving for one or more specific users and group of users by creating, configuring, and applying a user-level Archiving policy for the specified users and user groups. When you create a user-level Archiving policy, by default, archiving is not enabled. You can delete any user-level Archiving policy that you create, and you can change which users and group of users the Archiving policy applies to. A user-level Archiving policy overrides the global policy and any site policies, but only for the users and user groups to whom the policy is applied. For example, if you disable Archiving for internal and external communications in your global policy, create a site-level policy in which you enable Archiving for internal and external communications, and then create a user-level policy in which you disable Archiving for external communications, the communications would be archived for both external and internal communications for all site users except that, for the users to whom you apply the user-level policy, only internal communications would be archived.

For details about how to set up initial Archiving policies when you deploy Archiving, see Configuring and Assigning Archiving Policies in the Deployment documentation. For details about using Archiving policies to enable and disable communications after deployment, see Managing the Archiving of Internal and External Communications in the Operations documentation.

Note:

If you implement both Lync Server 2013 Archiving databases and enable Microsoft Exchange integration, Exchange 2013 policies override Lync Server Archiving policies, but

> only for users who are homed on Exchange 2013 and have had had their mailboxes put on In-Place Hold. Lync Archiving depends on Microsoft Exchange In-Place Hold policy only.

What Options Do I Have for Configuring Archiving?

In addition to using policies and to enable and disable Archiving, you have other Archiving options that can be configure for your entire deployment and, optionally, for specific sites and pools. You control most Archiving options by using one or more Archiving configurations, which are available in Lync Server 2013 Control Panel, but also have another option that is only available for configuration using Lync Server 2013 Management Shell.

Archiving Configuration Options Available in Lync Server 2013 Control Panel

Each archiving configuration provides the following options:

The global-level configuration is created automatically when you deploy archiving and can be configured, but not deleted. If you select the option to delete the global configuration, the settings are reset to the default values. You can create multiple site and pool configurations that, together with the global configuration, control archiving settings. For the global configuration and each site and pool configuration, you have the following options:

- Disable archiving, enable archiving only for instant messaging (IM), or enable archiving of both IM and conferencing.
- Configure critical mode to block IM and conferencing sessions in the event of a Lync Server failure. Failures include the following:
    - **IM**. A problem with the Lync Server storage service. In this case, IM is blocked for users who are enabled for Archiving.
    - **Conferencing**. A failure could be an unavailable file share or a problem with the storage service. In this case, all active conferences hosted in the pool at the time of failure are switched to restricted mode and new conferences cannot be activated.

    Both IM and conferencing automatically recover after the failures are corrected.
- Specify the use of Microsoft Exchange Server 2013 integration to use Exchange 2013 for storage of archived data, instead of setting up separate SQL Server databases for storage of Lync Server 2013 archiving data.
- Configure purging options for archived data. This includes specifying when to purge archived data, which can be either of the following:
    - After a specific number of days that you specify
    - After the archiving data has been exported (which includes data that has been uploaded to Exchange, if you enable Microsoft Exchange integration).

    > **Note:**
    >
    > If you enable Microsoft Exchange integration, purging for users homed on Exchange 2013 and with their mailboxes put on In-Place Hold is controlled by Exchange. The only qualification is for conferencing files, which are stored on the Lync Server file share. These files are purged from the file share only after the files have been exported (uploaded to Exchange), if you select the option to purge data after the archiving data has been exported, or after the specified maximum number of days, if you specify a maximum number of days for retention.

By default, no archiving options are enabled. You can manage Archiving configurations using Lync Server 2013 Control Panel.

You can specify the following Archiving configurations:

- **Global Archiving configuration**. This is the default Archiving configuration and applies to your entire deployment. It is created when you deploy Lync Server 2013 and, by default, does not enable archiving functionality. You can modify the global configuration, but you cannot delete it. If you choose the delete option for the configuration, the global configuration is reset to the default settings.

- **Site Archiving configuration**. Optionally, you can configure Archiving for one or more specific sites by creating and configuring a site-level Archiving configuration for an individual site. A site-level Archiving configuration exists only if you create it. You can modify or delete any site-level Archiving configuration. A site-level Archiving configuration overrides the global configuration, but only for the site specified in the site-level configuration. For example, if you enable Archiving for only IM in your global configuration and create a site configuration in which you enable Archiving for both IM and conferencing, conferencing would only be archived for the site, not for the remainder of your organization.
- **Pool Archiving configuration**. Optionally, you can specify Archiving settings for one or more specific pools by creating and configuring a pool-level configuration for the individual pool. A pool-level Archiving configuration exists only if you create it. You can modify and delete any pool-level Archiving configuration. A pool-level Archiving configuration overrides the global configuration and any site archiving configuration you may have created. For example, if you enable Archiving for only IM in your global configuration, create a site-level configuration in which you enable Archiving for both IM and conferencing for the site, and then create a pool-level configuration in which you enable Archiving only for IM, the communications would be archived for both IM and conferencing for all users of the site except the users homed in the pool specified in the pool-level configuration. For all other users in your organization, Archiving would be enabled only for IM.

For details about how to set up initial Archiving configurations when you deploy Archiving, see Configuring Archiving Options in the Deployment documentation. For details about using Archiving policies to enable and disable communications after deployment, see Managing Archiving Configuration Options for Your Organization, Sites, and Pools in the Operations documentation.

Archiving Options Available Only in Windows PowerShell

Using Lync Server 2013 Management Shell, you can use cmdlets to implement options that are not available in Lync Server 2013 Control Panel. These options include the following:

- **Archive duplicate messages**. For details, see New-CsArchivingConfiguration and Set-CsArchivingConfiguration in the Operations documentation.
- **Export archived data**. For details, see Export-CsArchivingData

How Do I Access Archived Data?

Access to archived data is dependent on where the data is stored:

- **Microsoft Exchange storage**. If you choose the SharePoint integration option, Lync Server deposits the archiving content in the Exchange 2013 store for all users who are homed on Exchange 2013, and who have had their mailboxes put on In-Place Hold. Archived data is stored in user mailboxes Recoverable items folder, which is generally invisible to users, and can only be searched by users with an Exchange **Discovery Management** role. Exchange enables federated search and discovery, along with SharePoint, if it is deployed. For more details about storage, retention, and discovery of data stored in Exchange, see the Exchange 2013 and SharePoint documentation.
- **Lync Server storage**. If you set up Lync Server 2013 Archiving databases for storage of Lync Server data, Lync Server deposits archiving content in the Lync Server Archiving databases (SQL Server databases) for any users not homed on Exchange 2013, and who have not had their mailboxes put on In-Place Hold. This data is not searchable, but it can be exported to formats that are searchable using other tools. For details about exporting data stored in Archiving databases, see Exporting Archived Data in the Operations documentation.

For more details about how Lync Server 2013 and Exchange 2013 work together, see Exchange Server and SharePoint Integration Support in the Supportability documentation.

1.7.12.2 Managing the Archiving of Internal and External Communications

Managing the Archiving of Internal and External Communications

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Archiving >

Topic Last Modified: *2012-10-09*

In Lync Server 2013, you use Archiving policies to enable and disable archiving for internal communications and external communications if you do not use Microsoft Exchange integration or you have users who are not homed on Exchange 2013 with their mailboxes put on In-Place Hold. This includes the following Archiving policies:

- A global policy that is created by default when you deploy Lync Server 2013.
- Optional site-level and user-level policies that you can create and use to specify how archiving is implemented for specific sites or users.

You initially set up Archiving policies when you deploy Archiving, but you can change, add, and delete policies after deployment. In Lync Server 2013 Control Panel, you can use the **Archiving Policy** page of the **Archiving and Monitoring** group to manage policies at the global level, site level, and user level. If you integrate your Lync Server storage with Exchange 2013 storage, the Exchange user policies take precedence over the Lync Server 2013 archiving policies.

For details about how policies are implemented, including the hierarchy of policies, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

To control the implementation of Archiving, you must specify options in Archiving configurations, such as whether to archive IM or conferencing, the use of critical mode, and purging options. By default no options are enabled in the global Archiving configuration or any site or pool Archiving configuration. You should specify all appropriate options in the Archiving configurations before enabling Archiving for internal or external communications in the Archiving policies. For details, see Managing Archiving Configuration Options for Your Organization, Sites, and Pools in the Operations documentation.

If you enable Microsoft Exchange integration for your deployment, Exchange policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.

- Creating an Archiving Policy to Enable or Disable Archiving of Internal or External Communications for Specific Sites or Users
- Changing an Archiving Policy to Enable or Disable Archiving of Internal or External Communications for Your Organization, Sites, or Users
- Applying an Archiving Policy to Users
- Setting Up Policies for Archiving When Using Exchange Server Integration
- Deleting an Archiving Policy

Creating an Archiving Policy to Enable or Disable Archiving of Internal or External Communications for Specific Sites or Users

See Also

Operations > Managing Lync Server 2013 Archiving > Managing the Archiving of Internal and External Communications >

Topic Last Modified: *2013-02-23*

In Lync Server 2013, you use policies to enable and disable archiving for internal communications and external communications for users homed on Lync Server 2013. This includes the following Archiving policies:

- A global policy that is created by default when you deploy Lync Server 2013.
- Optional site-level and user-level policies that you can create and use to specify how archiving is implemented for specific sites or users.

You initially set up Archiving policies when you deploy Archiving, but you can change, add, and delete policies after deployment. In Lync Server 2013 Control Panel, you can use the **Archiving Policy** page of the **Archiving and Monitoring** group to manage policies at the global level, site level, and user level. If you integrate your Lync Server storage with Exchange 2013 storage, the Exchange user policies take precedence over the Lync Server 2013 archiving policies.

For details about how policies are implemented, including the hierarchy of policies, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

To control the implementation of Archiving, you must specify options in Archiving configurations, such as whether to archive IM or conferencing, the use of critical mode, and purging options. By default no options are enabled in the global Archiving configuration or any site or pool Archiving configuration. You should specify all appropriate options in the Archiving configurations before enabling Archiving for internal or external communications in the Archiving policies. For details, see Managing Archiving Configuration Options for Your Organization, Sites, and Pools in the Operations documentation.

If you enabled Microsoft Exchange integration for your deployment, Exchange policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.

⊟To create an archiving policy for a site or users

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. Click **New**, and then do one of the following:
   - To create a site-level archiving policy, click **Site policy** and then, in **Select a site**, click the site to which the policy is to be applied.
   - To create a user-level archiving policy, click **User policy**.

5. In **New Archiving Policy**, do the following:
   - In **Name**, specify a name for the new policy (for example, externalContoso).
   - In **Description**, provide details about what the policy is (for example, External user archiving policy for Contoso).
   - To control archiving of communications with internal users, select or clear the **Archive internal communications** check box.
   - To control archiving of communications with external users, select or clear the **Archive external communications** check box.
6. Click **Commit**.

> **Important:**
> The settings of a user policy only apply to the specific users and user groups to which you apply the policy. For details, see Applying an Archiving Policy to Users

Creating an Archiving Policy by Using Windows PowerShell Cmdlets

Archiving policies can be created by using Windows PowerShell and the **Remove-CsArchivingPolicy** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To create a new archiving policy at the site scope

- This command creates a new archiving policy for the Redmond site:

```
New-CsArchivingPolicy -Identity "site:Redmond"
```

To create a new archiving policy at the per-user scope

- To create a new archiving policy at the per-user scope, simply specify a unique Identity when creating the policy:

```
New-CsArchivingPolicy -Identity "RedmondArchivingPolicy"
```

To create a new archiving policy that enables archiving of internal communication sessions

- Because no parameters (other than the mandatory Identity parameter) were specified in the preceding commands, the new policies will use the default values for all their properties. To create policies that use different property values, simply include the appropriate parameter and parameter value. For example, to create an archiving policy that permits archiving of internal instant messaging sessions use a command like this:

```
New-CsArchivingPolicy -Identity "site:Redmond" -ArchiveInternal $True
```

To create a new archiving policy that enables archiving of both internal and external communication sessions

- Multiple property values can be modified by including multiple parameters. For example, this command configures the new policy to archiving both internal and external instant messaging sessions:

```
New-CsArchivingPolicy -Identity "site:Redmond" -ArchiveInternal $True -
```

For more information, see the help topic for the New-CsArchivingPolicy cmdlet.

See Also

Other Resources

Managing the Archiving of Internal and External Communications

1.7.12.2.2 Changing an Archiving Policy to Enable or Disable Archiving of Internal or External Communications for Your Organization, Sites, or Users

Changing an Archiving Policy to Enable or Disable Archiving of Internal or External Communications for Your Organization, Sites, or Users

See Also

Operations > Managing Lync Server 2013 Archiving > Managing the Archiving of Internal and External Communications >

Topic Last Modified: *2013-02-23*

In Lync Server 2013, you use policies to enable and disable archiving for internal communications and external communications for users homed on Lync Server 2013. This includes the following Archiving policies:

- A global policy that is created by default when you deploy Lync Server 2013.
- Optional site-level and user-level policies that you can create and use to specify how archiving is implemented for specific sites or users.

You initially set up Archiving policies when you deploy Archiving, but you can change, add, and delete policies after deployment. In Lync Server 2013 Control Panel, you can use the **Archiving Policy** page of the **Archiving and Monitoring** group to manage policies at the global level, site level, and user level. If you integrate your Lync Server storage with Exchange 2013 storage, the Exchange user policies take precedence over the Lync Server 2013 archiving policies.

For details about how policies are implemented, including the hierarchy of policies, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

If you enabled Microsoft Exchange integration for your deployment, Exchange policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation. You should specify all appropriate options in the Archiving configurations before enabling Archiving. For details, see Managing Archiving Configuration Options for Your Organization, Sites, and Pools in the Operations documentation.

To change an archiving policy

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. In the list of policies, do one of the following:
   - To change the policy for your entire deployment, click **Global** in the list of policies, click **Edit**, and then click **Show details**.
   - To change the policy for a single site, click the site name in the list of

policies, click **Edit**, and then click **Show details**.
- To change the policy for a single user or user group, click the user or user group name in the list of policies, click **Edit**, and then click **Show details**.

5. On the **Edit Archiving Policy** page, do the following:
   - To enable or disable internal archiving for the policy, select or clear the **Archive internal communications** check box.
   - To enable or disable external archiving for the policy, select or clear the **Archive external communications** check box.
6. Click **Commit**.

Important:

The settings of a user policy only apply to the specific users and user groups to which you apply the policy. For details, see Applying an Archiving Policy to Users

Enabling and Disabling Archiving by Using Windows PowerShell Cmdlets

Archiving can be enabled and disabled (for both internal and external communication sessions) by using the **Set-CsArchivingPolicy** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable the archiving of internal communication sessions

- To enable archiving of internal communication sessions, set the value of the **ArchiveInternal** property to True ($True). For example:

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $True
```

To enable the archiving of external communication sessions

- To enable archiving of external communication sessions, set the value of the **ArchiveExternal** property to True ($True). For example:

```
Set-CsArchivingPolicy -Identity "global" -ArchiveExternal $True
```

To enable the archiving of both internal and external communication sessions

- To enable archiving of both internal and external communications sessions, set both the **ArchiveInternal** and the **ArchiveExternal** properties to True:

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $True -Archiv
```

To disable archiving

- To disable archiving altogether, set both the **ArchiveInternal** and **ArchiveExternal** properties to False ($False). For example:

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $False -Archi
```

For more information, see the help topic for the Set-CsArchivingPolicy cmdlet.

See Also

Other Resources

Managing the Archiving of Internal and External Communications

Applying an Archiving Policy to Users

See Also

Operations > Managing Lync Server 2013 Archiving > Managing the Archiving of Internal and External Communications >

Topic Last Modified: *2013-02-23*

If a user has been enabled for Lync Server 2013 and you have created one or more user policies for archiving for users homed on Lync Server 2013, you can implement archiving support for specific users by applying the appropriate policies to those users or user groups. For example, if you create a policy to support archiving of internal communications, you can apply it to at least one user or user group to support archiving of the user's Lync Server 2013 communications.

Note:

If you enabled Microsoft Exchange integration for your deployment, Exchange In-Place Hold policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.
You should specify all appropriate options in the Archiving configurations before enabling Archiving. For details, see Managing Archiving Configuration Options for Your Organization, Sites, and Pools in the Operations documentation.

Use the procedure in this topic to apply a previously created Archiving user policy to one or more user accounts or user groups.

⊟To apply an archiving user policy to a user account

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**, and then search for the user account that you want to configure.
4. In the table that lists the search results, click the user account, click **Edit**, and then click **Show details**.
5. In **Edit Lync Server User** under **Archiving policy**, select the archiving user policy that you want to apply.

   Note:

   The **<Automatic>** settings apply the default server installation settings. These settings are applied automatically by the server.
6. Click **Commit**.

Assigning a Per-User Archiving Policy by Using Windows PowerShell Cmdlets

Per-user archiving policies can be assigned by using Windows PowerShell and the **Grant-CsArchivingPolicy** cmdlet. You can run this cmdlet from either the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user archiving policy to a single user

- The following command assigns the per-user archiving policy RedmondArchivingPolicy to the user Ken Myer.

```
Grant-CsArchivingPolicy -Identity "Ken Myer" -PolicyName "RedmondArchiv
```

To assign a per-user archiving policy to multiple users

- This command assigns the per-user archiving policy RedmondArchivingPolicy to all users who have accounts homed on the Registrar pool atl-cs-001.litwareinc.com. For details about the Filter parameter used in this command, see the Get-CsUser cmdlet documentation.

```
Get-CsUser -Filter {RegistrarPool -eq "atl-cs-001.litwareinc.com"} | Gr
```

To assign a per-user archiving policy

- The following command unassigns any per-user archiving policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsArchivingPolicy -Identity "Ken Myer" -PolicyName $Null
```

For details, see the Grant-CsArchivingPolicy cmdlet documentation.

See Also

Other Resources

Managing the Archiving of Internal and External Communications
Assigning Per-User Policies

1.7.12.2.4 Setting Up Policies for Archiving When Using Exchange Server Integration

Setting Up Policies for Archiving When Using Exchange Server Integration

Configuring Support for Archiving > Configuring and Assigning Archiving Policies > Setting Up Archiving Policies for Users >

Topic Last Modified: *2012-10-09*

If users homed on Exchange 2013 have their mailboxes put on In-Place Hold, Exchange In-Place Hold policies control archiving for those users. If you use Microsoft Exchange integration for your deployment, Exchange 2013 policies override Lync Server Archiving policies for users who are homed on Exchange 2013. For information about configuring Exchange Archiving policies, see the Exchange 2013 documentation. For details about setting up user policies for users homed on Lync Server 2013, see Setting Up User Policies for Archiving in Lync Server in the Deployment documentation. For details about how policies work, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

If you deploy Exchange 2013 and Lync Server 2013 in the same forest, your Exchange 2013 In-Place Hold policies control archiving. If you deploy Exchange 2013 and Lync Server 2013 in separate forests, see “Deploying Lync Server and Microsoft Exchange in Different Forests” in Deployment Checklist for Archiving.

Deleting an Archiving Policy

See Also

Operations > Managing Lync Server 2013 Archiving > Managing the Archiving of Internal and External Communications >

Topic Last Modified: *2013-02-23*

You can delete a user policy or site policy. The global policy cannot be removed. If you try to delete the global policy, Lync Server 2013 automatically resets the policy to the default values.

> **Note:**
>
> If you enabled Microsoft Exchange integration for your deployment, Exchange policies control whether archiving is enabled for the users who are homed on Exchange 2013 and have their mailboxes put on In-Place Hold. For details, see Setting Up Policies for Archiving When Using Exchange Server Integration in the Deployment documentation.

To delete a user or site policy for archiving

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Policy**.
4. In the list of archiving policies, click the user or site policy that you want to delete, click **Edit**, and then click **Delete**.
5. Click **Commit**.

Removing Archiving Policies by Using Windows PowerShell Cmdlets

Archiving policies can be deleted by using Windows PowerShell and the **Remove-CsArchivingPolicy** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specified archiving policy

- As an example, **Remove-CsArchivingPolicy** deletes the policy with the Identity site:Redmond. Note that, when a policy configured at the site scope is deleted, users previously managed by the site policy will automatically be governed by the global archiving policy instead. The following command removes the archiving applied to the Redmond site:

```
Remove-CsArchivingPolicy -Identity site:Redmond
```

To remove all the archiving policies applied to the per-user scope

- This command removes all the archiving policies applied to the per-user scope:

```
Get-CsArchivingPolicy -Filter "tag:*" | Remove-CsArchivingPolicy
```

To remove all the archiving policies that disable internal archiving

- This command removes all the archiving policies where internal archiving has been disabled:

```
Get-CsArchivingPolicy | Where-Object {$_.ArchiveInternal -eq $False} |
```

For more information, see the help topic for the Remove-CsArchivingPolicy cmdlet.

See Also

Other Resources

Managing the Archiving of Internal and External Communications

1.7.12.3 Managing Archiving Configuration Options for Your Organization, Sites, and Pools

Managing Archiving Configuration Options for Your Organization, Sites, and Pools

See Also

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Archiving >

Topic Last Modified: *2012-11-01*

In Lync Server 2013 Control Panel, you use Archiving configurations to specify how archiving is implemented. This includes the following Archiving configurations:

- A global configuration that is created by default when you deploy Lync Server 2013.
- Optional site-level and pool-level configurations that you can create and use to specify how archiving is implemented for specific sites or pools.

You initially set up Archiving configurations when you deploy Archiving, but you can change, add, and delete configurations after deployment. In Lync Server 2013 Control Panel, you can use the **Archiving Configuration** page of the **Archiving and Monitoring** group to manage configurations at the global level, site level, and pool level. For details about how Archiving configurations are implemented, including which options you can specify, and the hierarchy of Archiving configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

To use archiving, you must configure Archiving policies to specify whether to enable archiving for internal communications, for external communications, or for both for all users homed on Lync Server 2013. By default, archiving is not enabled for either internal or external communications. If you use Microsoft Exchange integration, you must enable and configure Exchange 2013 to support archiving for all users homed on Exchange 2013 who have had their mailboxes put on In-Place Hold.

Prior to enabling Archiving, you should specify the appropriate Archiving configurations for your deployment and, optionally, for specific sites and pools, as described in this section. For details about enabling Archiving, see Configuring and Assigning Archiving Policies in the Deployment documentation.

To view archiving configuration information by using Windows PowerShell cmdlets

- You can view Archiving configuration information by using Windows PowerShell and the **Get-CsArchivingConfiguration** cmdlet. You can run this cmdlet from either the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

  In the Lync Server Management Shell, use the following command to view information about all of your archiving configuration settings:

```
Get-CsArchivingConfiguration
```

- Creating an Archiving Configuration to Manage Archiving for Specific Sites or Pools
- Enabling or Disabling Archiving of IM or Conferencing Sessions
- Enabling or Disabling the Purging of Archived Data
- Enabling or Disabling Critical Mode to Block or Allow IM and Web Conferencing Sessions If Archiving Fails
- Enable or Disable Sending an Archiving Disclaimer to Federated Partners
- Enabling or Disabling Integration with Exchange Storage
- Deleting an Archiving Configuration

⊟See Also

Other Resources

Managing Lync Server 2013 Archiving

1.7.12.3.1 Creating an Archiving Configuration to Manage Archiving for Specific Sites or Pools

Creating an Archiving Configuration to Manage Archiving for Specific Sites or Pools

See Also

Operations > Managing Lync Server 2013 Archiving > Managing Archiving Configuration Options for Your Organization, Sites, and Pools >

***Topic Last Modified:** 2013-02-23*

In Lync Server 2013 Control Panel, you use Archiving configurations to control how archiving is implemented in your deployment. This includes the following Archiving configurations:

- A global configuration that is created by default when you deploy Lync Server 2013.
- Optional site-level and pool-level configurations that you can create and use to specify how archiving is implemented for specific sites or pools.

You initially set up Archiving configurations when you deploy Archiving, but you can change, add, and delete configurations after deployment. For details about how Archiving configurations are implemented, including which options you can specify and the hierarchy of Archiving configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

To use archiving, you must configure Archiving policies to specify whether to enable archiving for internal communications, for external communications, or for both for users homed on Lync Server 2013. By default, archiving is not enabled for either internal or external communications. Before enabling Archiving in any policies, you should specify the appropriate Archiving configurations for your deployment and, optionally, for specific sites and pools, as described in this section. For details about enabling Archiving, see Configuring and Assigning Archiving Policies in the Deployment documentation.
If you decide after you deploy Archiving that you want to use Microsoft Exchange integration to store archiving data and files on Exchange 2013 servers and all your users are homed on your Exchange 2013 servers, you should remove the SQL Server database configuration from your topology. You must use Topology Builder to do this. For details, see Changing Archiving Database Options in the Operations documentation.

⊟To create an archiving configuration for a site or pool

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. On the **Archiving Configuration** page, click **New**, and then do one of the following:
   - To create a site archiving configuration, click **Site Configuration** and then, in **Select a site**, select the site to be configured for archiving.
   - To create a pool archiving configuration, click **Pool Configuration** and then, in **Select a pool**, select the pool to be configured for archiving.
5. In **New Archiving Setting**, in the **Archiving setting** drop-down list box, do one of the following:
   - To enable archiving only for instant messaging (IM) sessions, click **Archive IM sessions**.
   - To enable archiving for both IM sessions and web conferences, click **Archive IM and web conferencing sessions**.
   - To disable archiving for the policy, click **Disable archiving**.
6. Also in **New Archiving Setting**, do the following:
   - To block activity when archiving is not available, select the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.
   - To use Microsoft Exchange Server to store archiving data, click the **Microsoft Exchange integration** check box.
   - To enable data purging, select the **Enable purging of archiving data** check box, and then do one of the following:
     - To specify purging after a specific number of days, click **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
     - To limit purging to archiving data that has been exported, click **Purge exported archiving data only**.
7. Click **Commit**.

Creating Archiving Configuration Settings by Using Windows PowerShell Cmdlets

Archiving configuration settings can be created by using Windows PowerShell and the New-CsArchivingConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To create a new collection of archiving configuration settings for a site

- The following command creates a new collection of archiving configuration settings for the Redmond site:

  ```
  New-CsArchivingConfiguration -Identity "site:Redmond"
  ```

⊟To create a new collection of archiving configuration settings that only allow IM archiving

- Because no parameters (other than the mandatory Identity parameter) were specified in the preceding command, the new collection of configuration settings will use the default values for all its properties. To create settings that use different property values, simply include the appropriate parameter and parameter value. For example, to create a collection of archiving configuration settings that, by default, allow archiving of instant messaging sessions, only use a command like this:

```
New-CsArchivingConfiguration -Identity "site:Redmond" -EnableArchiving
```

To specify multiple property values when creating archiving configuration settings

- Multiple property values can be modified by including multiple parameters. For example, this command configures the new settings to archive instant messaging sessions and to block instant messaging of the archiving service is not available:

```
New-CsArchivingConfiguration -Identity "site:Redmond" -EnableArchiving
```

For more information, see the help topic for the New-CsArchivingConfiguration cmdlet.

See Also

Concepts

How Archiving Works

Other Resources

Managing Archiving Configuration Options for Your Organization, Sites, and Pools

1.7.12.3.2 Enabling or Disabling Archiving of IM or Conferencing Sessions

Enabling or Disabling Archiving of IM or Conferencing Sessions

See Also

Operations > Managing Lync Server 2013 Archiving > Managing Archiving Configuration Options for Your Organization, Sites, and Pools >

Topic Last Modified: *2012-10-10*

In Lync Server 2013 Control Panel, you use Archiving configurations to enable and disable archiving of IM, conferencing sessions, or both. This includes the following Archiving configurations:

- A global configuration that is created by default when you deploy Lync Server 2013.
- Optional site-level and pool-level configurations that you can create and use to specify how archiving is implemented for specific sites or pools.

You initially set up Archiving configurations when you deploy Archiving, but you can change, add, and delete configurations after deployment. For details about how Archiving configurations are implemented, including which options you can specify and the hierarchy of Archiving configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

To use archiving, you must configure Archiving policies to specify whether to enable archiving for internal communications, for external communications, or for both for users homed on Lync Server 2013. By default, archiving is not enabled for either internal or external communications. Before enabling Archiving in any policies, you should specify the appropriate Archiving configurations for your deployment and, optionally, for specific sites and pools, as described in this section. For details about enabling Archiving, see Configuring and Assigning Archiving Policies in the Deployment documentation.
If you decide after you deploy Archiving that you want to use Microsoft Exchange integration to store archiving data and files on Exchange 2013 servers and all your users

are homed on your Exchange 2013 servers, you should remove the SQL Server database configuration from your topology. You must use Topology Builder to do this. For details, see Changing Archiving Database Options in the Operations documentation.

⊟To enable or disable archiving of IM or conferencing sessions

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. Select the appropriate global, site, or pool configuration from the list of archiving configurations, click **Edit**, click **Show details**, and then do the following:
   - To enable archiving only for instant messaging (IM) sessions, click **Archive IM sessions**.
   - To enable archiving for both IM sessions and conferences, click **Archive IM and conferencing sessions**.
   - To disable archiving for the policy, click **Disable archiving**.
5. Click **Commit**.

Other Resources

Managing Archiving Configuration Options for Your Organization, Sites, and Pools
Configuring and Assigning Archiving Policies

1.7.12.3.3 Enabling or Disabling the Purging of Archived Data

Enabling or Disabling the Purging of Archived Data

See Also

Operations > Managing Lync Server 2013 Archiving > Managing Archiving Configuration Options for Your Organization, Sites, and Pools >

Topic Last Modified: *2013-02-23*

In Lync Server 2013 Control Panel, you use Archiving configurations to enable and disable purging and configure how purging is implemented. This includes the following Archiving configurations:

- A global configuration that is created by default when you deploy Lync Server 2013.
- Optional site-level and pool-level configurations that you can create and use to specify how archiving is implemented for specific sites or pools.

You initially set up Archiving configurations when you deploy Archiving, but you can change, add, and delete configurations after deployment. For details about how Archiving configurations are implemented, including which options you can specify and the hierarchy of Archiving configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

To use archiving for users who are homed on Lync Server 2013 you must configure Archiving policies to specify whether to enable archiving for internal communications, for external communications, or for both. By default, archiving is not enabled for either internal or external communications. Prior to enabling Archiving in any policies, you should specify the appropriate Archiving configurations for your deployment and, optionally, for specific sites and pools, as described in this section. For details about enabling Archiving,

see Configuring and Assigning Archiving Policies in the Deployment documentation.
If you decide after you deploy Archiving that you want to use Microsoft Exchange integration to store archiving data and files on Exchange 2013 servers and all your users are homed on your Exchange 2013 servers, you should remove the SQL Server database configuration from your topology. You must use Topology Builder to do this. For details, see Changing Archiving Database Options in the Operations documentation.

To enable or disable purging for archiving

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. Click the name of the appropriate global, site, or pool configuration in the list of archiving configurations, click **Edit**, click **Show details**, and then do the following:
   - To enable purging, select the **Enable purging of archiving data** check box and then do one of the following:
     - To purge all records, click the **Purge exported archiving data and stored archiving data after maximum duration (days)**, and then specify the number of days.
     - To purge only the data that has been exported, click **Purge exported archiving data only**.
   - To disable purging, clear the **Enable purging of archiving data** check box.
5. Click **Commit**.

Enabling or Disabling the Purging of Archiving Data by Using Windows PowerShell Cmdlets

Enabling and disabling the automated purging of archiving data can be managed by using Windows PowerShell and the **Set-CsArchivingConfiguration** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable the purging of all archiving data

- To enable the purging of all archiving data set the **EnablePurging** property to true ($True). For example:

  ```
  Set-CsArchivingConfiguration -Identity "site:Redmond" -EnablePurging $T
  ```

  After this command is run, then every day Lync Server will purge all archiving records older than the value specified for the **KeepArchivingDataForDays** property.

To enable the purging only of exported archiving data

- To limit purging to archiving records that have been exported to a data file (by using the Export-CsArchivingData cmdlet) you must also set the PurgeExportedArchivesOnly property to True ($True). For example:

  ```
  Set-CsArchivingConfiguration -Identity "site:Redmond" -EnablePurging $T
  ```

After this command is run, Lync Server will only purge archiving records that meet two criteria: 1) they are older than the value specified for the **KeepArchivingDataForDays** property; and, 2) they have been exported by using the **Export-CsArchivingData** cmdlet.

To disable the purging of all archiving data

- To disable the automated purging of archiving records, set the **EnablePurging** property to False ($False). For example:

```
Set-CsArchivingConfiguration -Identity "site:Redmond" -EnablePurging $F
```

For more information, including additional options for purging archiving data, see the help topic for the Set-CsArchivingConfiguration cmdlet.

See Also

Concepts

How Archiving Works

Other Resources

Configuring and Assigning Archiving Policies
Managing Archiving Configuration Options for Your Organization, Sites, and Pools

1.7.12.3.4 Enabling or Disabling Critical Mode to Block or Allow IM and Web Conferencing Sessions If Archiving Fails

Enabling or Disabling Critical Mode to Block or Allow IM and Web Conferencing Sessions If Archiving Fails

See Also

Operations > Managing Lync Server 2013 Archiving > Managing Archiving Configuration Options for Your Organization, Sites, and Pools >

Topic Last Modified: *2013-02-23*

In Lync Server 2013 Control Panel, you use Archiving configurations to enable and disable critical mode. This includes the following Archiving configurations:

- A global configuration that is created by default when you deploy Lync Server 2013.
- Optional site-level and pool-level configurations that you can create and use to specify how archiving is implemented for specific sites or pools.

You initially set up Archiving configurations when you deploy Archiving, but you can change, add, and delete configurations after deployment. For details about how Archiving configurations are implemented, including which options you can specify and the hierarchy of Archiving configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

Note:

To use archiving, you must configure Archiving policies to specify whether to enable archiving for internal communications, for external communications, or for both for users homed on Lync Server 2013. By default, archiving is not enabled for either internal or external communications. Prior to enabling Archiving in any policies, you should specify the appropriate Archiving configurations for your deployment and, optionally, for specific sites and pools, as described in this section. For details about enabling Archiving, see Configuring and Assigning Archiving Policies in the Deployment documentation.
If you decide after you deploy Archiving that you want to use Exchange Server integration to store archiving data and files on Exchange 2013 servers and all your users

are homed on your Exchange 2013 servers, you should remove the SQL Server database configuration from your topology. You must use Topology Builder to do this. For details, see Changing Archiving Database Options in the Operations documentation.

To enable or disable blocking of IM and web conferencing sessions if archiving fails

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. Click the name of the appropriate global, site, or pool configuration in the list of archiving configurations, click **Edit**, click **Show details**, and then do the following:
5. To set how archiving behaves when a failure occurs, select or clear the **Block instant messaging (IM) or web conferencing sessions if archiving fails** check box.
6. Click **Commit**.

Enabling and Disabling Critical Mode by Using Windows PowerShell Cmdlets

You can enable or disable critical mode using the **Set-CsArchivingConfiguration** cmdlet. You can run this cmdlet from either the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable critical mode

- To enable critical mode, set the value of the BlockOnArchiveFailure property to True ($True). For example:

```
Set-CsArchivingConfiguration -Identity "site:Redmond" -BlockOnArchiveFa
```

To disable critical mode

- To disable critical mode, set the value of the BlockOnArchiveFailure property to False ($False). For example:

```
Set-CsArchivingConfiguration -Identity "site:Redmond" -BlockOnArchiveFa
```

For more information, see the Help topic for the Set-CsArchivingConfiguration cmdlet.

See Also

Tasks

Changing Archiving Database Options

Concepts

How Archiving Works

Other Resources

Managing Archiving Configuration Options for Your Organization, Sites, and Pools

Enable or Disable Sending an Archiving Disclaimer to Federated Partners

Deployment > Deploying Archiving > Configuring Support for Archiving >

Topic Last Modified: *2013-02-23*

At the time you deployed your Edge Servers and enabled federation for your organization, you should have specified whether to automatically send the archiving disclaimer to federated partners. If you archive external communications, you should enable the sending of an archiving disclaimer. Use the procedure in this topic to change that configuration.

> **Note:**
>
> The following procedure assumes that you have already enabled federation for your organization. For details about enabling federation, see Enable or Disable Remote User Access in the Deployment documentation or the Operations documentation.

⊟To enable or disable sending of an archiving disclaimer to federated partners

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **External User Access**, click **Access Edge Configuration**.
4. On the **Access Edge Configuration** tab, click **Global**, click **Edit**, and then click **Show details**.
5. In **Edit Access Edge Configuration**, under **Enable communications with federated users**, select or clear the **Send archiving disclaimer to federated partners** check box to enable or disable automatically sending the archiving disclaimer.
6. Click **Commit**.

To enable federated users to collaborate with users in your Lync Server 2013 deployment, you must have also configured at least one external access policy to support federated user access. For details, see Manage XMPP Federated Partners for Your Organization in the Deployment documentation or the Operations documentation. For details about controlling access for specific federated domains, see Configure Support for Allowed External Domains in the Deployment documentation or Operations documentation.

Enabling or Disabling the Archiving Disclaimer by Using Windows PowerShell Cmdlets

The use of the archiving disclaimer can be managed by using Windows PowerShell and the Set-CsAccessEdgeConfiguration cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable the archiving disclaimer

- To enable the archiving disclaimer, set the value of the **EnableArchivingDisclaimer** property to True ($True):

```
Set-CsAccessEdgeConfiguration -EnableArchivingDisclaimer $True
```

To disable the archiving disclaimer

- To disable the archiving disclaimer, set the value of the **EnableArchivingDisclaimer** property to False ($False):

```
Set-CsAccessEdgeConfiguration -EnableArchivingDisclaimer $False
```

1.7.12.3.6 Enabling or Disabling Integration with Exchange Storage

Enabling or Disabling Integration with Exchange Storage

See Also

Operations > Managing Lync Server 2013 Archiving > Managing Archiving Configuration Options for Your Organization, Sites, and Pools >

Topic Last Modified: *2012-10-09*

In Lync Server 2013 Control Panel, you use Archiving configurations to enable and disable integration with Exchange storage. This includes the following Archiving configurations:

- A global configuration that is created by default when you deploy Lync Server 2013.
- Optional site-level and pool-level configurations that you can create and use to specify how archiving is implemented for specific sites or pools.

For details about how Archiving configurations are implemented, including which options you can specify and the hierarchy of Archiving configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

To enable or disable integration with Microsoft Exchange storage

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. Click the name of the appropriate global, site, or pool configuration in the list of archiving configurations, click **Edit**, click **Show details**, and then do the following:
   - To enable integration with Exchange 2013 storage, select the **Microsoft Exchange integration** check box.
   - To disable integration with Exchange 2013 storage, clear the **Microsoft Exchange integration** check box.
5. Click **Commit**.

Concepts

How Archiving Works

Other Resources

Managing Archiving Configuration Options for Your Organization, Sites, and Pools

Deleting an Archiving Configuration

See Also

Operations > Managing Lync Server 2013 Archiving > Managing Archiving Configuration Options for Your Organization, Sites, and Pools >

Topic Last Modified: *2013-02-23*

You can delete a site configuration or pool configuration. The global configuration cannot be removed. If you delete the global configuration, it is automatically reset to the default values. For details about how Archiving configurations are implemented, including which options you can specify and the hierarchy of Archiving configurations, see How Archiving Works in the Planning documentation, Deployment documentation, or Operations documentation.

To delete a site or pool configuration for archiving

1. From a user account that is assigned to the CsArchivingAdministrator or CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Archiving Configuration**.
4. In the list of archiving configurations, click the site or pool configuration that you want to delete, click **Edit**, and then click **Delete**.
5. Click **Commit**.

Removing Archiving Configuration Settings by Using Windows PowerShell Cmdlets

Archiving configuration settings can be deleted by using Windows PowerShell and the **Remove-CsArchivingConfiguration** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specified collection of archiving configuration settings

- The following command removes the archiving configuration settings applied to the Redmond site:

```
Remove-CsArchivingConfiguration -Identity "site:Redmond"
```

To remove all the archiving configuration settings applied to the site scope

- This command removes all the archiving configuration settings applied to the service scope:

```
Get-CsArchivingConfiguration -Filter "site:*" | Remove-CsArchivingConfi
```

To remove archiving configuration settings based on a specified property value

- This command removes all the archiving configuration settings where

Exchange archiving has been disabled:

```
Get-CsArchivingConfiguration | Where-Object {$_.EnableExchangeArchiving
```

For more information, see the help topic for the Remove-CsArchivingConfiguration cmdlet.

⊟See Also

Concepts

How Archiving Works

Other Resources

Managing the Archiving of Internal and External Communications

1.7.12.4 Changing Archiving Database Options

Changing Archiving Database Options

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Archiving >

Topic Last Modified: *2012-11-01*

If you deploy Archiving using SQL Server storage for archiving storage for any of your users, you can make the following database storage changes:

- Use a different SQL Server database for archiving storage. This includes the primary Archiving database and any database you use for SQL Server mirroring.
- Switch to Microsoft Exchange integration to store archiving data and files on Exchange 2013 servers. If all your users are homed on your Exchange 2013 servers and you want to use Microsoft Exchange storage for all users in your deployment, you should remove the SQL Server store databases from your topology.

To make either of these changes, you must run Topology Builder, make the changes, and then publish the topology again. You can use Topology Builder to do this. Do not specify **Archiving SQL Server store** or **Enable SQL Server store mirroring** information, unless you have Lync users who are not homed on Exchange 2013 servers.

⊟To change your archiving database option

1. On a computer that is running Lync Server 2013, or on which the Lync Server administrative tools are installed, log on by using an account that is a member of the local Users group (or an account with equivalent user rights).

   > **Note:**
   > You can define a topology by using an account that is a member of the local Users group, but to publish a topology, which is required to add a component to the topology, you must use an account that is a member of the **Domain Admins** group and the **RTCUniversalServerAdmins** group, and that has full control permissions (that is, read, write, and modify) on the file share that you are using for the Lync Server 2013 file store (that is, so that Topology Builder can configure the required discretionary access control lists (DACLs), or an account with equivalent rights.

2. Start Topology Builder.
3. In the console tree, navigate to the Front End pool in which you deployed Archiving, and then click the name of the Front End pool where you want to change the database options.
4. In the **Action** menu, click **Edit Properties**.
5. In the **Edit Properties** dialog box, click **General**.
6. Scroll down to **Archiving**.

7. In **Archiving**, do the following:
   - To change to a different existing SQL Server store, under **Archiving SQL Server store**, in the drop-down list box, do the following:
     - To use an existing SQL Server store, in the drop-down list box, click the name of the SQL Server store that you want to use.
     - To specify a new SQL Server store, click **New**, and then in the **Define New SQL Server store** dialog box, do the following:
       - To use an existing SQL Server store, in the drop-down list box, click the name of the SQL Server store that you want to use.
       - To specify a new SQL Server store, click **New**, and then in the **Define New SQL Server Store** dialog box, do the following:
         - In **SQL Server FQDN**, specify the FQDN of the server on which you want to create the new SQL Server store.
         - Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named instance**, and then specify the instance you want to use.
         - If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
   - To add SQL Server store for mirroring or change to a different existing SQL Server store for SQL Server store mirroring, select **Enable SQL Server store mirroring**, and then do the following:
     - To use an existing SQL Server store for mirroring, in the **Archiving SQL Server store mirror** drop-down list box, click the name of the SQL Server store that you want to use for mirroring.
     - To specify a new SQL Server store for mirroring, click **New**, and then in the **Define New SQL Server Store** dialog box, do one of the following:
       - In **SQL Server FQDN**, specify the FQDN of the SQL Server on which you want to create the new SQL Server store.
       - Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named Instance**, and then specify the instance you want to use.
       - If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
     - If you enable SQL Server mirroring and want to add or change a SQL Server mirroring witness (a third, separate SQL Server instance that can detect the health of the primary SQL Server server and mirror instances), select the **Use SQL Server mirroring witness to enable automatic failover** check box, and then do one of the following:
       - In **SQL Server FQDN**, specify the FQDN of the server on which you want to create the new SQL Server mirroring witness.
       - Either click **Default Instance** to use the default instance, or, to specify a different instance, click **Named Instance**, and then specify the instance you want to use for the mirroring witness.
       - If the specified SQL Server instance is in a mirroring relationship, select the **This SQL instance is in mirroring relation** check box, and then, in **Mirror port number**, specify the port number.
   - To switch to Microsoft Exchange integration to store archiving data and files on Exchange 2013 servers (if all users in your deployment are homed on your Exchange 2013 servers), delete all information for Archiving databases.

   ◆Important:

   If you have any Lync users who are not homed on Exchange 2013 servers, do not delete the SQL Server store information.

8. To save the configuration, click **OK**.

   ◆Important:

The changes you make in Topology Builder do not take effect until you publish the new topology. For details, see Publishing the Updated Topology to Add Archiving Databases in the Deployment documentation.

1.7.12.5 Exporting Archived Data

Exporting Archived Data

See Also

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Archiving >

Topic Last Modified: *2013-02-23*

Data archived in Archiving databases is not searchable or in a readable format, but you can use the Export-CsArchivingData cmdlet to extract records from the database and save them as an Outlook Electronic Mail (EML) file. For details about exporting archived data, see Export-CsArchivingData in the Operations documentation.

If you enable Microsoft Exchange integration, data is archived in Exchange 2013 stores. Data archived in Exchange 2013 is searchable and discoverable. For details about support for integrated communications for Exchange 2013 and Lync Server 2013, see Exchange Server and SharePoint Integration Support in the Supportability documentation. For details about accessing data that is archived in Exchange, see the Exchange 2013 documentation.

Exporting Archiving Data by Using Windows PowerShell Cmdlets

Archiving data can be exported by using the Export-CSArchivingData cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To export archiving data

- This command exports all the archiving data written to the archiving database atl-sql-001.litwareinc.com since June 1, 2012. The resulting output file will be stored in the folder C:\ArchivingExports.

```
Export-CsArchivingData -Identity "ArchivingDatabase:atl-sql-001.litware
```

To export archiving data for a single user

- The following command exports archiving data for a single user: kenmyer@litwareinc.com. This is done by including the UserUri parameter followed by the user’s SIP address. For example:

```
Export-CsArchivingData -Identity "ArchivingDatabase:atl-sql-001.litware
```

For more information, see the help topic for the Export-CsArchivingData cmdlet.

See Also

Concepts

Exchange Server and SharePoint Integration Support

Other Resources

Export-CsArchivingData
Managing Lync Server 2013 Archiving

1.7.13 Managing Lync Server 2013 Security and Authentication

Managing Lync Server 2013 Security and Authentication

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-10-15*

Use the following procedures to manage Lync Server 2013 security and authentication.

In this section

- Managing Certificates for Operational Processes
- Managing Server-to-Server Authentication (Oauth) and Partner Applications
- Configuring Security
- Managing PIN Settings

1.7.13.1 Managing Certificates for Operational Processes

Managing Certificates for Operational Processes

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Security and Authentication >

Topic Last Modified: *2012-11-01*

Use the following procedures to manage certificates by using the Lync Server Management Shell cmdlets.

- Staging AV and OAuth Certificates Using -Roll in Set-CsCertificate

1.7.13.1.1 Staging AV and OAuth Certificates Using -Roll in Set-CsCertificate

Staging AV and OAuth Certificates Using -Roll in Set-CsCertificate

See Also

Operations > Managing Lync Server 2013 Security and Authentication > Managing Certificates for Operational Processes >

Topic Last Modified: *2012-11-13*

Audio/Video (A/V) communications is a key component of Microsoft Lync Server 2013. Features such as application sharing and audio and video conferencing rely on the certificates assigned to the A/V Edge service, specifically the A/V Authentication service.

Important:

1. This new feature is designed to work for the A/V Edge service and the *OAuthTokenIssuer* certificate. Other certificate types can be provisioned along with the A/V Edge service and OAuth certificate type, but will not benefit from the coexistence behavior that the A/V Edge service certificate will.
2. The Lync Server Management Shell PowerShell cmdlets used to manage Microsoft Lync Server 2013 certificates refers to the A/V Edge service certificate as the *AudioVideoAuthentication* certificate type and the OAuthServer certificate as type *OAuthTokenIssuer*. For the rest of this topic and to uniquely identify the certificates, they will be referred to by the same

identifier type, *AudioVideoAuthentication* and *OAuthTokenIssuer*.

The A/V Authentication service is responsible for issuing tokens that are used by clients and other A/V consumers. The tokens are generated from attributes on the certificate, and when the certificate expires, loss of connection and requirement to rejoin with a new token generated by the new certificate will result. A new feature in Lync Server 2013 will alleviate this problem – the ability to stage a new certificate in advance of the old one expiring and allowing both certificates to continue to function for a period of time. This feature uses updated functionality in the Set-CsCertificate Lync Server Management Shell cmdlet. The new parameter –Roll, with the existing parameter –EffectiveDate, will place the new AudioVideoAuthentication certificate in the certificate store. The older AudioVideoAuthentication certificate will still remain for issued tokens to be validated against. Beginning with putting the new AudioVideoAuthentication certificate in place, the following series of events will occur:

Tip:

Using the Lync Server Management Shell cmdlets for managing certificates, you can request separate and distinct certificates for each purpose on the Edge Server. Using the Certificate Wizard in the Lync Server Deployment Wizard assists you in creating certificates, but is typically of the **default** type which couples all certificate uses for the Edge Server onto a single certificate. The recommended practice if you are going to use the rolling certificate feature is to decouple the AudioVideoAuthentication certificate from the other certificate purposes. You can provision and stage a certificate of the Default type, but only the AudioVideoAuthentication portion of the combined certificate will benefit from the staging. A user involved in (for example) an instant messaging conversation when the certificate expires will need to log out and log back in to make use of the new certificate associated with the Access Edge service. Similar behavior will occur for a user involved in a Web conference using the Web Conferencing Edge service. The OAuthTokenIssuer certificate is a specific type that is shared across all servers. You create and manage the certificate in one place and the certificate is stored in the Central Management store for all other servers.

Additional detail is needed to fully understand your options and requirements when using the Set-CsCertificate cmdlet and using it to stage certificates prior to the current certificate expiring. The –Roll parameter is important, but essentially single purpose. If you define it as a parameter, you are telling Set-CsCertificate that you will be providing information about the certificate that will be affected defined by –Type (for example AudioVideoAuthentication and OAuthTokenIssuer), when the certificate will become effective defined by –EffectiveDate.

-Roll: The –Roll parameter is required and has dependencies that must be supplied along with it. Required parameters to fully define which certificates will be affected and how they will be applied:

-EffectiveDate: The parameter –EffectiveDate defines when the new certificate will become co-active with the current certificate. The –EffectiveDate can be close to the expiry time of the current certificate, or it can be a longer period of time. A recommended minimum –EffectiveDate for the AudioVideoAuthentication certificate would be 8 hours, which is the default token lifetime for AV Edge service tokens issued using the AudioVideoAuthentication certificate.

When staging OAuthTokenIssuer certificates, there are different requirements for the lead time before the certificate can become effective. The minimum time that the OAuthTokenIssuer certificate should have for its lead time is 24 hours before the expiration time of the current certificate. The extended lead time for the coexistence is because of other server roles that are dependent on the OAuthTokenIssuer certificate (Exchange Server, for example) which has a longer retention time for certificate created authentication and encryption key materials.

-Thumbprint: The thumbprint is an attribute on the certificate that is unique to that certificate. The –Thumbprint parameter is used to identify the certificate that will be affected by the actions of the Set-CsCertificate cmdlet.

-Type: The –Type parameter can accept a single certificate usage type or a comma separated list of certificate usage types. The certificate types are those that identify to the cmdlet and to the server what the purpose of the certificate is. For example, type AudioVideoAuthentication is for use by the A/V Edge service and the AV Authentication service. If you decide to stage and provision certificates of a different type at the same time, you must consider the longest required minimum effective lead time for the certificates. For example, you need to stage certificates of type AudioVideoAuthentication and OAuthTokenIssuer. Your minimum –EffectiveDate must be the greater of the two certificates, in this case the OAuthTokenIssuer, which has a minimum lead time of 24 hours. If you do not want to stage the AudioVideoAuthentication certificate with a lead time of 24 hours, stage it separately with an EffectiveDate that is more to your requirements.

To update or renew an A/V Edge service certificate with a –Roll and -EffectiveDate parameters

1. Log on to the local computer as a member of the Administrators group.
2. Request a renewal or new AudioVideoAuthentication certificate with exportable private key for the existing certificate on the A/V Edge service.
3. Import the new AudioVideoAuthentication certificate to the Edge Server and all other Edge Server in your pool (if you have a pool deployed).
4. Configure the imported certificate with the Set-CsCertificate cmdlet and use the –Roll parameter with the –EffectiveDate parameter. The effective date should be defined as the current certificate expire time (14:00:00, or 2:00:00 PM) minus token lifetime (by default eight hours). This gives us a time that the certificate must be set to active, and is the –EffectiveDate <string>: “7/22/2012 6:00:00 AM”.

   Important:

   For an Edge pool, you must have all AudioVideoAuthentication certificates deployed and provisioned by the date and time defined by the –EffectiveDate parameter of the first certificate deployed to avoid possible A/V communications disruption due to the older certificate expiring before all client and consumer tokens have been renewed using the new certificate.

   The Set-CsCertificate command with the –Roll and –EffectiveTime parameter:

   ```
   Set-CsCertificate -Type AudioVideoAuthentication -Thumbprint <thumb pr
   ```

   An example Set-CsCertificate command:

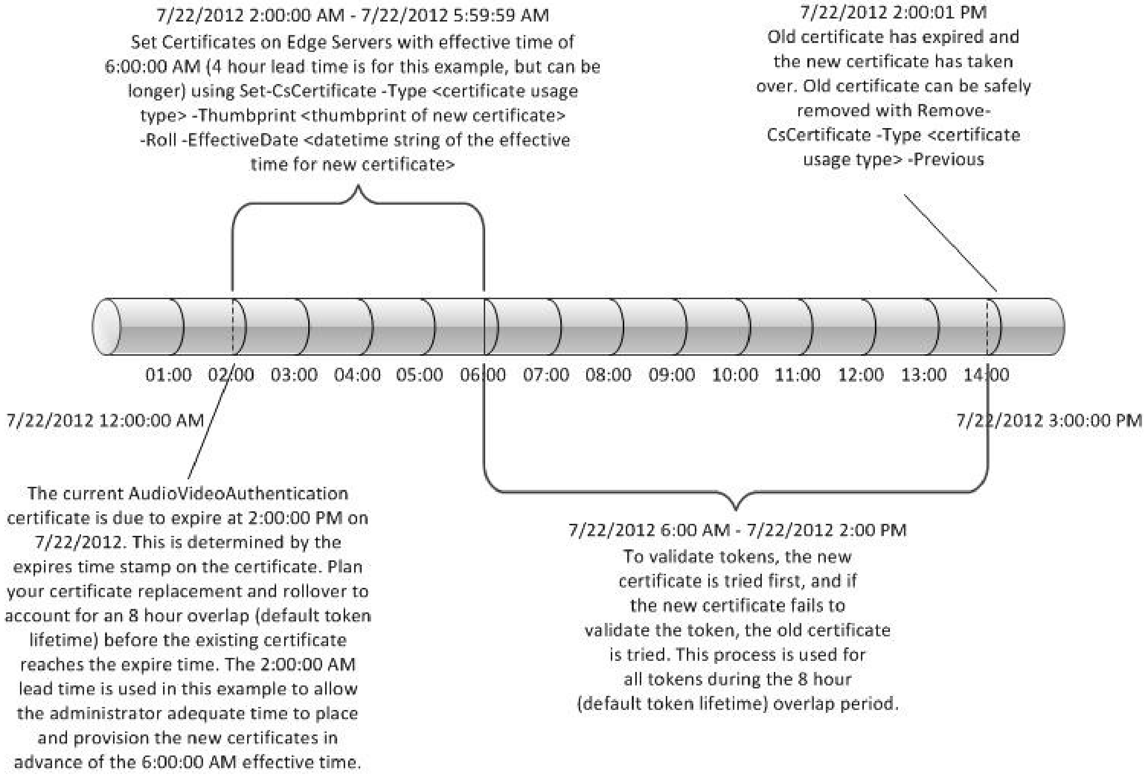
   ```
   Set-CsCertificate -Type AudioVideoAuthentication -Thumbprint "B142918E
   ```

   Important:

   The EffectiveDate must be formatted to match your server’s region and language settings. The example uses the US English Region and Language settings

To further understand the process that Set-CsCertificate, -Roll, and –EffectiveDate use to stage a new certificate for issuing new AudioVideoAuthentication tokens while still using an existing certificate to validate AudioVideoAuthentication that are in use by consumers, a visual timeline is an effective means of understanding the process.

In the following example, the administrator determines that the A/V Edge service certificate is due to expire at 2:00:00 PM on 07/22/2012. He requests and receives a new certificate and imports it to each Edge Server in his pool. At 2 AM on 07/22/2012, he begins running Get-CsCertificate with –Roll, -Thumbprint equal to the thumbprint string of the new certificate, and –EffectiveTime set to 07/22/2012 6:00:00 AM. He runs this command on each Edge Server.



7/22/2012 2:00:00 AM - 7/22/2012 5:59:59 AM
Set Certificates on Edge Servers with effective time of 6:00:00 AM (4 hour lead time is for this example, but can be longer) using Set-CsCertificate -Type <certificate usage type> -Thumbprint <thumbprint of new certificate> -Roll -EffectiveDate <datetime string of the effective time for new certificate>

7/22/2012 2:00:01 PM
Old certificate has expired and the new certificate has taken over. Old certificate can be safely removed with Remove-CsCertificate -Type <certificate usage type> -Previous

The current AudioVideoAuthentication certificate is due to expire at 2:00:00 PM on 7/22/2012. This is determined by the expires time stamp on the certificate. Plan your certificate replacement and rollover to account for an 8 hour overlap (default token lifetime) before the existing certificate reaches the expire time. The 2:00:00 AM lead time is used in this example to allow the administrator adequate time to place and provision the new certificates in advance of the 6:00:00 AM effective time.

7/22/2012 6:00 AM - 7/22/2012 2:00 PM
To validate tokens, the new certificate is tried first, and if the new certificate fails to validate the token, the old certificate is tried. This process is used for all tokens during the 8 hour (default token lifetime) overlap period.

When the effective time is reached (7/22/2012 6:00:00 AM), all new tokens are issued by the new certificate. When validating tokens, tokens will first be validated against the new certificate. If the validation fails, the old certificate is tried. The process of trying the new and falling back to the old certificate will continue until the expiry time of the old certificate. Once the old certificate has expired (7/22/2012 2:00:00 PM), tokens will only be validated by the new certificate. The old certificate can be safely removed using the Remove-CsCertificate cmdlet with the –Previous parameter.

```
Remove-CsCertificate -Type AudioVideoAuthentication -Previous
```

⊟To update or renew an OAuthTokenIssuer certificate with a –Roll and -EffectiveDate parameters

1. Log on to the local computer as a member of the Administrators group.
2. Request a renewal or new OAuthTokenIssuer certificate with exportable private key for the existing certificate on the A/V Edge service.
3. Import the new OAuthTokenIssuer certificate to a Front End Server in your pool (if you have a pool deployed). The OAuthTokenIssuer certificate is replicated globally and only needs to be updated and renewed at any server in your deployment. The Front End Server is used as an example.
4. Configure the imported certificate with the Set-CsCertificate cmdlet and use the –Roll parameter with the –EffectiveDate parameter. The effective date should be defined as the current certificate expire time (14:00:00, or 2:00:00 PM) minus a minimum of 24 hours.

   The Set-CsCertificate command with the –Roll and –EffectiveTime parameter:

   ```
   Set-CsCertificate -Type OAuthTokenIssuer -Thumbprint <thumb print of n
   ```

   An example Set-CsCertificate command:

   ```
   Set-CsCertificate -Type OAuthTokenIssuer -Thumbprint "B142918E463981A7
   ```

◆Important:

The EffectiveDate must be formatted to match your server's region and language settings. The example uses the US English Region and Language settings

When the effective time is reached (7/21/2012 1:00:00 AM), all new tokens are issued by the new certificate. When validating tokens, tokens will first be validated against the new certificate. If the validation fails, the old certificate is tried. The process of trying the new and falling back to the old certificate will continue until the expiry time of the old certificate. Once the old certificate has expired (7/22/2012 2:00:00 PM), tokens will only be validated by the new certificate. The old certificate can be safely removed using the Remove-CsCertificate cmdlet with the –Previous parameter.

```
Remove-CsCertificate -Type OAuthTokenIssuer -Previous
```

Concepts

Plan for Edge Server Certificates
Managing Server-to-Server Authentication (Oauth) and Partner Applications

Other Resources

Set Up Edge Certificates
Set-CsCertificate
Remove-CsCertificate

1.7.13.2 Managing Server-to-Server Authentication (Oauth) and Partner Applications

Managing Server-to-Server Authentication (Oauth) and Partner Applications

See Also

Microsoft Lync Server 2013 > Deployment >

Topic Last Modified: *2013-01-22*

Microsoft Lync Server 2013 must be able to securely, and seamlessly, communicate with other applications and server products. For example, you can configure Lync Server 2013 so that contact data and/or archiving data is stored in Microsoft Exchange Server 2013; however, this can only be done if Lync Server and Exchange are able to securely communicate with one another. Likewise, you can schedule a Lync Server conference from within Microsoft SharePoint Server; again, however, this can only be done if the two servers (SharePoint and Lync Server) trust one another. Although it's possible to use one authentication mechanism for Lync-to-Exchange communication and a separate mechanism for Lync-to-SharePoint communication, a better and more efficient approach is to use a standardized method for all server-to-server authentication and authorization.

Using a single, standardized method for server-to-server authentication is the approach taken by Lync Server 2013. For the 2013 release, Lync Server 2013 (as well as other Microsoft Server products, including Exchange 2013 and Microsoft SharePoint Server) support the OAuth (Open Authorization) protocol for server-to-server authentication and authorization. With OAuth, a standard authorization protocol used by a number of major websites, user credentials and passwords are not passed from one computer to another. Instead, authentication and authorization is based on the exchange of security tokens; these tokens grant access to a specific set of resources for a specific amount of time.

OAuth authentication typically involves three parties: a single authorization server and the two realms that need to communicate with one another. (You can also do server-to-server authentication without using an authorization server, a process that will be discussed later in this document.) Security tokens are issued by the authorization server (also known as a security token server) to the two realms that need to communicate;

these tokens verify that communications originating from one realm should be trusted by the other realm. For example, the authorization server might issue tokens that verify that users from a specific Lync Server 2013 realm are able to access a specified Exchange 2013 realm, and vice-versa.

Note:

A realm is simply a security container. By default, Lync Server 2013 uses your default SIP domain as its OAuth realm.

Lync Server 2013 supports three server-to-server authentication scenarios. With Lync Server 2013 you can:

- Configure server-to-server authentication between an on-premise installation of Lync Server 2013 and an on-premises installation of Exchange 2013 and/or Microsoft SharePoint Server.
- Configure server-to-server authentication between a pair of Office 365 components (for example, between Microsoft Exchange 365 and Microsoft Lync Server 365, or between Microsoft Lync Server 365 and Microsoft SharePoint 365).
- Configure server-to-server authentication in a cross-premises environment (that is, server-to-server authentication between an on-premises server and an Office 365 component).

Note that, at this point in time, only Exchange 2013, SharePoint Server, and Lync Server 2013 support server-to-server authentication; if you are not running one of these servers then you will not be able to fully implement OAuth authentication.

It should also be pointed out that you do not need to use server-to-server authentication: server-to-server authentication is not required in order to deploy Lync Server 2013. If Lync Server 2013 does not need to communicate with other servers (such as Exchange 2013) then server-to-server authentication is not needed.

However, server-to-server authentication is required if you want to use some of Lync Server's new features, such as the "unified contact store." With unified contact store, Lync Server 2013 contact information is stored in Exchange 2013 instead of in Lync Server; this enables users to have a single set of contacts that is readily accessible from within Lync, Microsoft Outlook, or Microsoft Outlook Web Access. Because the unified contact store requires Lync Server 2013 to share information with Exchange 2013, you must use server-to-server authentication in order to deploy the feature. Server-to-server authentication is also required if you choose to use Exchange archiving, in which the transcripts of instant messaging sessions are saved as Exchange 2013 emails rather than as individual database records.

For the Office 365 version of Lync Server to communicate with its Exchange counterpart, Lync Server 2013 must first obtain a security token from the authorization server. Lync Server then uses that security token to identify itself to Exchange 365. The Office 365 version of Exchange must go through the same process in order to communicate with Lync Server 2013.

However, for on-premises server-to-server authentication between two Microsoft servers there is no need to use a third-party token server. Server products such as Lync Server 2013 and Exchange 2013 have a built-in token server that can be used for authentication purposes with other Microsoft servers (such as SharePoint server) that support server-to-server authentication. For example, Lync Server 2013 can issue and sign a security token by itself, then use that token to communicate with Exchange 2013. In a case like this, there is no need for a third-party token server.

In order to configure server-to-server authentication for an on-premises implementation of Lync Server 2013 you must do two things:

- Assign a certificate to Lync Server's built-in token issuer.

- Configure the server that Lync Server 2013 will communicate with to be a "partner application." For example, if Lync Server 2013 needs to communicate with Exchange 2013 then you will need to configure Exchange to be a partner application.

> **Note:**
> A "partner application" is any application that Lync Server 2013 can directly exchange security tokens with, without having to go through a third-party security token server.

Concepts

Assigning a Server-to-Server Authentication Certificate to Microsoft Lync Server 2013
Configuring Microsoft Lync Server 2013 in a Cross-Premises Environment

1.7.13.2.1 Assigning a Server-to-Server Authentication Certificate to Microsoft Lync Server 2013

Assigning a Server-to-Server Authentication Certificate to Microsoft Lync Server 2013

Microsoft Lync Server 2013 > Deployment > Managing Server-to-Server Authentication (Oauth) and Partner Applications >

Topic Last Modified: *2012-10-01*

To determine whether or not a server-to-server authentication certificate has already been assigned to Microsoft Lync Server 2013, run the following command from the Lync Server 2013 Management Shell:

```
Get-CsCertificate -Type OAuthTokenIssuer
```

If no certificate information is returned you must assign a token issuer certificate before you can use server-to-server authentication. As a general rule, any Lync Server 2013 certificate can be used as your OAuthTokenIssuer certificate; for example, your Lync Server 2013 default certificate can also be used as the OAuthTokenIssuer certificate. (The OAUthTokenIssuer certificate can also be any Web server certificate that includes the name of your SIP domain in the Subject field.) The primary two requirements for the certificate used for server-to-server authentication are these: 1)the same certificate must be configured as the OAuthTokenIssuer certificate on all of your Front End Servers; and, 2) the certificate must be at least 2048 bits.

If you do not have a certificate that can be used for server-to-server authentication you can obtain a new certificate, import the new certificate, and then use that certificate for server-to-server authentication. After you have requested and obtained the new certificate you can then log on to any one of your Front End Servers and use a Windows PowerShell command similar to this one to import and assign that certificate:

```
Import-CsCertificate -Identity global -Type OAuthTokenIssuer -Path C:\Certificate
```

In the preceding command the Path parameter represents the full path to the certificate file, and the Password parameter represents the password that was assigned to the certificate. This procedure should be run just one time: Lync Server's replication service will then automatically create a set of scheduled tasks that will decrypt and deploy the certificate to all your Front End Servers.

Alternatively, you can use an existing certificate as your server-to-server authentication certificate. (As noted, the default certificate can be used as the server-to-server authentication certificate.) The following pair of Windows PowerShell commands retrieve the value of the default certificate's Thumbprint property, then use that value to make the default certificate the server-to-server authentication certificate:

```
$x = (Get-CsCertificate -Type Default).Thumbprint
```

```
Set-CsCertificate -Identity global -Type OAuthTokenIssuer -Thumbprint $x
```

In the preceding command, the retrieved certificate is configured to function as the global server-to-server authentication certificate; that means that the certificate will be replicated to, and used by, all your Front End Servers. Again, this command should only be run one time, and only on one of your Front End Servers. Although all Front End Servers must use the same certificate, you should not configure the OAuthTokenIssuer certificate on each Front End Server. Instead, configure the certificate once, then let Lync Server's replication server take care of copying that certificate to each server.

The Set-CsCertificate cmdlet takes the certificate in question and immediately configures that certificate to act as the current OAuthTokenIssuer certificate. (Lync Server 2013 keeps two copies of a certificate type: the current certificate and the previous certificate.) If you need the new certificate to immediately begin to act as the OAuthTokenIssuer certificate then you should use the Set-CsCertificate cmdlet.

You can also use the Set-CsCertificate cmdlet to "roll" a new certificate. "Rolling" a certificate simply means that you configure a new certificate to become the current OAuthTokenIssuer certificate at a specified point in time. For example, this command retrieves the default certificate and then configure that certificate to take over as the current OAuthTokenIssuer certificate as of July 1, 2012:

```
$x = (Get-CsCertificate -Type Default).Thumbprint
Set-CsCertificate -Identity global -Type OAuthTokenIssuer -Thumbprint $x -Effecti
```

On July 1, 2012 the new certificate will be configured as the current OAuthTokenIssuer certificate and the "old" OAuthTokenIssuer certificate will be configured as the previous certificate.

If you do not want to use Windows PowerShell you can also use the Certificates MMC console to export a certificate from one Front End Server and then import that same certificate on all your other Front End Servers. If you do this, make sure that you export the private key along with the certificate itself.

Caution:

In this case, the procedure must be performed on each Front End Server. When exporting and importing certificates in this manner Lync Server 2013 will not replicate that certificate to each Front End Server.

After the certificate has been imported to all your Front End Servers, that certificate can then be assigned by using the Lync Server Deployment Wizard instead of Windows PowerShell. To assign a certificate by using the Deployment Wizard, complete the following steps on a computer where the Deployment Wizard has been installed:

1. Click Start, click All Programs, click **Microsoft Lync Server 2013 (Technical Preview)**, and then click **Lync Server Deployment Wizard**.
2. In the Deployment Wizard, click **Install or Update Lync Server System**.
3. On the **Lync Server 2013 (Technical Preview)** page, click the **Run** button under the heading **Step 3: Request, Install or Assign Certificates**. (Note: If you have already installed certificates on this computer then the **Run** button will be labeled **Run Again**.)
4. In the Certificate Wizard, select the **OAuthTokenIssuer** certificate and then click **Assign**.
5. In the Certificate Assignment wizard, on the **Certificate Assignment** page, click **Next**.
6. On the **Certificate Store** page, select the certificate to be used for server-to-server authentication and then click **Next**.
7. On the Certificate Assignment Summary page, click **Next**.
8. On the Executing Commands page, click **Finish**.
9. Close the Certificate Wizard and the Deployment Wizard.

Configuring an On-Premises Partner Application for Microsoft Lync Server 2013

Microsoft Lync Server 2013 > Deployment > Managing Server-to-Server Authentication (Oauth) and Partner Applications >

Topic Last Modified: *2013-02-04*

After you have assigned the OAuthTokenIssuer certificate you must then configure your Microsoft Lync Server 2013 partner applications. (The procedure about to be discussed configures both Microsoft Exchange Server 2013 and Microsoft SharePoint to act as partner applications.) To configure an on-premises partner application, you must start by copying the following Windows PowerShell script and pasting the code into Notepad (or any other text editor):

```
if ((Get-CsPartnerApplication -ErrorAction SilentlyContinue) -ne $Null)
   {
       Remove-CsPartnerApplication app
   }
$exch = Get-CsPartnerApplication microsoft.exchange -ErrorAction SilentlyContinue
if ($exch -eq $null)
   {
      New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl https://
    }
else
    {
       if ($exch.ApplicationIdentifier -ne "00000002-0000-0ff1-ce00-000000000000"
          {
             Remove-CsPartnerApplication microsoft.exchange
New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl https://atl-ex
           }
        else
           {
             Set-CsPartnerApplication -Identity microsoft.exchange -ApplicationTr
           }
     }
$shp = Get-CsPartnerApplication microsoft.sharepoint -ErrorAction SilentlyContinu
if ($shp -eq $null)
   {
      New-CsPartnerApplication -Identity microsoft.sharepoint -MetadataUrl http:/
    }
else
    {
       if ($shp.ApplicationIdentifier -ne "00000003-0000-0ff1-ce00-000000000000")
          {
             Remove-CsPartnerApplication microsoft.sharepoint
             New-CsPartnerApplication -Identity microsoft.sharepoint -MetadataUrl
           }
        else
           {
             Set-CsPartnerApplication -Identity microsoft.sharepoint -Application
            }
   }
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000
```

After copying the code, save the script using a .PS1 file extension (for example, C:\Scripts \ServerToServerAuth.ps1). Note that, before you run this script, you must replace the metadata URLs https://atl-exchange-001.litwareinc.com/autodiscover/metadata/json/1 and http://atl-sharepoint-001.litwareinc.com/jsonmetadata.ashx with the metadata URLs used by your Exchange 2013 and SharePoint servers, respectively. See the product documentation for Exchange 2013 and SharePoint for information on how you can identify the respective product's metadata URL.

If you look at the last line of the script you will notice that the Set-CsOAuthConfiguration cmdlet is called using this syntax:

```
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000
```

Because the Realm parameter was not used when calling Set-CsOAuthConfiguration the realm will automatically be set to the fully qualified domain name (FQDN) of your organization (for example, litwareinc.com). If your realm name is different from your organization name then you should include the realm name, like this:

```
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000 -Realm
```

After making these changes you can then execute the script, and configure both Exchange 2013 and SharePoint as partner applications, by running the script file from within the Lync Server 2013 Management Shell. For example:

```
C:\Scripts\ServerToServerAuth.ps1
```

Note that you can run this script even if you do not have both Exchange 2013 and SharePoint Server installed:, no problems will occur if you, say, configure SharePoint Server as a partner application even though you do not have SharePoint Server installed.

When you run this script you might receive an error message similar to the following:

```
New-CsPartnerApplication : Cannot bind parameter 'MetadataUrl' to the target. Exc
```

This error message typically means one of two things: 1) that one of the URLs specified in the script is not valid (that is, one of your metadata URLs is not an actual metadata URL); or, 2) one of the metadata URLs could not be contacted. If this happens, verify that the URLs are correct and are accessible, and the re-run the script.

After creating the partner application for Lync Server 2013 you must then configure Lync Server to be a partner application for Exchange 2013. You can configure partner applications for Exchange 2013 by running the script Configure-EnterprisePartnerApplication.ps1; all you need to do is specify the metadata URL for Lync Server and indicate that Lync Server is the new partner application.

To configure Lync Server as a partner application for Exchange, open the Exchange Management Shell and run a command similar to this

```
"c:\Program Files\Microsoft\Exchange Server\V15\Scripts\Configure-EnterprisePartn
```

1.7.13.2.3 Configuring Microsoft Lync Server 2013 in a Cross-Premises Environment

Configuring Microsoft Lync Server 2013 in a Cross-Premises Environment

Microsoft Lync Server 2013 > Deployment > Managing Server-to-Server Authentication (Oauth) and Partner Applications >

Topic Last Modified: *2012-10-02*

In a cross-premise configuration, some of your users are homed on an on-premises installation of Microsoft Lync Server 2013 while other users are homed on the Office 365 version of Lync Server. In order to configure server-to-server authentication in a cross-premises environment, you must first configure your on-premises installation of Lync Server 2013 to trust the Office 365 Authorization server. The initial step in this process can be carried out by running the following Lync Server Management Shell script:

```
$TenantID = (Get-CsTenant -DisplayName "Fabrikam.com").TenantId
$sts = Get-CsOAuthServer microsoft.sts -ErrorAction SilentlyContinue
   if ($sts -eq $null)
      {
         New-CsOAuthServer microsoft.sts -MetadataUrl "https://accounts.accesscon
      }
   else
      {
         if ($sts.MetadataUrl -ne  "https://accounts.accesscontrol.windows.net/$T
            {
               Remove-CsOAuthServer microsoft.sts
               New-CsOAuthServer microsoft.sts -MetadataUrl "https://accounts.acc
            }
        }
$exch = Get-CsPartnerApplication microsoft.exchange -ErrorAction SilentlyContinue
if ($exch -eq $null)
   {
      New-CsPartnerApplication -Identity microsoft.exchange -ApplicationIdentifie
    }
else
    {
       if ($exch.ApplicationIdentifier -ne "00000002-0000-0ff1-ce00-000000000000"
          {
             Remove-CsPartnerApplication microsoft.exchange
             New-CsPartnerApplication -Identity microsoft.exchange -ApplicationId
          }
       else
          {
             Set-CsPartnerApplication -Identity microsoft.exchange -ApplicationTr
          }
   }
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000
```

Keep in mind that the realm name for a tenant is typically different than the organization name; in fact, the realm name is almost always the same as the tenant ID. Because of that, the first line in the script is used to return the value of the TenantId property for the specified tenant (in this case, fabrikam.com) and then assign that name to the variable $TenantId:

```
$TenantID = (Get-CsTenant -DisplayName "Fabrikam.com").TenantId
```

After the script completes you must then configure a trust relationship between Lync Server 2013 and the authorization server, and a second trust relationship between Exchange 2013 and the authorization server. This can only be done by using the Microsoft Online Services cmdlets.

Note:

If you have not installed the Microsoft Online Services cmdlets you will need to do two things before proceeding. First, download and install the 64-bit version of the Microsoft Online Services Sign-in Assistant. After installation is complete, download and install the 64-bit version of the Microsoft Online Services Module for Windows PowerShell. Detailed information for installing and using the Microsoft Online Services Module can be found on the Office 365 web site. These instructions will also tell you how to configure single sign-on, federation, and synchronization between Office 365 and Active Directory.

After you have configured Office 365, and after you have created Office 365 service principals for Lync Server 2013 and Exchange 2013, you will then need to register your credentials with these service principals. In order to do this, you must first obtain an X.509 Base64 saved as a .CER file. This certificate will then be applied to the Office 365 service principals.

When you have obtained the X.509 certificate, start the Microsoft Online Services Module (click **Start**, click **All Programs**, click **Microsoft Online Services**, and then click **Microsoft Online Services Module for Windows PowerShell**). After the Services Module opens, type the following to import the Microsoft Online Windows PowerShell module containing the cmdlets that can be used to manage service principals:

```
Import-Module MSOnlineExtended
```

When the module has been imported, type the following command and then press ENTER in order to connect to Office 365:

```
Connect-MsolService
```

After you press ENTER, a credentials dialog box will appear. Enter your Office 365 user name and password in the dialog box, and then click OK.

As soon as you are connected to Office 365 you can then run the following command in order to return information about your service principals:

```
Get-MsolServicePrincipal
```

You should get back information similar to this for all your service principals:

```
ExtensionData        : System.Runtime.Serialization.ExtensionDataObject
AccountEnabled       : True
Addresses            : {}
AppPrincipalId       : 00000004-0000-0ff1-ce00-000000000000
DisplayName          : Microsoft Lync Server
ObjectId             : aada5fbd-c0ae-442a-8c0b-36fec40602e2
ServicePrincipalName : LyncServer/litwareinc.com
TrustedForDelegation : True
```

The next step is to import, encode, and assign the X.509 certificate. To import and encode the certificate, use the following Windows PowerShell commands, being sure to specify the complete file path to your .CER file when you call the Import method:

```
$certificate = New-Object System.Security.Cryptography.X509Certificates.X509Certi
$certificate.Import("C:\Certificates\Office365.cer")
$binaryValue = $certificate.GetRawCertData()
$credentialsValue = [System.Convert]::ToBase64String($binaryValue)
```

After the certificate has been imported and encoded, you can then assign the certificate to your Office 365 service principals. To do that, first use the Get-MsolServicePrincipal to retrieve the value of the AppPrincipalId property for both the Lync Server and the Microsoft Exchange service principals; the value of the AppPrincipalId property will be used to identify the service principal being assigned the certificate. With the AppPrincipalId property value for Lync Server 2013 in hand, use the following command to assign the certificate to the Office 365 version of Lync Server (the StartDate and EndDate properties should correspond to the validity period for the certificate):

```
New-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000000
```

You should then repeat the command, this time using the AppPrincipalId property value for Exchange 2013.

If you later need to delete that certificate, you can do so by first retrieving the KeyId for the certificate:

```
Get-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000000
```

That command will return data like this one:

```
Type      : Asymmetric
Value     :
KeyId     : bc2795f3-2387-4543-a95d-f92c85c7a1b0
StartDate : 6/1/2012 8:00:00 AM
EndDate   : 5/31/2013 8:00:00 AM
Usage     : Verify
```

You can then delete the certificate by using a command similar to this:

```
Remove-MsolServicePrincipalCredential -AppPrincipalId 00000004-0000-0ff1-ce00-000
```

In addition to assigning a certificate you must also configure the Exchange Online Service Principal and configure your on-premise version of Lync Server 2013 as an Office 365 service principal. That can be done by carrying out the following two commands:

```
Set-MSOLServicePrincipal -AppPrincipalID 00000002-0000-0ff1-ce00-000000000000 -Ac
$lyncSP = Get-MSOLServicePrincipal -AppPrincipalID 00000004-0000-0ff1-ce00-000000
$lyncSP.ServicePrincipalNames.Add("00000004-0000-0ff1-ce00-000000000000/lync.cont
Set-MSOLServicePrincipal -AppPrincipalID 00000004-0000-0ff1-ce00-000000000000 -Se
```

1.7.13.3 Configuring Security

Configuring Security

See Also

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Security and Authentication >

Topic Last Modified: *2013-02-21*

Topics in this section provide step-by-step procedures for tasks you can perform using the **Security** group in Lync Server 2013 Control Panel.

- Create Registrar Configuration Settings
- Modify Existing Registrar Configuration Settings
- Delete Existing Registrar Configuration Settings
- Create New Web Service Configuration Settings
- Modify Existing Web Service Configuration Settings
- Delete Existing Web Service Configuration Settings

⊟See Also

Other Resources

Managing Meetings and Conferences

1.7.13.3.1 Create Registrar Configuration Settings

Create Registrar Configuration Settings

Operations > Managing Lync Server 2013 Security and Authentication > Configuring Security >

Topic Last Modified: *2012-11-01*

You can use the Registrar to configure proxy server authentication methods. The authentication protocol you specify determines which type of challenges the servers in the pool issue to clients. The available protocols are:

- **Kerberos** This is the strongest password-based authentication scheme available to clients, but it is normally available only to enterprise clients because it requires client connection to a Key Distribution Center (Kerberos domain controller). This setting is appropriate if the server authenticates only enterprise clients.
- **NTLM** This is the password-based authentication available to clients that use a challenge-response hashing scheme on the password. This is the only form of authentication available to clients without connectivity to a Key Distribution Center (Kerberos domain controller), such as remote users. If a server authenticates only remote users, you should choose NTLM.
- **Certificate authentication** This is the new authentication method when the

server needs to obtain certificates from Lync Phone Edition clients, common area phones and Lync 2013. On Lync Phone Edition clients, after a user signs in and is successfully authenticated by providing a personal identification number (PIN), Lync Server 2013 then provisions the SIP URI to the phone and provisions a Lync Server signed certificate or a user certificate that identifies Joe (Ex: SN=joe@contoso.com) to the phone. This certificate is used for authenticating with the Registrar and Web Services.

Note:

We recommend that you enable both Kerberos and NTLM when a server supports authentication for both remote and enterprise clients. The Edge Server and internal servers communicate to ensure that only NTLM authentication is offered to remote clients. If only Kerberos is enabled on these servers, they cannot authenticate remote users. If enterprise users also authenticate against the server, Kerberos is used.

Follow these steps to create a new Registrar.

⊟To create new Registrar configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **Registrar**.
4. On the **Registrar** page, click **New**
5. In **Select a Service**, click the service to which the Registrar is to be applied and then click **OK**.
6. In **New Registrar Setting**, select one or more of the following depending on the capabilities of the clients and support in your environment:
   - **Enable Kerberos authentication** to have the servers in the pool issue challenges using Kerberos authentication.
   - **Enable NTLM authentication** to have the servers in the pool issue challenges using NTLM.
   - **Enable certificate authentication** to have the servers in the pool issue certificates to clients.
7. Click **Commit**.

1.7.13.3.2 Modify Existing Registrar Configuration Settings

Modify Existing Registrar Configuration Settings

Operations > Managing Lync Server 2013 Security and Authentication > Configuring Security >

Topic Last Modified: *2012-11-01*

You can use the Registrar to configure proxy server authentication protocols. For information about the available protocols, see Create Registrar Configuration Settings.

Note:

We recommend that you enable both Kerberos and NTLM when a server supports authentication for both remote and enterprise clients. The Edge Server and internal servers communicate to ensure that only NTLM authentication is offered to remote clients. If only Kerberos is enabled on these servers, they cannot authenticate remote users. If enterprise users also authenticate against the server, Kerberos is used.

Follow these steps to modify an existing Registrar.

⊟To modify existing registrar configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **Registrar**.
4. On the **Registrar** page, click a service, click **Edit**, and then click **Show details**.
5. In **Edit Registrar Setting**, select one or more of the following depending on the capabilities of the clients and support in your environment:
   - **Enable Kerberos authentication** to have the servers in the pool issue challenges using Kerberos authentication.
   - **Enable NTLM authentication** to have the servers in the pool issue challenges using NTLM.
   - **Enable certificate authentication** to have the servers in the pool issue certificates to clients.
6. Click **Commit**.

1.7.13.3.3 Delete Existing Registrar Configuration Settings

Delete Existing Registrar Configuration Settings

Operations > Managing Lync Server 2013 Security and Authentication > Configuring Security >

Topic Last Modified: *2013-02-23*

Follow these steps to delete a Registrar.

⊟To delete Registrar configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **Registrar**.
4. On the **Registrar** page, and in the search field, type all or part of the name of the Registrar you want to delete.
5. In the list, click the Registrar that you want, click **Edit**, and then click **Delete**.
6. Click **OK**.

Removing Registrar Configuration Settings by Using Windows PowerShell Cmdlets

You can delete the Registrar configuration settings by using Windows PowerShell and the **Remove-CsProxyConfiguration** cmdlet. You can run this cmdlet from the Lync Server

2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To remove a specific set of Registrar security settings

- The following command removes the Registrar security settings applied to the edge Server atl-edge-011.litwareinc.com:

```
Remove-CsProxyConfiguration -Identity service:EdgeServer:atl-edge-011.l
```

⊟To remove all of the Registrar security settings applied to the site scope

- The following command removes all the Registrar security settings applied to the Registrar service:

```
Get-CsProxyConfiguration -Filter "service:Registrar:*" | Remove-CsProxy
```

⊟To remove all of the Registrar security settings that allow NTLM authentication

- The following command deletes all the Registrar security settings that allow the use of NTLM for client authentication:

```
Get-CsProxyConfiguration | Where-Object {$_.UseNtlmForClientToProxyAuth
```

For details, see Remove-CsProxyConfiguration.

1.7.13.3.4 Create New Web Service Configuration Settings

Create New Web Service Configuration Settings

Operations > Managing Lync Server 2013 Security and Authentication > Configuring Security >

Topic Last Modified: *2012-11-01*

You can use the **Web Service** page to configure the authentication methods for accessing Lync Server 2013 related web servers and Web Services.

Follow these steps to create a new Web Service policy.

⊟To create new web service configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **Web Service**.
4. On the **Web Service** page, click **New**, and then do one of the following:
   - To configure the Web Service for a site, click **Site configuration**. In **Select a Site**, click the site to which the Web Service policy will be applied a site and click **OK**.
   - To configure the Web Service for a pool, click **Pool configuration**. In **Select a Service**, click the service to which the Web Service policy will be applied and click **OK**.
5. In **New Web Service Setting**, in **Integrated Windows authentication**, select **Negotiate**, **Integrated Windows authentication**, or **None**.

6. Select one or more of the following depending on the capabilities of the clients and support in your environment:
   - **Enable PIN Authentication** to enable clients to be authenticated using PIN numbers.
   - **Enable certificate authentication** to have the servers in the pool issue certificates to clients.
   - **Enable certificate chain download** to have servers presented with an authentication certificate download the certificate chain for that certificate.

7. Click **Commit**.

1.7.13.3.5 Modify Existing Web Service Configuration Settings

Modify Existing Web Service Configuration Settings

See Also

Operations > Managing Lync Server 2013 Security and Authentication > Configuring Security >

Topic Last Modified: *2012-11-01*

You can use the **Web Service** page to configure the authentication methods for accessing Lync Server 2013 related web servers and Web Services.

Follow these steps to modify an existing Web Service policy.

⊟To modify existing Web service configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **Web Service**.
4. On the **Web Service** page, click a configuration, click **Edit**, and then click **Show details**.
5. In **Edit Web Service Setting**, in **Integrated Windows authentication**, select **Negotiate**, **Integrated Windows authentication**, or **None**.
6. Select one or more of the following depending on the capabilities of the clients and support in your environment:
   - **Enable PIN Authentication** to enable clients to be authenticated using PIN numbers.
   - **Enable certificate authentication** to have the servers in the pool issue certificates to clients.
   - **Enable certificate chain download** to have servers presented with an authentication certificate download the certificate chain for that certificate.
7. Click **Commit**.

Other Resources

Configuring Security

1.7.13.3.6 Delete Existing Web Service Configuration Settings

Delete Existing Web Service Configuration Settings

See Also

Operations > Managing Lync Server 2013 Security and Authentication > Configuring Security >

Topic Last Modified: *2013-02-23*

Follow these steps to delete web service configuration settings.

To delete web service configuration settings

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **Web Service**.
4. On the **Web Service** page, and in the search field, type all or part of the name of the policy you want to delete.
5. In the list of policies, click the policy that you want, click **Edit**, and then click **Delete**.
6. Click **OK**.

Deleting Web Service Configuration Settings by Using Windows PowerShell Cmdlets

You can delete web service configuration settings by using Windows PowerShell and the **Remove-CsWebServiceConfiguration** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To delete a specific collection of web service configuration settings

- The following command removes the Web Service security settings applied to the Redmond site:

```
Remove-CsWebServiceConfiguration -Identity "site:Redmond"
```

To delete all of the web service configuration settings applied to the site scope

- The following command removes all of the Web Service security settings applied to the service scope:

```
Get-CsWebServiceConfiguration -Filter "service:*" | Remove-CsWebService
```

To delete all of the web service configuration settings that allow certificate authentication

- The following command removes all the Web Service security settings that allow the use of certificate authentication:

```
Get-CsWebServiceConfiguration | Where-Object {$_.UseCertificateAuth -eq
```

For details, see Remove-CsWebServiceConfiguration.

See Also

Other Resources

Configuring Security

1.7.13.4 Managing PIN Settings

Managing PIN Settings

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Security and Authentication >

Topic Last Modified: *2012-11-01*

Use the procedures in the following section to manage PIN settings in Lync Server 2013.

- Managing PIN Policies
- Managing User PINs

1.7.13.4.1 Managing PIN Policies

Managing PIN Policies

See Also

Operations > Managing Lync Server 2013 Security and Authentication > Managing PIN Settings >

Topic Last Modified: *2012-11-01*

You can manage Lync Server 2013 PIN polices from either Lync Server 2013 Control Panel or Lync Server Management Shell. Use the following procedures to configure PIN policies for your organization.

- View PIN Policy Inforrmation
- Create a New PIN Policy
- Modify an Existing PIN Policy
- Delete a PIN Policy
- Assign a Per-User PIN Policy

⊟See Also

Other Resources

Managing User PINs

1.7.13.4.1.1 View PIN Policy Inforrmation

View PIN Policy Inforrmation

See Also

Managing Lync Server 2013 Security and Authentication > Managing PIN Settings > Managing PIN Policies >

Topic Last Modified: *2013-02-23*

You can use the **PIN Policy** tab to view personal identification number (PIN) authentication of users who are connecting to Lync 2013 with IP Phones. To use PIN authentication, make sure that **Enable PIN Authentication** is selected in Web Service settings. For details, see Modify Existing Web Service Configuration Settings.

Follow these steps to modify a user-level or a site-level PIN policy.

⊟To view information about a PIN policy in Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins

group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **PIN Policy**.
4. On the **PIN Policy** page, click a policy, click **Edit**, and then click **Show details**.

Viewing PIN Policies by Using Windows PowerShell Cmdlets

You can also view PIN policies by using Windows PowerShell and the Get-CsPinPolicy cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view PIN policies

- To view information about all your PIN policies, type the following command in the Lync Server Management Shell and then press ENTER:

```
Get-CsPinPolicy
```

That will return information similar to this:

```
Identity             : Global
Description          :
MinPasswordLength    : 5
PINHistoryCount      : 0
AllowCommonPatterns  : False
PINLifetime          : 0
MaximumLogonAttempts :
```

For more information, see the help topic for the Get-CsPinPolicy cmdlet.

See Also

Tasks

Modify Existing Web Service Configuration Settings
Create a New PIN Policy

1.7.13.4.1.2 Create a New PIN Policy

Create a New PIN Policy

Managing Lync Server 2013 Security and Authentication > Managing PIN Settings > Managing PIN Policies >

Topic Last Modified: *2012-06-19*

You can use the **PIN Policy** page to provide personal identification number (PIN) authentication to users who are connecting to Lync 2013 with IP Phones. To use PIN authentication, make sure that **Enable PIN Authentication** is selected in Web Service settings. For details, see Modify Existing Web Service Configuration Settings.

Follow these steps to create a user-level or a site-level PIN policy.

To create a user or site PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **PIN Policy**.
4. On the **PIN Policy** page, click **New**, and then do one of the following:
   - To create a user-level policy, click **User policy**. In **New PIN Policy**, in **Name**, type a name that describes the policy.
   - To create a site-level policy, click **Site policy**. In the **Select a Site** search field, type all or part of the name of the site for which you want to create a policy. In the resulting list of sites, click the site you want, and then click **OK**.
5. In the **Description** field, type a description of the PIN policy.
6. In the **Minimum PIN length** field, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
7. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum number of attempts is automatically determined.
8. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
9. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
10. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
11. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
12. To allow common patterns of digits in PINs, such as sequential numbers and repetitive sets of numbers, select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

Important:
We recommend that you do not allow common patterns.

13. Click **Commit**.

1.7.13.4.1.3 Modify an Existing PIN Policy

Modify an Existing PIN Policy

Managing Lync Server 2013 Security and Authentication > Managing PIN Settings > Managing PIN Policies >

Topic Last Modified: *2012-06-19*

You can use the **PIN Policy** tab to provide personal identification number (PIN) authentication to users who are connecting to Lync 2013 with IP Phones. To use PIN authentication, make sure that **Enable PIN Authentication** is selected in Web Service settings. For details, see Modify Existing Web Service Configuration Settings.

Follow these steps to modify a user-level or a site-level PIN policy.

⊟To modify an existing PIN policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **PIN Policy**.
4. On the **PIN Policy** page, click a policy, click **Edit**, and then click **Show details**.
5. In **Edit PIN Policy**, in **Minimum PIN length**, type or select the minimum PIN length that you want to allow. The default minimum length is five digits.
6. To be able to specify the maximum number of logon attempts before a user is locked out, select the **Specify maximum logon attempts** check box. If you do not select this option, the maximum number of allowed attempts is automatically determined based on the PIN length. By default, the maximum number of attempts is automatically determined.
7. If you selected the **Specify maximum logon attempts** check box, in **Maximum logon attempts**, type or select the maximum number of logon attempts that you want to allow.
8. To have PINs expire, select the **Enable PIN expiration** check box. If you do not select this option, PINs will never expire. By default, PINs never expire.
9. If you selected the **Enable PIN expiration** check box, in **PIN expires after (days)**, type or select the number of days after which PINs expire.
10. In **PIN history count**, type the number of PINs that a user must create before the user can reuse a PIN. By default, users can reuse their PINs.
11. To allow common patterns of digits in PINs, such as sequential numbers and repetitive sets of numbers, select the **Allow common patterns** check box. If you do not select this option, only complex patterns of digits are allowed. By default, only complex patterns of digits are allowed.

Important:
We recommend that you do not allow common patterns.

12. Click **Commit**.

1.7.13.4.1.4 Delete a PIN Policy

Delete a PIN Policy

Managing Lync Server 2013 Security and Authentication > Managing PIN Settings > Managing PIN Policies >

Topic Last Modified: *2013-02-23*

Follow these steps to delete a personal identification number (PIN) policy.

Note:
You cannot delete the global PIN policy.

⊟To delete a PIN policy in Lync Server 2013 Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Security** and then click **PIN Policy**.
4. On the **PIN Policy** page, and in the search field, type all or part of the name

of the policy you want to delete.

5. In the list of policies, click the policy that you want, click **Edit**, and then click **Delete**.
6. Click **OK**.

Removing PIN Policies by Using Windows PowerShell Cmdlets

You can delete PIN policies by using Windows PowerShell and the Remove-CsPinPolicy cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specific PIN policy

- This command removes the PIN policy with the Identity RedmondPinPolicy:

```
Remove-CsPinPolicy -Identity "RedmondPinPolicy"
```

To remove all the PIN policies applied to the site scope

- This command removes all the PIN policies configured at the site scope:

```
Get-CsPinPolicy -Filter "site:*" | Remove-CsPinPolicy
```

To remove all the PIN policies that allow the use of common patterns

- And this one removes all the PIN policies that allow the use of common patterns:G

```
et-CsPinPolicy | Where-Object {$_.AllowCommonPatterns -eq $True} | Remo
```

For more information, see the help topic for the Remove-CsPinPolicy cmdlet.

1.7.13.4.1.5 Assign a Per-User PIN Policy

Assign a Per-User PIN Policy

See Also

[Managing Users in Lync Server 2013](#) > [User Accounts Enabled for Lync Server 2013](#) > [Assigning Per-User Policies](#) >

Topic Last Modified: *2013-02-22*

The dial-in conferencing personal identification number (PIN) policy is one of the individual settings of a user account that can be configured in the Lync Server 2013 Control Panel.

Deploying one or more per-user PIN policies is optional. You can also deploy only a global-level PIN policy or site-level PIN policy. If you do deploy per-user policies, you must explicitly assign them to users, groups, or contact object. User rights and permissions regarding the use of PINs for dial-in conferencing automatically default to those defined in the global-level PIN policy when no specific site-level or per-user policy is assigned.

After creating at least one per-user PIN policy, use the procedures in this topic to assign the policy that specifies the constraints you want the server to impose on the PINs created by and used by a particular user.

For details about creating per-user dial-in conferencing PIN policies, see [Create or Modify](#)

Dial-in Conferencing PIN Settings for a Site or Group of Users.

To assign a per-user PIN policy

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

     > **Tip:**
     > To add additional search clauses to your query, click **Add Filter**.

   - Click **Find**.
6. Click a user in the search results, click **Action**, and then click **Assign policies**.

   > **Tip:**
   > If you want the same per-user PIN policy to apply to multiple users, select multiple users in the search results, then click **Actions**, and then click **Assign policies**.

7. In **Assign Policies**, under **PIN policy**, do one of the following:

   > **Note:**
   > Because there are multiple policies that you can configure by using the **Assign Policies** dialog box, **<Keep as is>** is selected by default for every policy in the dialog box. Continue using the policy previously assigned to the user by making no changes to this setting.

   - Allow Lync Server 2013 to automatically choose either the global-level policy or, if defined, the site-level policy.
   - Click the name of a per-user PIN policy you previously defined on the **PIN Policy** page.

     > **Tip:**
     > To help you decide the policy you want to assign, after you click a policy name, click **View** to view the user rights and permissions defined in the policy.

8. When you are finished, click **OK**.

Assigning a Per-User PIN Policy by Using Windows PowerShell Cmdlets

You can assign per-user PIN policies by using Windows PowerShell and the **Grant-**

CsPinPolicy cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To assign a per-user PIN policy to a single user

- The following command assigns the per-user PIN policy RedmondPinPolicy to the user Ken Myer.

```
Grant-CsPinPolicy -Identity "Ken Myer" -PolicyName "RedmondPinPolicy"
```

To assign a per-user PIN policy to multiple users

- The following command assigns the per-user PIN policy RedmondUsersPinPolicy to all the users who work in the city of Redmond. For details about the LdapFilter parameter used in this command, see Get-CsUser.

```
Get-CsUser -LdapFilter "l=Redmond" | Grant-CsPinPolicy -PolicyName "Red
```

To unassign a per-user PIN policy

- The following command unassigns any per-user PIN policy previously assigned to Ken Myer. After the per-user policy is unassigned, Ken Myer will automatically be managed by using the global policy or, if one exists, his local site policy. A site policy takes precedence over the global policy.

```
Grant-CsPinPolicy -Identity "Ken Myer" -PolicyName $Null
```

For details, see Grant-CsPinPolicy.

See Also

Tasks

Create a New PIN Policy

Other Resources

Assigning Per-User Policies

1.7.13.4.2 Managing User PINs

Managing User PINs

See Also

Operations > Managing Lync Server 2013 Security and Authentication > Managing PIN Settings >

Topic Last Modified: *2012-10-15*

Use the following procedures to manage users' dial-in conferencing PINs from the **Users** section of Lync Server 2013 Control Panel.

- Set a User's Dial-in Conferencing PIN
- View User PIN information
- Lock or Unlock a User PIN

See Also

Tasks

Assign a Per-User PIN Policy

1.7.13.4.2.1 Set a User's Dial-in Conferencing PIN

Set a User's Dial-in Conferencing PIN

See Also

Managing Lync Server 2013 Security and Authentication > Managing PIN Settings > Managing User PINs >

Topic Last Modified: *2013-02-23*

To join a dial-in conference as an authenticated user, a Lync Server 2013 user with Active Directory Domain Services (AD DS) credentials requires a personal identification number (PIN). If a user forgets the dial-in conferencing PIN or has not set the PIN by using Lync Server, you can set the user’s PIN from Lync Server Control Panel. You can automatically generate the PIN or create one manually.

Note:

Specific characteristics of the PIN, such as its minimum length, can be configured as a policy. In addition to the global policy, you can configure a PIN policy for individual sites or users. For details about configuring a PIN policy, see Configure Dial-in Conferencing Personal Identification Number (PIN) Rules.

⊟To set a user’s PIN

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria that you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

     Tip:

     To add additional search clauses to your query, click **Add Filter**.
   - Click **Find**.

   Note:

   If the PIN is locked, you must unlock the PIN before you can set it. To unlock the PIN, click the user, click **Action**, and then click **Unlock PIN**.
6. Click a user in the search results, click **Action**, and then click **Set PIN**.
7. In the **Set PIN** dialog box, do one of the following:
   - To allow Lync Server 2013 to generate the user’s PIN, select **Automatically generate a valid PIN** (the default).
   - To create your own PIN, click **Manually enter a specific PIN**, click the text

box, and then type a PIN that meets the PIN requirements specified in your PIN policy settings.

8. Click **OK**.
9. In **Set PIN**, do one of the following:
    - Select the **Show PIN** check box to see the PIN, and then copy the PIN and communicate it to the user using your organization's preferred method.
    - Click **Open my email application to send the new PIN to the user** to send the PIN by email. If Microsoft Office Outlook is your email client, the PIN is automatically copied into a new email message. If you use a different email client, select the **Show PIN** check box to see the PIN and then copy it into your email message.
10. Click **Close**.

Assigning a User PIN by Using Windows PowerShell Cmdlets

You can assign PIN numbers can also be assigned by using the Set-CsClientPin cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To auto-assign a PIN number to a user

- The following command assigns a PIN number to the user Ken Myer. Because the Pin parameter is not included, Lync Server will automatically generate and assign the PIN number.

```
Set-CsClientPin -Identity "Ken Myer" -Pin 18723834
```

To assign a specific PIN number to a user

- This command uses the Pin parameter to assign the PIN number 121989 to the user Ken Myer.

```
Set-CsClientPin -Identity "Ken Myer" -Pin 121989
```

For more information, see the help topic for the Set-CsClientPin cmdlet.

See Also

Concepts

Dial-in Access Number

Other Resources

Configure Dial-in Conferencing Personal Identification Number (PIN) Rules

1.7.13.4.2.2 View User PIN information

View User PIN information

See Also

Managing Lync Server 2013 Security and Authentication > Managing PIN Settings > Managing User PINs >

Topic Last Modified: *2013-02-23*

To join a dial-in conference as an authenticated user, a Lync Server 2013 user with Active Directory Domain Services (AD DS) credentials requires a personal identification number

(PIN). You can view a user’s PIN information from Lync Server 2013 Control Panel.

Note:

You can view PIN status information such as whether the PIN has been set or when the PIN was last changed, but you cannot see the current PIN by looking at the PIN status. If a user has lost their PIN, you can reset it by following the procedures in Set a User's Dial-in Conferencing PIN

To view a user’s PIN in Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria that you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

     Tip:

     To add additional search clauses to your query, click **Add Filter**.
   - Click **Find**.

   Note:

   If the PIN is locked, you must unlock the PIN before you can set it. To unlock the PIN, click the user, click **Action**, and then click **Unlock PIN**.
6. Click a user in the search results, click **Action**, and then click **View PIN status**.

Viewing User PIN Information by Using Windows PowerShell cmdlets

You can view user PIN information by using the Get-CsClientPinInfo cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view user PIN information

- To view PIN information for a user, type a command similar to the following in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsClientPinInfo -Identity "Ken Myer"
  ```

  That will return information similar to this:

```
Identity           : sip:kenmyer@litwareinc.com
IsPinSet           : False
IsLockedOut        : False
LastPinChangeTime  : 9/25/2012 1:35:03 PM
PinExpirationTime  :
```

For more information, see the help topic for the Get-CsConferenceDisclaimer cmdlet.

See Also

Tasks

Set a User's Dial-in Conferencing PIN
Lock or Unlock a User PIN

1.7.13.4.2.3 Lock or Unlock a User PIN

Lock or Unlock a User PIN

Managing Lync Server 2013 Security and Authentication > Managing PIN Settings > Managing User PINs >

Topic Last Modified: *2013-02-23*

You can lock or unlock a user's PIN from the **Users** section of Lync Server 2013 Control Panel.

To lock a user's PIN in Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
   - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
   - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
   - Click **Add Filter**.
   - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
   - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
   - Depending on the user property you selected, enter the criteria that you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

Tip:
To add additional search clauses to your query, click **Add Filter**.

   - Click **Find**.
   - Click the user, click **Action**, and then click **Lock PIN**.

To unlock a user's PIN in Lync Server Control Panel

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync

Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.

3. In the left navigation bar, click **Users**.
4. Use one of the following methods to locate a user:
    - In the **Search users** box, type all or the first portion of the display name, first name, last name, Security Accounts Manager (SAM) account name, SIP address, or line Uniform Resource Identifier (URI) of the user account, and then click **Find**.
    - If you have a saved query, click the **Open query** icon, use the **Open** dialog box to retrieve the query (a .usf file), and then click **Find**.
5. (Optional) Specify additional search criteria to narrow the results:
    - Click **Add Filter**.
    - Enter the user property by typing it or by clicking the arrow in the drop-down list to select the property.
    - In the **Equal to** drop-down list, click the operator (for example, **Equal to** or **Not equal to**).
    - Depending on the user property you selected, enter the criteria that you want to use to filter the search results by typing it or by clicking the arrow in the drop-down list.

> **Tip:**
> To add additional search clauses to your query, click **Add Filter**.

- Click **Find**.
- Click the user, click **Action**, and then click **Unlock PIN**.

Locking and Unlocking User PINs by Using Windows PowerShell Cmdlets

You can lock and unlock user PINs by using Windows PowerShell and the Lock-CsClientPin and Unlock-CsClientPin cmdlets. You can run these cmdlets either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To lock a user PIN

- To lock a user’s PIN, use the Lock-CsClientPin cmdlet. For example:

```
Lock-CsClientPin -Identity "Ken Myer"
```

⊟To unlock a user PIN

- To unlock a user’s PIN, use the Unlock-CsClientPin cmdlet. For example:

```
Unlock-CsClientPin -Identity "Ken Myer"
```

For more information, see the help topic for the Lock-CsClientPin and Unlock-CsClientPin cmdlets.

1.7.14 Managing the Lync Server 2013 Network Infrastructure

Managing the Lync Server 2013 Network Infrastructure

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-10-15*

Microsoft Lync Server 2013 includes support for call admission control (CAC) and media bypass. To implement these features you must configure a network of regions, sites, subnets, and so on that will allow you to manage bandwidth in situations where audio and video transmissions need to be restricted. You can also use the Quality of Service (QoS) networking technology to help provide an optimal end-user experience for audio and video communications.

You can use the Lync Server Control Panel to set up and manage CAC, media bypass, and QoS. The following topics provide steps for how to do this.

- Managing Quality of Service (QoS)
- Managing Call Admission Control
- Lync Server 2013 Network Interfaces
- Prevent New Connections to Lync Server for Server Maintenance

1.7.14.1 Managing Quality of Service (QoS)

Managing Quality of Service (QoS)

Microsoft Lync Server 2013 > Planning > Network Planning for Lync Server >

Topic Last Modified: *2013-02-21*

Quality of Service (QoS) is a networking technology used in some organizations to help provide an optimal end-user experience for audio and video communications. QoS is most-commonly used on networks where bandwidth is limited: with a large number of network packets competing for a relatively small amount of available bandwidth, Quality of Service provides a way for administrators to assign higher priorities to packets carrying audio or video data. By giving these packets a higher priority, audio and video communications are likely to complete faster, and with less interruption, than network sessions involving things like file transfers, web browsing, or database backups. That's because network packets used for file transfers or database backups are assigned a "best effort" priority.

> **Note:**
>
> As a general rule, Quality of Service applies only to communication sessions on your internal network. When you implement QoS, you configure your servers and routers to support packet marking; however, you configure these devices to support packet marking in a particular manner. You cannot assume that Quality of Service will be supported on the Internet or on other networks. Even if Quality if Service is supported on other networks, there is no guarantee that QoS will be configured the same way that you configured the service on your network.

Microsoft Lync Server 2013 does not require Quality of Service; if you do not currently use QoS there is no requirement that you install the service before installing Lync Server 2013. If you experience a considerable amount of packet loss on your network the recommended way to alleviate this problem is to add additional bandwidth. If adding more bandwidth is not possible, then you might want to implement Quality of Service instead.

Lync Server 2013 offers full support for Quality of Service: that means that organizations that are already using QoS can easily integrate Lync Server into their existing network infrastructure. In order to do this you must perform the following tasks:

- Enabling QoS for Devices that Are Not Based on Windows. By default, QoS is disabled for computers and other devices (such as iPhones) that run other operating systems. Although you can use Lync Server to enable and disable Quality of Service for devices, you typically cannot use the product to modify the DSCP codes used by these devices.
- Configuring Port Ranges for Your Conferencing, Application, and Mediation

Servers. You must reserve a unique set of ports for different packet types, such as audio and video. With Lync Server 2013 you do not enable or disable Quality of Service by, say, setting a property value to True or to False. Instead, you enable Quality of Service by configuring port ranges and then creating and applying Group Policy. If you later decide not to use QoS you can “disable” Quality of Service simply by removing the appropriate Group Policy objects.

- Configuring Port Ranges for Your Edge Servers. Although not required, you can configure your Edge servers to use the same port ranges as your other servers.
- Configuring Port Ranges for Your Microsoft Lync Clients. These port ranges apply only to client computers and are typically not the same as the port ranges configured on your servers.
- Configuring a Quality of Service Policy for Your Conferencing, Application, and Mediation Servers. These policies determine the DSCP codes that are applied to different packet types.
- Configuring a Quality of Service Policy for Your A/V Edge Servers. This should only be done for the internal side of your Edge servers. That's because Quality of Service is designed for use on your internal network and not on the Internet.
- Configuring Quality of Service Policies for Clients Running on Windows 7 or Windows 8. Note that Microsoft Lync Server 2013 does not support QoS for other Windows operating systems, such as Windows Vista or Windows XP.
- Configuring Quality of Service on Microsoft Lync Phone Edition Devices. By default, QoS is enabled for Lync Phone Edition devices. However, you might want to change the default DSCP value in order to ensure that all audio packets in your organization use the same DSCP code.

Note:

If you are using Microsoft Windows Server 2012 you might be interested in the new set of Windows PowerShell cmdlets available for managing Quality of Service on that platform. For more information, see Network Quality of Service Cmdlets in Windows PowerShell at http://go.microsoft.com/fwlink/p/?LinkId=285379.

1.7.14.1.1 Enabling QoS for Devices that Are Not Based on Windows

Enabling QoS for Devices that Are Not Based on Windows

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Quality of Service (QoS) >

Topic Last Modified: *2012-11-01*

When you install Microsoft Lync Server 2013, Quality of Service (QoS) will not be enabled for any devices used in your organization that use an operating system other than Windows. You can verify this by running the following command from within the Lync Server 2013 Management Shell:

```
Get-CsMediaConfiguration
```

Assuming you have not made any changes to your media configuration settings you should get back information similar to this:

```
Identity                          : Global
EnableQoS                         : False
EncryptionLevel                   : RequireEncryption
EnableSiren                       : False
MaxVideoRateAllowed               : VGA600K
EnableG722StereoCodec             : True
EnableH264Codec                   : True
```

```
EnableAdaptiveBandwidthEstimation : True
```

If the EnableQoS property is set to False (as in the preceding output) that means that Quality of Service is not enabled for computers and devices that use an operating system other than Windows. QoS is enabled by default for Lync Phone Edition devices; however, it is possible to disable Quality of Service for Lync Phone Edition.

To enable Quality of Service at the global scope, run the following command from within the Lync Server Management Shell:

```
Set-CsMediaConfiguration -EnableQoS $True
```

The preceding command enables QoS at the global scope; however, it's important to note that media configuration settings can also be applied to the site scope. If you need to enable Quality of Service for a site you must include the Identity of the configuration settings when calling Set-CsMediaConfiguration. For example, this command enables QoS for the Redmond site:

```
Set-CsMediaConfiguration -Identity site:Redmond -EnableQoS $True
```

Note:

Do you need to enable QoS at the site scope? That depends. Settings assigned to the site scope take precedence over settings assigned to the global scope. Suppose you have QoS enabled at the global scope but disabled at the site scope (for the Redmond site.) In that case, Quality of Service will be disabled for the Redmond site; that's because the site settings take precedence. To enable QoS for the Redmond site you will have to do so using the media configuration settings applied to that site.

If you want to simultaneously enable QoS for all your media configuration settings (regardless of scope) then run this command from within the Lync Server Management Shell:

```
Get-CsMediaConfiguration | Set-CsMediaConfiguration -EnableQoS $True
```

You can disable QoS for devices that use an operating system other than Windows by setting the value of the EnableQoS property to False. For example:

```
Set-CsMediaConfiguration -Identity site:Redmond -EnableQoS $False
```

This gives you the ability to implement QoS on some portions of your network (for example, on the Redmond site) while leaving Quality of Service disabled on other portions of your network.

QoS can only be enabled and disabled by using Windows PowerShell These options are not available in the Lync Server Control Panel.

1.7.14.1.2 Configuring Port Ranges for Your Conferencing, Application, and Mediation Servers

Configuring Port Ranges for Your Conferencing, Application, and Mediation Servers

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Quality of Service (QoS) >

Topic Last Modified: *2012-11-01*

In order to implement Quality of Service, you should configure identical port ranges for audio, video, and application sharing on your Conferencing, Application, and Mediation servers; furthermore, those port ranges must not overlap in any way. To use a simple example, suppose you use ports 10000 through 10999 for video on your Conferencing servers. That means that you must also reserve ports 10000 through 10999 for video on your Application and Mediation servers. If you do not, QoS will not work as expected.

Similarly, suppose you reserve ports 10000 through 10999 for video, but then reserve ports 10500 through 11999 for audio. This can create problems for Quality of Service, because the port ranges overlap. With QoS, each modality must have a unique set of ports: if you use ports 10000 through 10999 for video, then you'll have to use a different range (for example, 11000 through 11999 for audio).

By default, audio and video port ranges do not overlap in Microsoft Lync Server 2013; however, the port ranges assigned to application sharing overlap with both the audio and video port ranges. (Which, in turn, means that none of these ranges are unique.) You can verify the existing port ranges for your Conferencing, Application, and Mediation servers by running the following three commands from within the Lync Server 2013 Management Shell:

```
Get-CsService -ConferencingServer | Select-Object Identity, AudioPortStart, Audio
Get-CsService -ApplicationServer | Select-Object Identity, AudioPortStart, AudioP
Get-CsService -MediationServer | Select-Object Identity, AudioPortStart, AudioPor
```

Warning:

As you can see in the preceding commands, each port type – audio, video, and application sharing – is assigned two separate property values: the port start and the port count. The port start indicates the first port used for that modality; for example, if the audio port start is equal to 50000 that means that the first port used for audio traffic is port 50000. If the audio port count is 2 (which is not a valid value, but is used here for illustration purposes) that means that only 2 ports are allocated for audio. If the first port is port 50000 and there are a total of two ports, that means the second port must be port 50001 (port ranges have to be contiguous). As a result, the port range for audio would be ports 50000 through 50001, inclusive.
Note, too that Application server and Mediation server only support QoS for audio; you do not need to change video or application sharing ports in your Application servers or Mediation servers.

If you run the preceding three commands you'll see that that the default port values for Lync Server 2013 are configured like this:

Property	Conferencing Server	Application Server	Mediation Server
AudioPortStart	49152	49152	49152
AudioPortCount	8348	8348	8348
VideoPortStart	57501	--	--
VideoPortCount	8034	--	--
ApplicationSharingPortStart	49152	--	--
ApplicationSharingPortCount	16383	--	--

As noted previously, when configuring Lync Server ports for QoS, you should ensure that: 1) audio port settings are identical across yours Conferencing, Application, and Mediation servers; and, 2) port ranges do not overlap. If you look closely at the preceding table, you will see that the port ranges are identical across the three server types. For example, the starting audio port is set to port 49152 on each server type, and the total number of ports reserved for audio in each server is also identical: 8348. However, the port ranges overlap: audio ports start at port 49152, but so do the ports set aside for application sharing. In order to make optimal use of Quality of Service, application sharing should be reconfigured to use a unique port range. For example, you could configure application sharing to start at port 40803 and to use 8348 ports. (Why 8348 ports? If you add those values together -- 40803 + 8348 -- that means that application sharing will use ports 40803 through port 49151. Because audio ports do not begin until port 49152, you will no longer have any overlapping port ranges.)

After you have selected the new port range for application sharing you can make your change by using the Set-CsConferencingServer cmdlet. This change does not need to be made on your Application servers or on your Mediation servers, because these servers do not handle application sharing traffic. You only need to change port values on these servers if you decide to reassign the ports used for audio traffic.

To modify the port values for application sharing on a single Conferencing server run a command similar to this from within the Lync Server Management Shell:

```
Set-CsConferenceServer -Identity ConferencingServer:atl-cs-001.litwareinc.com -Ap
```

If you want to make these changes on all your Conferencing servers you can run this command instead:

```
Get-CsService -ConferencingServer | ForEach-Object {Set-CsConferencingServer -Ide
```

After changing port settings you should stop and then restart each service affected by the changes.

It is not mandatory that your Conferencing servers, Application servers, and Mediation servers share the exact same port range; the only true requirement is that you set aside unique port ranges on all your servers. However, administration will typically be easier if you use the same set of ports on all your servers.

1.7.14.1.3 Configuring Port Ranges for Your Edge Servers

Configuring Port Ranges for Your Edge Servers

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Quality of Service (QoS) >

Topic Last Modified: *2012-10-19*

With Edge servers you do not have to configure separate port ranges for audio, video, and application sharing; likewise, the port ranges used for Edge servers do not have to match the port ranges used with your Conferencing, Application, and Mediation servers. However, to make administration easier you might want to go ahead and change your Edge server port ranges to match the port ranges on your other servers. For example, suppose you have configured your Conferencing, Application, and Mediation servers to use these port ranges:

Packet Type	Starting Port	Number of Ports Reserved
Application sharing	40803	8348
Audio	49152	8348
Video	57501	8034
Totals	--	24730

As you can see, your port ranges for audio, video, and application sharing start at port

40803 and encompass a total of 24730 ports. If you prefer, you can configure a given Edge Server to use these overall port values by running a command similar to this one from within the Lync Server Management Shell:

```
Set-CsEdgeServer -Identity EdgeServer:atl-edge-001.litwareinc.com -MediaCommunica
```

Or, use the following command to simultaneously configure all the Edge Servers in your organization:

```
Get-CsService -EdgeServer | ForEach-Object {Set-CsEdgeServer -Identity $_.Identit
```

You can verify the current port settings for your Edge Servers by using this Lync Server Management Shell command:

```
Get-CsService -EdgeServer | Select-Object Identity, MediaCommunicationPortStart,
```

1.7.14.1.4 Configuring Port Ranges for Your Microsoft Lync Clients

Configuring Port Ranges for Your Microsoft Lync Clients

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Quality of Service (QoS) >

Topic Last Modified: *2013-01-22*

By default, Lync client applications can use any port between ports 1024 and 65535 when involved in a communication session; this is because specific port ranges are not automatically enabled for clients. In order to use Quality of Service, however, you will need to reassign the various traffic types (audio, video, media, application sharing, and file transfer) to a series of unique port ranges. This can be done by using the Set-CsConferencingConfiguration cmdlet.

You can determine which port ranges are currently used for communication sessions by running the following command from within the Microsoft Lync Server 2013 Management Shell:

```
Get-CsConferencingConfiguration
```

Assuming that you have not made any changes to your conferencing settings since you installed Lync Server 2013, you should get back information that includes these property values:

```
ClientMediaPortRangeEnabled : False
ClientAudioPort             : 5350
ClientAudioPortRange        : 40
ClientVideoPort             : 5350
ClientVideoPortRange        : 40
ClientAppSharingPort        : 5350
ClientAppSharingPortRange   : 40
ClientFileTransferPort      : 5350
ClientTransferPortRange     : 40
```

If you look closely at the preceding output, you'll see two things of importance. First, the ClientMediaPortRangeEnabled property is set to False:

```
ClientMediaPortRangeEnabled : False
```

That's important because, when this property is set to False, Lync clients will use any available port between ports 1024 and 65535 when involved in a communication session; this is true regardless of any other port settings (for example, ClientMediaPort or ClientVideoPort). If you want to restrict usage to a specified set of ports (and this is something you do want to do if you plan on implementing Quality of Service) then you must first enable client media port ranges. That can be done using the following Windows PowerShell command:

```
Set-CsConferencingConfiguration -ClientMediaPortRangeEnabled $True
```

The preceding command enables client media port ranges for the global collection of conferencing configuration settings; however, these settings can also be applied to the site scope and/or the service scope (for the Conferencing Server service only). To enable client media port ranges for a specific site or server, specify the Identity of that site or server when calling Set-CsConferencingConfiguration:

```
Set-CsConferencingConfiguration -Identity "site:Redmond" -ClientMediaPortRangeEna
```

Alternatively, you can use this command to simultaneously enable port ranges for all your conferencing configuration settings:

```
Get-CsConferencingConfiguration | Set-CsConferencingConfiguration  -ClientMediaPo
```

The second thing of importance you will notice is that the sample output shows that, by default, the media port ranges set for each type of network traffic are identical:

```
ClientAudioPort            : 5350
ClientVideoPort            : 5350
ClientAppSharingPort       : 5350
ClientFileTransferPort     : 5350
```

In order to implement QoS, each of these port ranges will need to be unique. For example, you might configure the port ranges like this:

Client Traffic Type	Port Start	Port Range
Audio	50020	20
Video	58000	20
Application sharing	42000	20
File transfer	42020	20

In the preceding table, client port ranges represent a subset of the port ranges configured for your servers. For example, on the servers, application sharing was configured to use ports 40803 through 49151; on the client computers, application sharing is configured to use ports 42000 through 42019. This, too is done primarily to make administration of QoS easier: client ports do not have to represent a subset of the ports used on the server. (For example, on the client computers you could configure application sharing to use, say, ports 10000 through 10019.) However, it is recommended that you make your client port ranges a subset of your server port ranges.

In addition, you might have noticed that 8348 ports were set aside for application sharing on the servers, but only 20 ports were set aside for application sharing on the clients. This, too is recommended, but is not a hard-and-fast rule. In general, you can consider each available port to represent a single communication session: if you have 100 ports available in a port range that means that the computer in question could participate in, at most, 100 communication sessions at any given time. Because servers will likely take part in many more conversations than clients, it makes sense to open many more ports on servers than on clients. Setting aside 20 ports for application sharing on a client means that a user could participate in 20 application sharing sessions on the specified device, and all at the same time. That should prove sufficient for the vast majority of your users.

To assign the preceding port ranges to your global collection of conferencing configuration settings you can use the following Lync Server Management Shell command:

```
Set-CsConferencingConfiguration -Identity global -ClientAudioPort 50020 -ClientAu
```

Or, use this command to assign these same port ranges for all your conferencing configuration settings:

```
Get-CsConferencingConfiguration | Set-CsConferencingConfiguration-ClientAudioPort
```

Individual users must log off from Lync and then log back on before these changes will actually take effect.

Note:

You can also enable client media port ranges, and then assign those port ranges, using a single command. For example:

```
Set-CsConferencingConfiguration -ClientMediaPortRangeEnabled $True-
ClientAudioPort 50020 -ClientAudioPortRange 20 -ClientVideoPort 58000
-ClientVideoPortRange 20 -ClientAppSharingPort 42000 -
ClientAppSharingPortRange 20 - ClientFileTransferPort 42020 -
ClientFileTransferPortRange 20
```

1.7.14.1.5 Configuring a Quality of Service Policy for Your Conferencing, Application, and Mediation Servers

Configuring a Quality of Service Policy for Your Conferencing, Application, and Mediation Servers

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Quality of Service (QoS) >

Topic Last Modified: *2013-01-22*

Configuring port ranges facilitates the use of Quality of Service by ensuring that all traffic of a specified type (for example, all audio traffic) travels through the same set of ports. This makes it easy for the system to identify and mark a given packet: if port 49152 is reserved for audio traffic, then any packet traveling through port 49152 can be marked with a DSCP code that indicates that this is an audio packet. In turn, this enables routers to identify the packet as an audio packet, and give it higher priority than unmarked packets (such as packets used to copy a file from one server to another).

However, simply restricting a set of ports to a specific type of traffic does not result in packets traveling through those ports being marked with the appropriate DSCP code. In addition to defining port ranges you must also create Quality of Service policies that specify the DSCP code to be associated with each port range. For Microsoft Lync Server 2013 that typically means creating two policies: one for audio and one for video.

Quality of Service policies are most-easily created, and managed, by using Group Policy. (These same policies can also be created by using local security policies. However, that requires you to repeat the same procedure on each and every computer.) Your initial set of QoS policies (one for audio and one for video) should be applied only to Lync Server computers running the Conferencing server, Application server, and/or Mediation server services. If all of these computers are located in the same Active Directory OU then you can simply assign the new Group Policy object (GPO) to that OU. Alternatively, you can take other steps to target the new policy to the specified computers; for example, you can place the appropriate computers in a security group, then use Group Policy security filtering to apply the GPO just to that security group.

In order to create a Quality of Service policy for managing audio, log on to a computer where Group Policy Management has been installed. Open Group Policy Management (click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**) and then complete the following procedure:

1. In Group Policy Management, locate the container where the new policy should be created. For example, if all your Lync Server computers are located in an OU named Lync Server then the new policy should be created in the Lync Server OU.
2. Right-click the appropriate container and then click **Create a GPO in this domain, and Link it here**.
3. In the **New GPO** dialog box, type a name for the new Group Policy object in the **Name** box (for example, **Lync Server Audio**) and then click **OK**.
4. Right-click the newly-created policy and then click **Edit**.
5. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, right-click **Policy-based QoS**, and then click **Create new policy**.
6. In the **Policy-based QoS** dialog box, on the opening page, type a name for the new policy (e.g., **Lync Server Audio**) in the **Name** box. Select **Specify DSCP Value** and set the value to **46**. Leave **Specify Outbound Throttle Rate** unselected, and then click **Next**.
7. On the next page, make sure that **All applications** is selected and then click **Next**. This simply ensures that all applications will match packets from the specified port range with the specified DSCP code.
8. On the third page, make sure that both **Any source IP address and Any destination IP address** are selected and then click **Next**. These two settings ensure that packets will be managed regardless of which computer (IP address) sent those packets and which computer (IP address) will receive those packets.
9. On page four, select **TCP and UDP** from the **Select the protocol this QoS policy applies to** dropdown list. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the two networking protocols most-commonly used by Lync Server and its client applications.
10. Under the heading **Specify the source port number**, select **From this source port or range**. In the accompanying text box, type the port range reserved for audio transmissions. For example, if you reserved ports 49152 through ports 57500 for audio traffic enter the port range using this format: **49152:57500**. Click **Finish**.

Note:

The DSCP value of 46 is somewhat arbitrary: although DSCP 46 is often used for marking audio packets, you do not have to use DSCP 46 for audio communications. If you have already implemented QoS and you are using a different DSCP code for audio (for example, DSCP 40) then you should configure your Quality of Service policy to use that same code (i.e., 40 for audio). If you are just now implementing Quality of Service, then it is recommended that you use DSCP 46 for audio, simply because that value is commonly used to mark audio packets.

After you have created the QoS policy for audio traffic you should then create a second policy for video traffic (and, optionally, a third policy for managing application sharing traffic). To create a policy for video, follow the same basic procedure you followed when creating the audio policy, making these substitutions:

- Use a different (and unique) policy name (for example, **Lync Server Video**).
- Set the DSCP value to **34** instead of 46. (Note that you do not have to use a DSCP value of 34. The only requirement is that you use a different DSCP value for video than you used for audio.)
- Use the previously-configured port range for video traffic. For example, if you have reserved ports 57501 through 65535 for video, then set the port range to this: **57501:65535**.

If you decide to create a policy for managing application sharing traffic you must create a third policy, making the following substitutions:

- Use a different (and unique) policy name (for example, **Lync Server**

Application Sharing).

- Set the DSCP value to **24** instead of 46. (Again, you do not have to use a DSCP value of 24. The only requirement is that you use a different DSCP value for application sharing than you used for audio or for video.)
- Use the previously-configured port range for video traffic. For example, if you have reserved ports 40803 through 49151 for application sharing, then set the port range to this: **40803:49151**.

The new policies you have created will not take effect until Group Policy has been refreshed on your Lync Server computers. Although Group Policy periodically refreshes on its own, you can force an immediate refresh by running the following command on each computer where Group Policy needs to be refreshed:

```
Gpupdate.exe /force
```

This command can be run from within the Lync Server Management Shell or from any command window that is running under administrator credentials. To run a command window under administrator credentials, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.

To verify that the new QoS policies have been applied, do the following:

1. On a Lync Server computer, click **Start** and then click **Run**.
2. In the **Run** dialog box, type **regedit** and then press ENTER.
3. In Registry Editor, expand **Computer**, expand **HKEY_LOCAL_MACHINE**, expand **SOFTWARE**, expand **Policies**, expand **Microsoft**, expand **Windows**, and then click **QoS**. Under **QoS** you should see registry keys for each of the QoS policies you just created. For example, if you created two new policies (one named Lync Server Audio and the other named Lync Server Video) you should registry entries for Lync Server Audio and Lync Server Video.

To help ensure that network packets are marked with the appropriate DSCP value, you should also create a new registry entry on each computer by completing the following procedure:

1. Click **Start** and then click **Run**.
2. In the **Run** dialog box, type **regedit** and then press ENTER.
3. In the Registry Editor, expand **HKEY_LOCAL_MACHINE**, expand **SYSTEM**, expand **CurrentControlSet**, expand **services**, and then expand **Tcpip**.
4. Right-click **Tcpip**, point to **New**, and then click **Key**. After the new registry key is created, type **QoS** and then press ENTER to rename the key.
5. Right-click **QoS**, point to **New**, and then click **String Value**. After the new registry value is created, type **Do not use NLA** and then press ENTER to rename the value.
6. Double-click **Do no use NLA**. In the **Edit String** dialog box, type **1** in the **Value data** box and then click **OK**.
7. Close the Registry Editor and then reboot your computer.

1.7.14.1.6 Configuring a Quality of Service Policy for Your A/V Edge Servers

Configuring a Quality of Service Policy for Your A/V Edge Servers

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Quality of Service (QoS) >

Topic Last Modified: *2012-10-19*

In addition to creating QoS policies for your Conferencing, Application, and Mediation servers, you must also create both audio and video policies for the internal side of your A/V Edge servers. However, the policies used on your Edge servers are different from the policies used on your Conferencing, Application, and Mediation servers. For the Conferencing, Application, and Mediation servers you specified a source port range; with Edge servers, you need to specify a destination port range. Because of that you cannot simply apply the Conferencing, Application, and Mediation server QoS policies to your Edge servers: these policies simply won't work. Instead, you must create new policies and apply those policies to your Edge servers only.

The following procedure describes the process for creating Active Directory Group Policy objects that can be used to manage Quality of Service on Edge Servers. Of course, it's possible that your Edge servers are stand-alone servers that do not have Active Directory accounts. If that's the case, you can use local Group Policy instead of Active Directory Group Policy: the only difference is that you must create these local policies using the Local Group Policy Editor, and must individually create the same set of policies on each Edge Server. To start the Local Group Policy Editor on an Edge server do the following:

1. Click **Start** and then click **Run**.
2. In the **Run** dialog box, type **gpedit.msc** and then press ENTER.

If you are creating Active Directory-based policies, then you should log on to a computer where Group Policy Management has been installed. In that case, open Group Policy Management (click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**) and then complete the following steps:

1. In Group Policy Management, locate the container where the new policy should be created. For example, if all your Lync Server computers are located in an OU named Lync Server then the new policy should be created in the Lync Server OU.
2. Right-click the appropriate container and then click **Create a GPO in this domain, and Link it here**.
3. In the **New GPO** dialog box, type a name for the new Group Policy object in the **Name** box (for example, **Lync Server Audio**) and then click **OK**.
4. Right-click the newly-created policy and then click **Edit**.

From here the process is identical regardless of whether you are creating an Active Directory policy or a local policy:

1. In the Group Policy Management Editor or the Local Group Policy Editor, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, right-click **Policy-based QoS**, and then click **Create new policy**.
2. In the **Policy-based QoS** dialog box, on the opening page, type a name for the new policy (e.g., **Lync Server Audio**) in the **Name** box. Select **Specify DSCP Value** and set the value to **46**. Leave **Specify Outbound Throttle Rate** unselected, and then click **Next**.
3. On the next page, make sure that **All applications** is selected and then click **Next**. This setting instructs the network to look for all packets with a DSCP marking of 46, not just packets created by a specific application.
4. On the third page, make sure that both **Any source IP address** and **Any destination IP address** are selected and then click **Next**. These two settings ensure that packets will be managed regardless of which computer (IP address) sent those packets and which computer (IP address) will receive those packets.
5. On page four, select **TCP and UDP** from the **Select the protocol this QoS policy applies to** dropdown list. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the two networking protocols most-commonly used by Lync Server and its client applications.
6. Under the heading **Specify the destination port number**, select **From this destination port or range**. In the accompanying text box, type the port range reserved for audio transmissions. For example, if you reserved ports 49152 through ports 57500 for audio traffic then enter the port range using this format: **49152:57500**. Click **Finish**.

After you have created the QoS policy for audio traffic you should create a second policy for video traffic. To create a policy for video, follow the same basic procedure you followed when creating the audio policy, making these substitutions:

- Use a different (and unique) policy name (for example, **Lync Server Video**).
- Set the DSCP value to **34** instead of 46. (Note that you do not have to use a DSCP value of 34. The only requirement is that you use a different DSCP value for video than you used for audio.)
- Use the previously-configured port range for video traffic. For example, if you have reserved ports 57501 through 65535 for video, then set the port range to this: **57501:65535**. Again, this should be configured as the destination port range.

If you decide to create a policy for managing application sharing traffic you must create a third policy, making the following substitutions:

- Use a different (and unique) policy name (for example, **Lync Server Application Sharing**).
- Set the DSCP value to **24** instead of 46. (Again, you do not have to use a DSCP value of 24. The only requirement is that you use a different DSCP value for application sharing than you used for audio or for video.)
- Use the previously-configured port range for video traffic. For example, if you have reserved ports 40803 through 49151 for application sharing, then set the port range to this: **40803:49151**.

The new policies you have created will not take effect until Group Policy has been refreshed on your Edge servers. Although Group Policy periodically refreshes on its own, you can force an immediate refresh by running the following command on each computer where Group Policy needs to be refreshed:

```
Gpudate.exe /force
```

This command can be run from within the Lync Server or from any command window that is running under administrator credentials. To run a command window under administrator credentials, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**. Note that you might need to restart the Edge server even after running Gpudate.exe.

To help ensure that network packets are marked with the appropriate DSCP value, you should also create a new registry entry on each computer by completing the following procedure:

1. Click **Start** and then click **Run**.
2. In the **Run** dialog box, type **regedit** and then press ENTER.
3. In the Registry Editor, expand **HKEY_LOCAL_MACHINE**, expand **SYSTEM**, expand **CurrentControlSet**, expand **services**, and then expand **Tcpip**.
4. Right-click **Tcpip**, point to **New**, and then click **Key**. After the new registry key is created, type **QoS** and then press ENTER to rename the key.
5. Right-click **QoS**, point to **New**, and then click **String Value**. After the new registry value is created, type **Do not use NLA** and then press ENTER to rename the value.
6. Double-click **Do no use NLA**. In the **Edit String** dialog box, type **1** in the **Value data** box and then click **OK**.
7. Close the Registry Editor and then reboot your computer.

1.7.14.1.7 Configuring Quality of Service Policies for Clients Running on Windows 7 or Windows 8

Configuring Quality of Service Policies for Clients Running on Windows 7 or Windows 8

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Quality of Service (QoS) >

Topic Last Modified: *2012-11-01*

In addition to specifying port ranges for use by your Lync clients you must also create separate Quality of Service policies that will be applied to client computers. (The Quality of Service policies created for Conferencing, Application, and Mediation servers should not be applied to client computers.) Keep in mind that only computers running Windows 7 or Windows 8 can use Quality of Service in Microsoft Lync Server 2013; computers running other Windows operating systems, such as Windows XP or Windows Server 2003, are not supported.

The following example uses this set of port ranges to create an audio policy and a video policy:

Client Traffic Type	Port Start	Port Range
Audio	50020	20
Video	58000	20
Application sharing	42000	20
File transfer	42020	20

To create a Quality of Service audio policy for Windows 7 or Windows 8 computers, first log on to a computer where Group Policy Management has been installed. Open Group Policy Management (click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**) and then complete the following procedure:

1. In Group Policy Management, locate the container where the new policy should be created. For example, if all your client computers are located in an OU named Clients then the new policy should be created in the Client OU.
2. Right-click the appropriate container and then click **Create a GPO in this domain, and Link it here**.
3. In the **New GPO** dialog box, type a name for the new Group Policy object in the **Name** box (for example, **Lync Audio**) and then click **OK**.
4. Right-click the newly-created policy and then click **Edit**.
5. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, right-click **Policy-based QoS**, and then click **Create new policy**.
6. In the **Policy-based QoS** dialog box, on the opening page, type a name for the new policy (e.g., **Lync Audio**) in the **Name** box. Select **Specify DSCP Value** and set the value to **46**. Leave **Specify Outbound Throttle Rate** unselected, and then click **Next**.
7. On the next page, make sure that **All applications** is selected and then click **Next**. This setting instructs the network to look for all packets with a DSCP marking of 46, not just packets created by a specific application.
8. On the third page, make sure that both **Any source IP address** and **Any destination IP address** are selected and then click **Next**. These two settings ensure that packets will be managed regardless of which computer (IP address) sent those packets and which computer (IP address) will receive those packets.
9. On page four, select **TCP and UDP** from the **Select the protocol this QoS policy applies to** dropdown list. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the two networking protocols most-commonly used by Lync Server and its client applications.
10. Under the heading **Specify the source port number**, select **From this source port or range**. In the accompanying text box, type the port range reserved for audio transmissions. For example, if you reserved ports 50020 through ports 50039 for audio traffic enter the port range using this format: **50020:50039**. Click **Finish**.

After you have created the QoS policy for audio you should then create a second policy for video. To create a policy for video, follow the same basic procedure you followed when creating the audio policy, making these substitutions:

- Use a different (and unique) policy name (for example, **Lync Video**).
- Set the DSCP value to **34** instead of 46. (As noted previously, you do not have to use the DSCP value 34; you simply must assign a different DSCP value than the one used for audio.)
- Use the previously-configured port range for video traffic. For example, if you have reserved ports 58000 through 58019 for video, then set the port range to this: **58000:58019**.

If you decide to create a policy for managing application sharing traffic make these substitutions:

- Use a different (and unique) policy name (for example, **Lync Server Application Sharing**).
- Set the DSCP value to **24** instead of 46. (Again, this value does not have to be 24; it simply must be different than the DSCP values used for audio and for video.)
- Use the previously-configured port range for video traffic. For example, if you have reserved ports 42000 through 42019 for application sharing, then set the port range to this: **42000:42019**.

For a file transfer policy:

- Use a different (and unique) policy name (for example, **Lync Server File Transfers**).
- Set the DSCP value to **14**. (Again, this value does not have to be 14; it simply must be a unique DSCP code.)
- Use the previously-configured port range for application. For example, if you have reserved ports 42020 through 42039 for application sharing, then set the port range to this: **42020:42039**.

The new policies you have created will not take effect until Group Policy has been refreshed on your client computers. Although Group Policy periodically refreshes on its own, you can force an immediate refresh by running the following command on each computer where Group Policy needs to be refreshed:

```
Gpudate.exe /force
```

This command can be run from any command window that is running under administrator credentials. To run a command window under administrator credentials, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.

Keep in mind that these policies should be targeted towards your client computers. They should not be applied to servers running Lync Server.

To help ensure that network packets are marked with the appropriate DSCP value, you should also create a new registry entry on each computer by completing the following procedure:

1. Click **Start** and then click **Run**.
2. In the **Run** dialog box, type **regedit** and then press ENTER.
3. In the Registry Editor, expand **HKEY_LOCAL_MACHINE**, expand **SYSTEM**, expand **CurrentControlSet**, expand **services**, and then expand **Tcpip**.
4. Right-click **Tcpip**, point to **New**, and then click **Key**. After the new registry key is created, type **QoS** and then press ENTER to rename the key.
5. Right-click **QoS**, point to **New**, and then click **String Value**. After the new registry value is created, type **Do not use NLA** and then press ENTER to rename the value.
6. Double-click **Do no use NLA**. In the **Edit String** dialog box, type **1** in the **Value data** box and then click **OK**.

7. Close the Registry Editor and then reboot your computer.

Configuring Quality of Service on Computers with Multiple Network Adapters

If you have a computer that has multiple network adapters you might occasionally run into issues where DSCP values are shown as 0x00 rather than the configured value. This will typically occur on computers where one or more of the network adapters are not able to access your Active Directory domain (for example, if these adapters are used for a private network). In cases like that, DSCP values will be tagged for the adapters that can access the domain, but will not be tagged for adapters that cannot access the domain.

If you would like to tag DSCP values for all the network adapters in a computer, including adapters that do not have access to your domain, then you will need to add and configure a value to the registry. That can be done by completing the following procedure:

1. Click **Start** and then click **Run**.
2. In the **Run** dialog box, type **regedit** and then press ENTER.
3. In the Registry Editor, expand **HKEY_LOCAL_MACHINE**, expand **SYSTEM**, expand **CurrentControlSet**, expand **services**, and then expand **Tcpip**.
4. If you do not see a registry key labeled **QoS** then right-click **Tcpip**, point to **New**, and then click **Key**. After the new key is created, type **QoS** and then press ENTER to rename the key.
5. Right-click **QoS**, point to **New**, and then click **String Value**. After the new registry value is created, type **Do not use NLA** and then press ENTER to rename the value.
6. Double-click **Do not use NLA**. In the **Edit String** dialog box, type **1** in the **Value data** box and then click **OK**.

After creating and configuring the new registry value you will need to reboot your computer in order for the changes to take effect.

1.7.14.1.8 Configuring Quality of Service on Microsoft Lync Phone Edition Devices

Configuring Quality of Service on Microsoft Lync Phone Edition Devices

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Quality of Service (QoS) >

Topic Last Modified: *2012-11-01*

Although Quality of Service (QoS) is not enabled by default for devices such as iPhones, QoS is enabled by default for devices running Lync Phone Edition. (These devices are commonly referred to as UC or Unified Communication phones.) To verify this, run the following Windows PowerShell command from within the Lync Server Management Shell:

```
Get-CsUCPhoneConfiguration
```

If you have not made any changes to your UC phone configuration settings then you will get back information that looks like this:

```
Identity            : Global
CalendarPollInterval : 00:03:00
EnforcePhoneLock     : True
PhoneLockTimeout     : 00:10:00
MinPhonePinLength    : 6
```

```
SIPSecurityMode       : High
VoiceDiffServTag      : 40
Voice8021p            : 0
LoggingLevel          : Off
```

For Quality of Service purposes, only one of these properties is of interest: VoiceDiffServTag. The VoiceDiffServTag represents the DSCP value assigned to voice traffic emanating from a Lync Phone Edition device.

Note:

The Voice8021p parameter is no longer supported in Lync Server 2013. The parameter is still valid for backward compatibility with Microsoft Lync Server 2010; however, it has no effect on devices used with Lync Server 2013.

In most networks, marking Lync Phone Edition packets with a VoiceDiffServTag of 40 should not cause any problems. However, 40 is not the value typically used for audio traffic; instead, audio traffic is almost always marked with the DSCP code 46. In order to maintain consistency throughout your network, you might want to change the VoiceDiffServTag property of your UC phones to 46.

To do that, you can use either Windows PowerShell or the Lync Server Control Panel. To modify the VoiceDiffServTag value by using Windows PowerShell, run the following command from within the Lync Server Management Shell:

```
Set-CsUCPhoneConfiguration -VoiceDiffServTag 46
```

The preceding command modifies the global collection of UC phone configuration settings. Note, however, that UC phone settings can also be assigned to the site scope. To modify UC phone configuration settings at the site scope, you must specify the site Identity. For example:

```
Set-CsUCPhoneConfiguration -Identity "site:Redmond" -VoiceDiffServTag 46
```

You can also use the following command to simultaneously modify all your UC phone configuration settings:

```
Get-CsUCPhoneConfiguration | Set-CsUCPhoneConfiguration -VoiceDiffServTag 46
```

If you prefer to make this change using Lync Server Control Panel, then start the Control Panel and then complete the following procedure:

1. Click **Clients** and then click **Device Configuration**.
2. On the **Device Configuration** tab, double-click the collection of settings you want to modify (for example, **Global**).
3. In the **Edit Device Configuration** dialog box, set the value of the **Voice Quality of Service (QoS)** box to **46** and then click **Commit**.

If you have multiple collections you will need to repeat this process for each collection of UC phone settings. Lync Server Control Panel will not allow you to simultaneously modify multiple setting collections.

If you have devices that are not based on the Windows operating system (such as iPhones) in your organization these devices will not be affected by changing the VoiceDiffServTag setting. If you want to change DSCP values on those devices you will need to refer to the administration manual for each of your device types.

1.7.14.1.9 Configure Voice Quality of Service for Lync Phone Edition

Configure Voice Quality of Service for Lync Phone Edition

See Also

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Quality of Service (QoS) >

Topic Last Modified: *2012-09-29*

You can configure voice Quality of Service (QoS) requirements for Lync Phone Edition devices in a pool by setting the QoS level for IP phones that connect to Lync Server 2013.

⊟To configure voice Quality of Service for Lync Phone Edition

1. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
2. In the left navigation bar, click **Clients**, and then click **Device Configuration**.
3. On the **Device Configuration** page, in the list of device configurations, double-click the configuration for which you want to change QoS settings.
4. In **Edit Device Configuration**, under **Voice quality of service**, specify the QoS level. The default level is **40**.

Other Resources

Managing the Lync Server 2013 Network Infrastructure

1.7.14.2 Managing Call Admission Control

Managing Call Admission Control

See Also

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Network Infrastructure >

Topic Last Modified: *2012-11-01*

Call admission control (CAC) determines, based on available network bandwidth, whether to allow real-time communications sessions such as voice or video calls to be established. Use the following procedures to manage different CAC features for your Lync Server 2013 environment.

- Enabling Call Admission Control
- Managing Network Bandwidth Policy Profiles
- Network Regions
- Network Region Routes
- Call Admission Control for Sites
- Enabling and Disabling Media Bypass
- Linking Network Regions
- Managing Network Subnets

⊟See Also

Concepts

Overview of Call Admission Control

1.7.14.2.1 Enabling Call Admission Control

Enabling Call Admission Control

See Also

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control >

Topic Last Modified: *2012-11-01*

Call admission control (CAC) is a network of regions, sites, and subnets that enable you to place restrictions on audio and video transmissions based on available bandwidth. After you configure the CAC network, you must enable CAC to enforce the bandwidth limitations. You can use Lync Server Control Panel to do this.

To enable CAC from Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Global**.
4. On the **Global** page, click the **Global** configuration.

   > **Note:**
   > Only one network can be configured for any Microsoft Lync Server 2013 deployment, so there will never be more than one network configuration in the list. You cannot rename the Global configuration.

5. On the **Edit** menu, click **Show details**.
6. On the **Edit Global Setting** page, select the **Enable call admission control** check box, and then click **Commit**.

When you click **Commit**, you run a test of the configuration. The **Edit Global Settings** dialog box closes, returning you to the **Global** page. You will receive a warning if any errors or inconsistencies are discovered in your network configuration that will prevent it from working correctly (for example, if every region is not connected to every other region through an interregion route).

If you make changes to your network configuration, you can run the validation check again by opening the Global configuration and clicking **Commit**. You do not need to disable CAC first: leave the check box checked and click **Commit**. You can do this at any time without making any configuration changes.

Concepts

Overview of Call Admission Control

Other Resources

Planning for Call Admission Control
Configure Call Admission Control
Get-CsNetworkConfiguration
Set-CsNetworkConfiguration
Remove-CsNetworkConfiguration

1.7.14.2.2 Managing Network Bandwidth Policy Profiles

Managing Network Bandwidth Policy Profiles

See Also

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control >

Topic Last Modified: *2012-10-15*

Use the procedures in this section to manage your network bandwidth policy profiles. For details on network bandwidth requirements for media traffic, see Network Bandwidth

Requirements for Media Traffic.

- Viewing Network Bandwidth Policy Profile Information
- Creating or Modifying Bandwidth Policy Profiles
- Deleting Network Bandwidth Policy Profiles

⊟Related Sections

Network Planning for Lync Server

⊟See Also

Concepts

Network Bandwidth Requirements for Media Traffic

1.7.14.2.2.1 Viewing Network Bandwidth Policy Profile Information

Viewing Network Bandwidth Policy Profile Information

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Managing Network Bandwidth Policy Profiles >

***Topic Last Modified:** 2013-02-23*

As part of call admission control (CAC), a bandwidth policy is used to define bandwidth limitations for certain modalities. In Microsoft Lync Server 2013, only audio and video modalities can be assigned bandwidth limitations. You can set overall bandwidth limitations and session limitations. You can use the Lync Server Control Panel to create, modify, or delete a container profile for these policies. Each bandwidth policy profile can be associated with one or more network sites. Use the following procedures to view a bandwidth policy profile. To create or modify a bandwidth policy profile, see Creating or Modifying Bandwidth Policy Profiles.

⊟To view a bandwidth policy profile

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Bandwidth Policy**.
4. On the **Bandwidth Policy** page, click the bandwidth policy profile that you want to view.
5. On the **Edit** menu, click **Show details**.

Viewing Network Bandwidth Policy Profile Information by Using Windows PowerShell Cmdlets

Network bandwidth profiles can be viewed by using Windows PowerShell and the Get-CsNetworkBandwidthPolicyProfile cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view network bandwidth policy profile information

- To view information about all your network bandwidth policy profiles, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsNetworkBandwidthPolicyProfile
  ```

  That will return information similar to this:

  ```
  Identity           : RedmondBandwidthPolicy
  BWPolicy           : {BWLimit=200;BWSessionLimit=200;
                        BWPolicyModality=Audio,
                        BWLimit=1400;BWSessionLimit=500;
                        BWPolicyModality=Video}
  BWPolicyProfileID : RedmondBandwidthPolicy
  Description        :
  ```

For more information, see the help topic for the Get-CsNetworkBandwidthPolicyProfile cmdlet.

See Also

Tasks

Creating or Modifying Bandwidth Policy Profiles
Deleting Network Bandwidth Policy Profiles

Other Resources

Configure Call Admission Control

1.7.14.2.2.2 Creating or Modifying Bandwidth Policy Profiles

Creating or Modifying Bandwidth Policy Profiles

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Managing Network Bandwidth Policy Profiles >

Topic Last Modified: *2012-10-15*

As part of call admission control (CAC), a bandwidth policy is used to define bandwidth limitations for certain modalities. In Microsoft Lync Server 2013, only audio and video modalities can be assigned bandwidth limitations. You can set overall bandwidth limitations and session limitations. You can use the Lync Server Control Panel to create, modify, or delete a container profile for these policies. Each bandwidth policy profile can be associated with one or more network sites. Use the following procedures to create or modify a bandwidth policy profile. To delete a bandwidth policy profile, see Deleting Network Bandwidth Policy Profiles

To create a new bandwidth policy profile

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Bandwidth Policy**.
4. On the **Bandwidth Policy** page, click **New**.
5. In **New Bandwidth Policy Profile**, type a name in the **Name** field. This name must be unique among all bandwidth policy profiles.

6. In the **Audio limit** field, type a numeric value. This value is the maximum amount of bandwidth to allocate for all audio connections, expressed in kbps.
7. Enter a numeric value in the **Audio session limit** field. This value is the maximum amount of bandwidth to allocate for an individual audio connection, expressed in kbps. This value must be 40 or higher.
8. Enter a numeric value in the **Video limit** field. This value is the maximum amount of bandwidth to allocate for all video connections, expressed in kbps.
9. Enter a numeric value in the **Video session limit** field. This value is the maximum amount of bandwidth to allocate for an individual video connection, expressed in kbps. This value must be 100 or higher.
10. (Optional) Type a value in the **Description** field to provide more information about this bandwidth policy profile that cannot be expressed by the name alone.
11. Click **Commit**.

Note:
Creating a new bandwidth policy profile does not automatically enforce bandwidth restrictions. You must first associate the policy profile with a site. For details about how to associate a policy profile with a site, see Creating or Modifying Network Sites.

To modify a bandwidth policy profile

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Bandwidth Policy**.
4. On the **Bandwidth Policy** page, click the bandwidth policy profile that you want to modify.
5. On the **Edit** menu, click **Show details**.
6. On the **Edit Bandwidth Policy Profile** page, modify the fields as necessary (for details, see the "To create a bandwidth policy profile" section earlier in this topic).
7. Click **Commit**.

Note:
When you modify the bandwidth policy profile, it will immediately update the bandwidth limitations of all network sites associated with this bandwidth policy profile.

Tasks

Deleting Network Bandwidth Policy Profiles

Other Resources

Configure Call Admission Control
New-CsNetworkBandwidthPolicyProfile
Set-CsNetworkBandwidthPolicyProfile
Get-CsNetworkBandwidthPolicyProfile

1.7.14.2.2.3 Deleting Network Bandwidth Policy Profiles

Deleting Network Bandwidth Policy Profiles

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Managing Network Bandwidth Policy Profiles >

Topic Last Modified: *2012-11-01*

As part of call admission control (CAC), a bandwidth policy is used to define bandwidth limitations for certain modalities. In Microsoft Lync Server 2013, only audio and video modalities can be assigned bandwidth limitations. You can set overall bandwidth limitations and session limitations. You can use the Lync Server Control Panel to create, modify, or delete a container profile for these policies. Use the following procedures to delete a network bandwidth policy profiles. For details on creating or modifying a network bandwidth policy profile, see Creating or Modifying Bandwidth Policy Profiles.

⊟To delete a bandwidth policy profile

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Bandwidth Policy**.
4. On the **Bandwidth Policy** page, click the bandwidth policy profile that you want to delete.

   Note:

   You can delete more than one profile at a time. To do this, press CTRL and select multiple profiles while holding down the CTRL key. Or, to select all profiles, click **Select all** on the **Edit** menu.
5. On the **Edit** menu, click **Delete**.

   Warning:

   You cannot delete a bandwidth policy profile that is associated with a network site. You must first remove the association with the network site before you can delete the profile. For details about how to modify the network site, see Creating or Modifying Network Sites.

Tasks

Creating or Modifying Bandwidth Policy Profiles
Viewing Network Bandwidth Policy Profile Information

Other Resources

Configure Call Admission Control
Remove-CsNetworkBandwidthPolicyProfile

1.7.14.2.3 Network Regions

Network Regions

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control >

Topic Last Modified: *2013-02-21*

Network regions are the network hubs or backbones used in the configuration of call admission control, E9-1-1, and media bypass. Use the following procedures to view, create, or modify network regions. For example, if you have already created network regions for one Voice feature, you do not need to create new network regions; other advanced Enterprise Voice features will use those same network regions. You may, however, need to modify an existing network region definition to apply feature-specific settings. For example, if you have created network regions for E9-1-1 (which do not require an associated central site) and you then deploy call admission control, you need to modify the network region definitions to specify a central site. For details, see

Configure Network Regions for CAC.

Note:
Any feature-specific requirements for network region definitions are documented in the Deployment topics for the feature.

- Viewing Network Region Information
- Creating or Modifying Network Regions
- Deleting Existing Network Regions

Reference

Deploying Advanced Enterprise Voice Features

1.7.14.2.3.1 Viewing Network Region Information

Viewing Network Region Information

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Network Regions >

Topic Last Modified: *2013-02-23*

A network region interconnects various parts of a network across multiple geographic areas. Every network region must be associated with a central site. The central site is the data center site on which the call admission control (CAC) bandwidth policy service is running. You can use Lync Server Control Panel to view network regions. Network regions include settings that determine whether alternate paths through the Internet are allowed for audio and video connections. Use this topic to view existing network regions. For details about creating or modifying existing network regions, see Creating or Modifying Network Regions.

To view information about a network region with Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region**.
4. On the **Region** page, click the region you want to view.

   Note:
   You can only view one region at a time.
5. On the **Edit** menu, click **Show details**.

Viewing Network Region Information by Using Windows PowerShell Cmdlets

You can view network region information by using Windows PowerShell and the **Get-CsNetworkRegion** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view network region information

- To view information about all your network regions, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsNetworkRegion
  ```

  That will return information similar to this:

  ```
  Identity          : Pacific Northwest
  Description       :
  BypassID          : 3b232b84-2c1d-4da2-8181-e9330bafebe9
  CentralSite       : Site:Redmond1
  BWAlternatePaths  : {BWPolicyModality=Audio;AlternatePath=True,
                      BWPolicyModality=Video;AlternatePath=True}
  NetworkRegionID   : Pacific Northwest
  ```

For more information, see the help topic for the Get-CsNetworkRegion cmdlet.

See Also

Tasks

Creating or Modifying Network Regions
Deleting Existing Network Regions

1.7.14.2.3.2 Creating or Modifying Network Regions

Creating or Modifying Network Regions

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Network Regions >

Topic Last Modified: *2012-11-01*

A network region interconnects various parts of a network across multiple geographic areas. Every network region must be associated with a central site. The central site is the data center site on which the call admission control (CAC) bandwidth policy service is running. You can use Lync Server Control Panel to configure network regions. Network regions include settings that determine whether alternate paths through the Internet are allowed for audio and video connections. From the Lync Server Control Panel, you can create, modify, or delete a network region. Use this topic to create and modify network regions. For details about deleting existing network regions, see Deleting Existing Network Regions.

To create a network region

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region**.
4. On the **Region** page, click **New**.
5. In the **New Region** page, type a value in the **Name** field. This value must be unique within your Microsoft Lync Server 2013 deployment.
6. From the **Central site** drop-down list, select the central site for this network region.
7. The **Enable audio alternate path** check box is checked by default. This field determines whether audio calls will be routed through an alternate path if

adequate bandwidth does not exist in the primary path. Clear this check box only if you need to turn off the offload to the Internet. If any of your calls will be Internet calls, this check box must be checked, regardless of bandwidth settings.

8. The **Enable video alternate path** check box is checked by default. This field determines whether video calls will be routed through an alternate path if adequate bandwidth does not exist in the primary path. Clear this check box only if you need to turn off the offload to the Internet. If any of your calls will be Internet calls, this check box must be checked, regardless of bandwidth settings.
9. (Optional) Type a value in the **Description** field to provide more information about this region that cannot be expressed by the name alone.
10. Click **Commit**.

The **Associated sites** table is not used for creating a network region. You associate a site with a region when you create or modify the site. For details, see Creating or Modifying Network Sites.

⊟To modify a network region

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region**.
4. On the **Region** page, click the region that you want to modify.
5. On the **Edit** menu, click **Show details**.
6. On the **Edit Region** page, you can modify the settings for enabling and disabling audio and video alternate paths, and change the description (for details, see the "To create a network region" section earlier in this topic.
7. Click **Commit**.

You cannot modify the **Associated sites** on this page. The list of associated sites is provided for reference so you are aware of which sites will be affected when you modify the region settings.

Tasks

Deleting Existing Network Regions
Configure Network Regions for CAC

Other Resources

New-CsNetworkRegion
Set-CsNetworkRegion
Remove-CsNetworkRegion
Get-CsNetworkRegion

1.7.14.2.3.3 Deleting Existing Network Regions

Deleting Existing Network Regions

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Network Regions >

Topic Last Modified: *2013-02-21*

A network region interconnects various parts of a network across multiple geographic areas. Every network region must be associated with a central site. The central site is the data center site on which the call admission control (CAC) bandwidth policy service is running. You can use Lync Server Control Panel to configure network regions. Network regions include settings that determine whether alternate paths through the Internet are allowed for audio and video connections. From the Lync Server Control Panel, you can create, modify, or delete a network region. Use this topic to delete existing network regions. For details about creating or modifying existing network regions, see Creating or Modifying Network Regions.

⊟To delete a network region

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region**.
4. On the **Region** page, click the region you want to delete.

> **Note:**
> You can delete more than one region at a time. To do this, press CTRL and select multiple regions while holding down the CTRL key. Or, to select all regions, click **Select all** on the **Edit** menu.

5. On the **Edit** menu, click **Delete**.
6. Click **OK**.

> ⚠**Warning:**
> A network region cannot be removed if it is associated with a network site. If you attempt to remove a region associated with a site you will receive an error message. To see if a region is associated with any sites, select the region and then click **Show details** on the **Edit** menu.

Tasks

Creating or Modifying Network Regions

1.7.14.2.4 Network Region Routes

Network Region Routes

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control >

Topic Last Modified: *2013-02-21*

A *network region route* defines the route between a pair of network regions. Each pair of network regions in your call admission control deployment requires a network region route. This enables every network region within the deployment to access every other region. Use the procedures in this section to view, create, modify, or delete network region routes.

- Creating or Modifying Network Regions
- Viewing Network Region Route Information
- Deleting Existing Network Region Routes

⊟Reference

Deploying Advanced Enterprise Voice Features

1.7.14.2.4.1 Viewing Network Region Route Information

Viewing Network Region Route Information

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Network Region Routes >

Topic Last Modified: *2013-02-23*

Every region within a call admission control (CAC) configuration must have some way to access every other region. While region links set bandwidth limitations on the connections between regions and also represent the physical links, a route determines which linked path the connection will traverse from one region to another. Use the following procedures to view existing network region routes in Lync Server 2013 Control Panel or Lync Server 2013 Management Shell. For details about creating or modifying network region routes, see Creating or Modifying Network Region Routes.

⊟To view network region route information in Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region Route**.
4. On the **Region Route** page, click the region route that you want to view.

   Note:
   You can only view one region route at a time.
5. On the **Edit** menu, click **Show details**.

Viewing Network Region Route Information by Using Windows PowerShell Cmdlets

Network region route information can be viewed by using Windows PowerShell and the Get-CsNetworkInterRegionRoute cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To view network region route information

- To view information about all your network region routes, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsNetworkInterRegionRoute
  ```

  That will return information similar to this:

  ```
  Identity                   : TransAmericaRoute
  NetworkRegionLinks         : {NorthwestToNortheast}
  InterNetworkRegionRouteID  : TransAmericaRoute
  NetworkRegionID1           : Pacific Northwest
  NetworkRegionID2           : Northeast
  ```

For more information, see the help topic for the Get-CsNetworkInterRegionRoute cmdlet.

⊟See Also

Tasks

Creating or Modifying Network Region Routes
Deleting Existing Network Region Routes

1.7.14.2.4.2 Creating or Modifying Network Region Routes

Creating or Modifying Network Region Routes

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Network Region Routes >

Topic Last Modified: *2012-10-08*

Every region within a call admission control (CAC) configuration must have some way to access every other region. While region links set bandwidth limitations on the connections between regions and also represent the physical links, a route determines which linked path the connection will traverse from one region to another. You can use Lync Server Control Panel to configure network region routes. From Lync Server Control Panel, you can create, modify, or delete a network region route. Use this topic to create or modify a network region route. For details about deleting an existing network region routes, see Deleting Existing Network Region Routes.

⊟To create a network region route

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region Route**.
4. On the **Region Route** page, click **New**.
5. In **New Region Route**, type a value in the **Name** field.

   > **Note:**
   > This value must be unique within your Microsoft Lync Server 2013 deployment.

6. From the **Network region #1** drop-down list, select one of the two regions to be connected by this route.
7. From the **Network region #2** drop-down list, select the other region for this route. This region must be different from the region selected for Network region #1.
8. Use the **Network region links** list box to add region links to the route. Click the **Add** button to display the **Region Link** page. Click a region link to add to this route, and then click **OK**.

   > **Note:**
   > Continue to click the **Add** button to add more links, or select a link and click **Remove** to remove a link.

9. Click **Commit**.

⊟To modify a network region route

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region Route**.
4. On the **Region Route** page, click the region route that you want to modify.
5. On the **Edit** menu, click **Show details**.
6. In **Edit Region Route**, you can modify the regions joined by this route and the region links associated with the route.
7. Click **Commit**.

Tasks

Deleting Existing Network Region Routes

1.7.14.2.4.3 Deleting Existing Network Region Routes

Deleting Existing Network Region Routes

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Network Region Routes >

Topic Last Modified: *2012-11-01*

Every region within a call admission control (CAC) configuration must have some way to access every other region. While region links set bandwidth limitations on the connections between regions and also represent the physical links, a route determines which linked path the connection will traverse from one region to another. You can use Lync Server Control Panel to configure network region routes. From Lync Server Control Panel, you can create, modify, or delete a network region route. Use this topic to delete existing network region routes. For details about creating or modifying network region routes, see Creating or Modifying Network Region Routes.

⊟To delete a network region route

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region Route**.
4. On the **Region Route** page, click the region route that you want to delete.

   Note:
   You can delete more than one region route at a time. To do this, press CTRL and select multiple region routes while holding down the CTRL key. Or, to select all region routes, click **Select all** on the **Edit** menu.

5. On the **Edit** menu, click **Delete**.
6. Click **OK**.

Tasks

Creating or Modifying Network Region Routes

Concepts

Configure a Network Region Route

Other Resources

New-CsNetworkInterRegionRoute
Set-CsNetworkInterRegionRoute
Remove-CsNetworkInterRegionRoute
Get-CsNetworkInterRegionRoute

1.7.14.2.5 Call Admission Control for Sites

Call Admission Control for Sites

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control >

Topic Last Modified: *2013-02-21*

Network sites are the offices or locations within each network region of call admission control (CAC), E9-1-1, and media bypass deployments. Use the procedures in this section to configure call admission control for network sites.

- Viewing Network Site Information
- Creating or Modifying Network Sites
- Deleting an Existing Network Site

Related Sections

Planning for Call Admission Control

1.7.14.2.5.1 Configuring Network Site Links

Configuring Network Site Links

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Call Admission Control for Sites >

Topic Last Modified: *2012-11-01*

Within a call admission control (CAC) configuration, you can create network inter-site policies that define bandwidth limitations between sites that are directly linked. When network sites share a direct link, bandwidth limitations for audio and video connections can be defined between those two sites. You cannot use the Lync Server Control Panel to configure network site policies, this can be done only by using cmdlets from the Lync Server Management Shell. You can create, modify, and remove a network site link (also known as a network inter-site policy) from the Lync Server Management Shell.

To create a network site link

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. From the command prompt, type the following command, substituting values that are valid for your configuration:

   ```
   New-CsNetworkInterSitePolicy -Identity Reno_Portland -NetworkSiteID1 R
   ```

   This example creates a new network site link named Reno_Portland that sets bandwidth limitations between the Reno and Portland network sites. The network sites and the bandwidth policy profile must already exist before running this command.

For detailed parameter descriptions, see New-CsNetworkInterSitePolicy in the Lync Server Management Shell documentation. To retrieve a list of bandwidth policy profiles that can be applied to the network site link, call the **Get-CsNetworkBandwidthPolicyProfile** cmdlet. For details, see Get-CsNetworkBandwidthPolicyProfile in the Lync Server Management Shell documentation.

To modify a network site link

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Use the **Set-CsNetworkInterSitePolicy** cmdlet to modify the properties of a given network site link. You can modify either (or both) or the connected sites, and you can modify the bandwidth policy profile associated with the link. Here is an example of modifying the bandwidth policy profile of a site link named Reno_Portland:

```
Set-CsNetworkInterSitePolicy -Identity Reno_Portland -BWPolicyProfileI
```

For detailed parameter descriptions, see Set-CsNetworkInterSitePolicy in the Lync Server Management Shell documentation.

To delete a network site link

1. Log on to the computer where Lync Server Management Shell is installed as a member of the RTCUniversalServerAdmins group or with the necessary user rights as described in Delegate Setup Permissions.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Use the **Remove-CsNetworkInterSitePolicy** cmdlet to remove a network site link. The following example deletes the Reno_Portland network site link:

```
Remove-CsNetworkInterSitePolicy -Identity Reno_Portland
```

For detailed parameter descriptions, see Remove-CsNetworkInterSitePolicy in the Lync Server Management Shell documentation.

Concepts

Call Admission Control Cmdlets

Other Resources

New-CsNetworkInterSitePolicy
Set-CsNetworkInterSitePolicy
Remove-CsNetworkInterSitePolicy
Get-CsNetworkInterSitePolicy
Get-CsNetworkBandwidthPolicyProfile

1.7.14.2.5.2 Viewing Network Site Information

Viewing Network Site Information

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Call Admission Control for Sites >

Topic Last Modified: *2013-02-23*

Network sites are the offices or locations configured within each region of a call admission control (CAC) or Enhanced 9-1-1 deployment. You can view network site information in either Lync Server 2013 Control Panel or Lync Server Management Shell . For details about creating or modifying network sites, see Creating or Modifying Network Sites.

To view network site information in Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Site**.
4. On the **Site** page, click the site that you want to view.

   Note:

   You can only view information for one site at a time.
5. On the **Edit** menu, click **Show details**.

Viewing Network Site Information by Using Windows PowerShell Cmdlets

You can view network site information by using Windows PowerShell and the Get-CsNetworkSite cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view network site information

- To view information about all your network sites, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsNetworkSite
  ```

  That will return information similar to this:

  ```
  Identity           : Redmond
  NetworkSiteID      : Redmond
  Description        :
  NetworkRegionID    : Pacific Northwest
  BypassID           : 3b232b84-2c1d-4da2-8181-e9330bafebe9
  BWPolicyProfileID :
  LocationPolicy     :
  ```

For more information, see the help topic for the Get-CsNetworkSite cmdlet.

See Also

Tasks

Creating or Modifying Network Sites
Deleting an Existing Network Site

Creating or Modifying Network Sites

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Call Admission Control for Sites >

Topic Last Modified: *2012-10-08*

Network sites are the offices or locations configured within each region of a call admission control (CAC) or Enhanced 9-1-1 deployment. You can use the Microsoft Lync Server 2013 Control Panel to configure sites and associate them with regions. For example, a network region for North America might be associated with networks sites such as Chicago, Redmond, and Vancouver. A CAC network site must be created for every site within an organization, even if that site has no bandwidth limitations. From the Lync Server Control Panel you can create, modify, and delete network sites. Use the following procedures to create or modify a network site. For details on deleting an existing network site, see Deleting an Existing Network Site.

⊟To create a network site

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Site**.
4. On the **Site** page, click **New**.
5. In **New Site**, type a name for this site in the **Name** field.

Note:
Site names must be unique within the Lync Server 2013 deployment.

6. In the **Region** drop-down list, select a network region to associate with this site.
7. (Optional) If you want to place bandwidth limitations on audio or video calls to this site, select the bandwidth policy profile with the appropriate settings from the **Bandwidth policy** drop-down list.

Note:
You can view the details of the available bandwidth policy profiles, or create a new bandwidth policy profile, on the **Policy Profile** page of the **Network Configuration** group. For details, see Creating or Modifying Bandwidth Policy Profiles.

8. (Optional) If you want to provide location settings for this site, select a location policy from the **Location policy** drop-down list.

Note:
The location policy assigns specific Enhanced 9-1-1 (E9-1-1) and client location settings to the site. You can view the details of the available location policies, or create a new location policy, from the **Location Policy** page of the **Network Configuration** group. For details, see Viewing Location Policy Information.

9. (Optional) Type a value in the **Description** field to provide more information about this site that cannot be expressed by the name alone.
10. Click **Commit**.

Note:
You do not use the **Associated Subnets** table when you create a new

network site. You associate a subnet with a site when you create or modify the subnet. For details, see Create or Modify Network Subnets.

⊟To modify a network site

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Site**.
4. On the **Site** page, click the site that you want to modify.
5. On the **Edit** menu, click **Show details**.
6. On the **Edit Site** page, you can modify the description, region, bandwidth policy profile, and location policy associated with the site. For details, see "To create a network site" section earlier in this topic.
7. Click **Commit**.

You cannot modify the **Associated Subnets** table on this page. The list of associated subnets is provided for reference so that you are aware of what subnets will be affected when you modify the site settings.

⊟To delete a network site

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Site**.
4. On the **Site** page, click the site that you want to delete.

Note:

You can delete more than one site at a time. To do this, press CTRL and select multiple sites while holding down the CTRL key. Or, to select all sites, click **Select all** on the **Edit** menu.

5. On the **Edit** menu, click **Delete**.
6. Click **OK**.

⚠**Warning:**

You cannot remove a network site if it is associated with a network subnet. If you attempt to remove a site associated with a subnet you will receive an error message. To see if a site is associated with any subnets, click the site and then click **Show details** on the **Edit** menu.

Tasks

Deleting an Existing Network Site

Other Resources

New-CsNetworkSite
Set-CsNetworkSite
Remove-CsNetworkSite
Get-CsNetworkSite

1.7.14.2.5.4 Deleting an Existing Network Site

Deleting an Existing Network Site

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Call Admission Control for Sites >

Topic Last Modified: *2012-11-01*

Network sites are the offices or locations configured within each region of a call admission control (CAC) or Enhanced 9-1-1 deployment. You can use the Lync Server 2013 Control Panel to configure sites and associate them with regions. For example, a network region for North America might be associated with networks sites such as Chicago, Redmond, and Vancouver. A CAC network site must be created for every site within an organization, even if that site has no bandwidth limitations. From the Lync Server Control Panel you can create, modify, and delete network sites. Use the following procedure to delete an existing network site. For details about creating or modifying network sites, see Creating or Modifying Network Sites

⊟To delete a network site

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Site**.
4. On the **Site** page, click the site that you want to delete.

> **Note:**
> You can delete more than one site at a time. To do this, press CTRL and select multiple sites while holding down the CTRL key. Or, to select all sites, click **Select all** on the **Edit** menu.

5. On the **Edit** menu, click **Delete**.
6. Click **OK**.

> **Warning:**
> You cannot remove a network site if it is associated with a network subnet. If you attempt to remove a site associated with a subnet you will receive an error message. To see if a site is associated with any subnets, click the site and then click **Show details** on the **Edit** menu.

1.7.14.2.6 Enabling and Disabling Media Bypass

Enabling and Disabling Media Bypass

See Also

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control >

Topic Last Modified: *2012-11-01*

Use the procedures in this section to enable or disable media bypass by using the Lync Server Control Panel. For details about when to use media bypass, see Planning for Media Bypass.

- Enabling Network Media Bypass
- Disabling Network Media Bypass

⊟See Also

Concepts

Overview of Media Bypass

Other Resources

Planning for Media Bypass

1.7.14.2.6.1 Enabling Network Media Bypass

Enabling Network Media Bypass

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Enabling and Disabling Media Bypass >

Topic Last Modified: *2012-11-01*

Media bypass settings apply globally across a Microsoft Lync Server 2013 deployment. Media bypass allows calls to bypass the Mediation Server. For details about when to use Media bypass, see Planning for Media Bypass in the Planning section.

You can enable and configure media bypass from the Lync Server Control Panel.

⊟To enable and configure media bypass

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Global**.
4. On the **Global** page, click the **Global** configuration. There is always only one configuration, and it is always named Global.
5. On the **Edit** menu, click **View details**.
6. On the **Edit Global Setting** page, click the **Enable media bypass** check box.
7. Select one of the following options:
   - **Always bypass**   Select this option to attempt media bypass on all calls. This option will be unavailable if call admission control (CAC) is enabled. If CAC is not enabled, select this option in the following situations:
     - There is no need for bandwidth control.
     - There is no need for fine-grained configuration to determine when bypass should happen.
     - There is full connectivity between gateways and clients.
   - **Use sites and region configuration**   If CAC is enabled, this option is selected by default and cannot be changed. When this option is selected, network configuration sites and regions will be used to determine when media bypass is possible. If you select this option, you can choose to enable bypass for sites that are not mapped. Click the **Enable bypass for non-mapped sites** check box only if you have one or more large sites associated with the same region that do not have bandwidth constraints (for example, a large central site) and you also have some branch sites associated with the same region that do have bandwidth constraints. When you enable bypass for non-mapped sites, configuration is streamlined because you specify only the subnets associated with the branch sites rather than needing to specify all subnets associated with all sites. We recommend that you do not select the **Enable bypass for non-mapped sites** check box if CAC is enabled.
8. Click **Commit** to save your changes.

Tasks

Disabling Network Media Bypass

Concepts

Global Media Bypass Options

Other Resources

Planning for Media Bypass

1.7.14.2.6.2 Disabling Netw ork Media Bypass

Disabling Network Media Bypass

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Enabling and Disabling Media Bypass >

Topic Last Modified: *2012-10-15*

Media bypass settings apply globally across a Microsoft Lync Server 2013 deployment. Media bypass allows calls to bypass the Mediation Server. For details about when to use Media bypass, see Planning for Media Bypass in the Planning section.You can disable media bypass from the Lync Server Control Panel. For details on enabling and configuring medial bypass, see Enabling Network Media Bypass

⊟To disable media bypass

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Global**.
4. On the **Global** page, click the **Global** configuration. There is always only one configuration, and it is always named Global.
5. On the **Edit** menu, click **View details**.
6. On the **Edit Global Setting** page, clear the **Enable media bypass** check box.
7. Click **Commit** to save your changes.

Tasks

Enabling Network Media Bypass

1.7.14.2.7 Linking Netw ork Regions

Linking Network Regions

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control >

Topic Last Modified: *2013-02-21*

You can configure links between two network regions as part of call admission control (CAC).

- Viewing Network Region Link Information
- Configuring Network Region Links
- Deleting Network Region Links

⊟Related Sections

Configure Call Admission Control

1.7.14.2.7.1 Viewing Network Region Link Information

Viewing Network Region Link Information

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Linking Network Regions >

Topic Last Modified: *2013-02-23*

You can view links between two network regions as part of call admission control (CAC). Regions within a network are linked through physical wide area network (WAN) connectivity. You can use the Lync Server Control Panel to view an existing link between two network regions. For details about creating or modifying network region link, see Configuring Network Region Links.

To view a network region link in Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region Link**.
4. On the **Region Link** page, click the region link that you want to view.

   > **Note:**
   > You can only view information about one region link at a time.

5. From the **Edit** menu, select **Show details**.

Viewing Network Region Link Information by Using Windows PowerShell Cmdlets

You can view network region links by using Windows PowerShell and the **Get-CsNetworkRegionLink** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view network region link information

- To view information about all your network region links, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsNetworkRegionLink
  ```

  This command returns information similar to the following:

  ```
  Identity            : NorthwestToCalifornia
  BWPolicyProfileID   :
  NetworkRegionLinkID : NorthwestToCalifornia
  NetworkRegionID1    : Pacific Northwest
  NetworkRegionID2    : California
  ```

For details, see Get-CsNetworkRegionLink.

See Also

Tasks

Configuring Network Site Links

1.7.14.2.7.2 Configuring Network Region Links

Configuring Network Region Links

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Linking Network Regions >

Topic Last Modified: *2012-11-01*

You can configure links between two network regions as part of call admission control (CAC). Regions within a network are linked through physical wide area network (WAN) connectivity. You can use the Lync Server Control Panel to define a link between two network regions and set the bandwidth limitations on audio and video connections between these regions. For details about deleting an existing network region link, see Deleting Network Region Links.

⊟To create a network region link

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region Link**.
4. On the **Region Link** page, click **New**.
5. In **New Region Link**, type a value in the **Name** field.

Note:
This value must be unique within your Lync Server 2013 deployment.

6. From the **Network region #1** drop-down list, select one of the two regions to be linked.
7. From the **Network region #2** drop-down list, select the other region to be linked. This region must be different from the region selected for Network region #1.
8. (Optional) If you want to place bandwidth limitations on audio or video calls between these regions, select a bandwidth policy profile from the **Bandwidth policy** drop-down list.
9. Click **Commit**.

⊟To modify a network region link

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region Link**.
4. On the **Region Link** page, click the region link that you want to modify.
5. On the **Edit** menu, click **Show details**.
6. In **Edit Region Link**, you can modify the regions that are linked or the bandwidth policy profile for this link.

7. Click **Commit**.

Tasks

Deleting Network Region Links

Other Resources

New-CsNetworkRegionLink
Set-CsNetworkRegionLink
Remove-CsNetworkRegionLink
Get-CsNetworkRegionLink

1.7.14.2.7.3 Deleting Network Region Links

Deleting Network Region Links

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Linking Network Regions >

Topic Last Modified: *2012-11-01*

You can configure links between two network regions as part of call admission control (CAC). Regions within a network are linked through physical wide area network (WAN) connectivity. You can use the Lync Server Control Panel to delete an existing link between two network regions. For details about creating or modifying network region link, see Configuring Network Region Links

⊟To delete a network region link

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Region Link**.
4. On the **Region Link** page, click the region link that you want to delete.

> **Note:**
> You can delete more than one region link at a time. To do this, press CTRL and select multiple region links while holding down the CTRL key. Or, to select all region links, click **Select all** on the **Edit** menu.

5. From the **Edit** menu, select **Delete**.
6. Click **OK**.

Tasks

Configuring Network Region Links

1.7.14.2.8 Managing Network Subnets

Managing Network Subnets

See Also

Operations > Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control >

Topic Last Modified: *2012-10-15*

You can use either Lync Server 2013 Control Panel or Lync Server 2013 Management Shell to manage network subnets. In most deployments of Lync Server 2013 where call admission control (CAC) is implemented, there will typically be a large number of subnets.

Because of this, it is often best to configure subnets from the Lync Server Management Shell.

- Viewing Network Subnet Information
- Create or Modify Network Subnets
- Deleting Network Subnets

⊟See Also

Tasks

Associate a Subnet with a Network Site

1.7.14.2.8.1 Viewing Network Subnet Information

Viewing Network Subnet Information

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Managing Network Subnets >

Topic Last Modified: *2013-02-23*

You can use the following procedure to view a network subnet. From the Lync Server Control Panel, you can create, modify, or delete a network subnet. For details about creating or modifying network subnets, see Create or Modify Network Subnets.

⊟To view a network subnet

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Subnet**.
4. On the **Subnet** page, click the subnet that you want to view.

> **Note:**
>
> You can only view one subnet at a time.

5. On the **Edit** menu, click **Show details...**.

Viewing Network Subnet Configuration Information by Using Windows PowerShell Cmdlets

Network subnet information can be viewed by using Windows PowerShell and the Get-CsNetworkSubnet cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To view network subnet information

- To view information about all your network subnets, type the following command in the Lync Server Management Shell and then press ENTER:

```
Get-CsNetworkSubnet
```

That will return information similar to this:

```
Identity      : 172.11.15.0
MaskBits      : 28
Description   :
NetworkSiteID : Redmond
SubnetID      : 172.11.15.0
```

For more information, see the help topic for the Get-CsNetworkSubnet cmdlet.

⊟See Also

Tasks

Create or Modify Network Subnets
Deleting Network Subnets

1.7.14.2.8.2 Create or Modify Netw ork Subnets

Create or Modify Network Subnets

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Managing Network Subnets >

Topic Last Modified: *2013-02-21*

A network subnet must be associated with a network site for the purposes of determining the geographic location of the host belonging to this subnet. You can use Lync Server Control Panel to configure subnets. From the Lync Server Control Panel, you can create, modify, or delete a network subnet. For details about deleting network subnets, see Deleting Network Subnets.

In most deployments of Microsoft Lync Server 2013 where call admission control (CAC) is implemented, there will typically be a large number of subnets. Because of this, it is often best to configure subnets from the Lync Server Management Shell. From there you can call **New-CsNetworkSubnet** in conjunction with the Windows PowerShell cmdlet **Import-CSV**. By using these cmdlets together, you can read in subnet settings from a comma-separated values (.csv) file and create multiple subnets at the same time. For examples of how to create subnets from a .csv file, see New-CsNetworkSubnet.

⊟To create a network subnet

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Subnet**.
4. On the **Subnet** page, click **New**.
5. In **New Subnet**, enter a value in the **Subnet ID** field. This must be an IP address (for example, 174.11.12.0), and it must be the first address in the IP address range defined by the subnet.
6. In the **Mask** field, enter a numeric value from 1 through 32.

Note:
This value is the bitmask that is to be applied to the subnet being created.

7. In **Network site ID**, select the site to which this subnet belongs.
8. (Optional) Type a value in the **Description** field to provide more information about this subnet that cannot be expressed by the name alone.

9. Click **Commit**.

⊟To modify a network subnet

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Subnet**.
4. On the **Subnet** page, click the subnet that you want to modify.
5. On the **Edit** menu, click **Show details**.
6. On the **Edit Subnet** page, you can modify the bitmask, associated network site, or description. If you modify the bitmask, keep in mind that the Subnet ID must still be the first address in the IP address range defined by the subnet.
7. Click **Commit**.

Tasks

Deleting Network Subnets

Concepts

About Network Regions, Sites, and Subnets

Other Resources

New-CsNetworkSubnet
Set-CsNetworkSubnet
Remove-CsNetworkSubnet
Get-CsNetworkSubnet

1.7.14.2.8.3 Deleting Network Subnets

Deleting Network Subnets

See Also

Managing the Lync Server 2013 Network Infrastructure > Managing Call Admission Control > Managing Network Subnets >

Topic Last Modified: *2013-02-21*

You can use the following procedure to delete a subnet. From the Lync Server Control Panel, you can create, modify, or delete a network subnet. For details on creating or modifying network subnets, see Create or Modify Network Subnets.

In most deployments of Microsoft Lync Server 2013 where call admission control (CAC) is implemented, there will typically be a large number of subnets. Because of this, it is often best to configure subnets from the Lync Server Management Shell. From there you can call **New-CsNetworkSubnet** in conjunction with the Windows PowerShell cmdlet **Import-CSV**. By using these cmdlets together, you can read in subnet settings from a comma-separated values (.csv) file and create multiple subnets at the same time. For examples of how to create subnets from a .csv file, see New-CsNetworkSubnet.

⊟To delete a network subnet

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Subnet**.
4. On the **Subnet** page, click the subnet that you want to delete.

> **Note:**
> You can delete more than one subnet at a time. To do this, press CTRL and select multiple subnets while holding down the CTRL key. Or, to select all subnets, click **Select all** on the **Edit** menu.

5. On the **Edit** menu, click **Delete**.
6. Click **OK**.

Tasks

Create or Modify Network Subnets

1.7.14.3 Lync Server 2013 Network Interfaces

Lync Server 2013 Network Interfaces

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Network Infrastructure >

Topic Last Modified: *2012-10-15*

Use the procedures in this section to manage network interfaces for your Lync Server 2013 environment.

- Viewing Network Interface Information

1.7.14.3.1 Viewing Network Interface Information

Viewing Network Interface Information

Operations > Managing the Lync Server 2013 Network Infrastructure > Lync Server 2013 Network Interfaces >

Topic Last Modified: *2013-02-23*

You can view network interface information by using Windows PowerShell and the **Get-CsNetworkInterface** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To view network interface information

- To view network interface information, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsNetworkInterface
  ```

  This command returns information similar to the following for each network interface:

  ```
  Identity              : dc.vdomain.com/Primary/1
  ComputerFqdn          : dc.vdomain.com
  IPAddress             : 0.0.0.0
  IPv6Address           :
  Interface             : Primary
  InterfaceNumber       : 1
  ConfiguredFqdn        :
  ConfiguredIPAddress   :
  ConfiguredIPv6Address :
  ```

  For details, see Get-CsNetworkInterface.

1.7.14.4 Prevent New Connections to Lync Server for Server Maintenance

Prevent New Connections to Lync Server for Server Maintenance

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Network Infrastructure >

Topic Last Modified: *2012-11-01*

Lync Server enables you to take a server offline (for example, to apply software or hardware upgrades) without any loss of service to users.

When you specify the option to prevent new connections or calls to a server in a pool, it stops taking any new connections and calls as soon as you implement this option. These new connections and calls are routed through other servers in the pool. A server that is preventing new connections allows its sessions on existing connections to continue until they naturally end. When all existing sessions have ended, the server is ready to be taken offline.

When you prevent new connections to a Front End Server, some Lync Server features and services rely on DNS load balancing to ensure that it functions properly. If you are not using DNS load balancing on the pool, connections through these services may not be re-routed to other servers during the period that the server is preventing new connections, and thus when the server is taken offline some sessions and calls may be interrupted. The features that rely on DNS load balancing to ensure that this option operates properly are as follows:

- Attendant
- Conferencing Announcement application
- Response Group application
- Announcement application
- Call Park application

For details about DNS load balancing, see DNS Load Balancing in the Planning documentation.

In addition to preventing new connections for all services on a server running Lync Server, you can also prevent new connections for individual Lync Server services. For example, this method is useful in a situation where you need to apply a Lync Server update that does not require the whole server to be shut down. Note that when you prevent connections for one service, you must select a service as it is grouped and displayed in the Windows list of services. For example, the Lync Server Front-End service and the data collection agent for Monitoring are separate Lync Server services, but in the Windows services list they are consolidated and shown as the Lync Server Front End service. You can prevent new connections for the Lync Server Front End service, but you cannot prevent new connections for these two individual underlying Lync Server services separately.

Important:

When you set a server to prevent new connections, and then restart the server, by default the server will immediately begin accepting new connections after it starts. To prevent this, set the server to only pause and resume manually, before you restart the server.

⊟To prevent new connections to Lync Server:

1. Log on to the local computer as a member of the Administrators group.
2. Open the Services snap-in console: Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Services**.

3. In the list, double-click the Lync Server Windows service to which you want to prevent new connections.
4. In the Properties dialog box, under **Service status: Started**, click **Pause**.
5. Optionally, but recommended, next to **Startup type**, click **Manual**.

Important:
When you set a server to prevent new connections, and then restart the server, by default the server will immediately begin accepting new connections after it starts. To prevent this, set the server to only pause and resume manually, before you restart the server.

6. When you are finished, click **OK**.

1.7.15 Managing Enhanced 9-1-1 and the Location Service

Managing Enhanced 9-1-1 and the Location Service

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-11-01*

Lync Server 2013 supports Enhanced 9-1-1 (E9-1-1) calling from Lync clients and Lync Phone Edition devices. When you configure Lync Server 2013 for E9-1-1, emergency calls placed from Lync 2013 or Lync Phone Edition include Emergency Response Location (ERL) information from the Location Information service database. Use the procedures in this section to manage location policy.

Note:
For details on deploying advanced Enterprise Voice features, such as E9-1-1 and the Location Information service, see Deploying Advanced Enterprise Voice Features.

- Managing Location Policy

1.7.15.1 Managing Location Policy

Managing Location Policy

See Also

Microsoft Lync Server 2013 > Operations > Managing Enhanced 9-1-1 and the Location Service >

Topic Last Modified: *2012-10-15*

Use the procedures in this section to manage the Lync Server 2013 location policy from the **Network Configuration** group in Lync Server Control Panel.

- Viewing Location Policy Information
- Creating or Modifying a Location Policy
- Deleting a Location Policy

⊟Related Sections

Planning for Emergency Services (E9-1-1)

⊟See Also

Concepts

Defining the Location Policy

Viewing Location Policy Information

See Also

Operations > Managing Enhanced 9-1-1 and the Location Service > Managing Location Policy >

Topic Last Modified: *2012-11-01*

In Lync Server 2013, you can use the location policy to apply settings that relate to Enhanced 9-1-1 (E9-1-1) functionality and to location settings for users or contacts. The location policy determines whether a user is enabled for E9-1-1, and if so what the behavior is of an emergency call. For example, you can use the location policy to define what number constitutes an emergency call (for example, 911 in the United States), whether corporate security should be automatically notified, and how the call should be routed.

You can configure location policies from the **Network Configuration** group in Lync Server 2013 Control Panel. From Lync Server Control Panel you can view, create, modify, or delete location policies. Use the following procedure to view information about location policies. For details on creating or modifying location policies, see Creating or Modifying a Location Policy.

⊟To view information about a location policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Location Policy**.
4. On the **Location Policy** page, select the location policy that you want to modify.
5. On the **Edit** menu, click **Show details**.

Note:
You can only view information about one location policy at a time.

A single policy, called Global, exists by default and cannot be deleted or renamed. However, you can modify the Global policy. This policy will apply to all users and contacts, unless you create site policies or per-user policies. Per-user policies must be applied to specific users.

Tasks

Creating or Modifying a Location Policy
Create Location Policies
Create or Modify a Network Site

Other Resources

New-CsLocationPolicy
Set-CsLocationPolicy
Remove-CsLocationPolicy
Get-CsLocationPolicy

Creating or Modifying a Location Policy

See Also

Operations > Managing Enhanced 9-1-1 and the Location Service > Managing Location Policy >

***Topic Last Modified:** 2012-11-01*

In Lync Server 2013, you can use the location policy to apply settings that relate to Enhanced 9-1-1 (E9-1-1) functionality and to location settings for users or contacts. The location policy determines whether a user is enabled for E9-1-1, and if so what the behavior is of an emergency call. For example, you can use the location policy to define what number constitutes an emergency call (for example, 911 in the United States), whether corporate security should be automatically notified, and how the call should be routed.

You can configure location policies from the **Network Configuration** group in Lync Server 2013 Control Panel. From Lync Server Control Panel you can view, create, modify, or delete location policies. Use the procedures in this section to create or modify a location policy. For details on deleting location policies, see Deleting a Location Policy.

In Lync Server 2013, you can override the default amount of time between client requests for a location update from the Location Information service. The default value is 4 hours. Use the **Set-CsLocationPolicy** cmdlet with the LocationRefreshInterval parameter to override the default value.

⊟To create a new location policy in Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Location Policy**.
4. On the **Location Policy** page, click **New** and then select the type of policy you want to create:
   - To create a site policy, click **Site policy**. In **Select a Site**, choose the site to which you want the policy applied and click **OK**. On the **New Location Policy** page, the **Scope** field contains the value **Site**, and the **Name** field contains the name of the site you chose. You cannot modify either of these fields. A site policy is automatically applied to all users on the specified site and overrides the global policy for those users.
   - To create a **User policy**, click **User policy**. In the **New Location Policy**, the **Scope** field contains the value **User**. You cannot modify this value. In the **Name** field, type the name you want to give this policy. A user policy does not automatically apply to any users. After creating the user policy, you must manually grant the policy to the users or network sites to which you want to policy to apply.
5. Fill in the remaining fields as follows:
   - **Enable enhanced emergency services**   Select this check box to enable the users associated with this policy for E9-1-1. When emergency services are enabled, Lync Server clients will retrieve location information on registration and include that information when an emergency call is made.
   - **Location**   Specify one of the following values:
     - **Required**   The user will be prompted to input location information when the client registers at a new location. The user can dismiss the prompt

  without entering any information. If information is entered, an emergency call will first be answered by the emergency services provider to verify the location before being routed to the Public Safety Answering Point (PSAP) operator (that is, the 911 operator).
  - **Not Required** The user will not be prompted for a location. When a call is made with no location information, the emergency services provider will answer the call and ask for a location.
  - **Disclaimer** This option is the same as **Required** except that the user cannot dismiss the prompt without entering location information. The user can still complete an emergency call, but no other calls can be completed without entering the information. In addition, disclaimer text will be displayed to the user that can alert them to the consequences of declining to enter location information. To set the disclaimer text, you must use Lync Server Management Shell to run the **Set-CsLocationPolicy** cmdlet or the **New-CsLocationPolicy** cmdlet with the EnhancedEmergencyServiceDisclaimer parameter. For details, see Set-CsLocationPolicy or New-CsLocationPolicy in the Lync Server Management Shell documentation.

> **Note:**
> In Lync Server 2013, you can use location policy to set different disclaimers for different locales or different sets of users, unlike in Lync Server 2010 where you could specify only a global disclaimer for the entire organization.

- **Use location for emergency services only** Lync can use location information for various reasons (for example, to notify teammates of your current location). Select this check box to ensure location information is available only for use with an emergency call.
- **PSTN usage** The public switched telephone network (PSTN) usage that will be used to determine which voice route will be used to route emergency calls from clients using this profile. The route associated with this usage should point to a SIP trunk dedicated to emergency calls or to an Emergency Location Identification Number (ELIN) gateway that routes emergency calls to the nearest Public Safety Answering Point (PSAP).
- **Emergency dial number** The number that is dialed to reach emergency services. In the United States this value is 911. The string must be made of the digits 0 through 9 and can be from 1 to 10 digits in length.
- **Emergency dial mask** A number that you want to translate into the value of the emergency dial number value when it is dialed. For example, if you enter a value of 212 in this field and the emergency dial number field has a value of 911, if a user dials 212 the call will be made to 911. This allows for alternate emergency numbers to be dialed and still have the call reach emergency services (for example, if someone from a country or region with a different emergency number attempts to dial that country or region’s number rather than the number for the country or region they are currently in). You can define multiple emergency dial masks by separating the values with semicolons. For example, 212;414. Maximum length of the string is 100 characters. Each character must be a digit 0 through 9.

> **Important:**
> Ensure that the specified dial mask value is not the same as a number in a call park orbit range. Call park routing will take precedence over emergency dial string conversion. To see the existing call park orbit ranges, click **Voice Features** in the left navigation bar and then click **Call Park**. For details, see Configure Phone Number Extensions for Parking Calls.

- **Notification URI** One or more SIP Uniform Resource Identifiers (URIs) to be notified when an emergency call is made. For example, the company security office could be notified through an instant message whenever an emergency call is made. If the caller's location is available that location will be included in the notification. Multiple SIP URIs can be included as a comma-separated list. For example, "sip:security@litwareinc.com","sip:kmyer@litwareinc.com". Distribution lists are supported. The string must be from 1 to 256 characters in length and must begin with the prefix "sip:". Before you click in the Notification URI field an example is displayed.

- **Conference URI** The SIP URI, in this case the telephone number, of a third party that will be conferenced in to any emergency calls that are made. For example, the company security office could receive a call when an emergency call is made and listen in or participate in that call (depending on the value supplied in the **Conference mode** field). The string must be from 1 to 256 characters in length and must begin with the prefix sip:. An example is displayed until you click inside this field.
- **Conference mode** If you specify a value in the **Conference URI** field, the **Conference mode** determines whether a third party can participate in the call or can only listen in. Specify one of the following options:
  - **One-way** A third party can only listen to the conversation between the caller and the PSAP operator.
  - **Two-way** A third party can listen in and participate in the call between the caller and the PSAP operator.

6. Click **Commit**.

> **Important:**
>
> When you create a user policy, initially that policy does not apply to any users or network sites. To apply the policy to a user, click **Users** in the left navigation bar. Find the user to which you want to apply the policy. On the **Edit** menu, click **Show details**. On the **Edit Lync Server User** page, select the new location policy from the **Location policy** drop-down list and then click **Commit**.
>
> To apply the policy to a network site, click **Network Configuration** in the left navigation bar and then click **Site**. Find the network site to which you want to apply the policy. On the **Edit** menu, click **Show details**. In **Edit Site**, select the new location policy from the **Location policy** drop-down list and then click **Commit**.

⊟To modify a location policy in Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Location Policy**.
4. On the **Location Policy** page, select the location policy that you want to modify.
5. On the **Edit** menu, click **Show details**.
6. On the **Edit Location Policy** page, modify the fields as necessary (for details, see Step 5 in the "To create a new location policy" procedures earlier in this topic).
7. Click **Commit**.

Tasks

Deleting a Location Policy

Concepts

Defining the Location Policy

Other Resources

Configure Phone Number Extensions for Parking Calls

1.7.15.1.3 Deleting a Location Policy

Deleting a Location Policy

See Also

Operations > Managing Enhanced 9-1-1 and the Location Service > Managing Location Policy >

Topic Last Modified: *2012-10-10*

In Lync Server 2013, you can use the location policy to apply settings that relate to Enhanced 9-1-1 (E9-1-1) functionality and to location settings for users or contacts. The location policy determines whether a user is enabled for E9-1-1, and if so what the behavior is of an emergency call. For example, you can use the location policy to define what number constitutes an emergency call (for example, 911 in the United States), whether corporate security should be automatically notified, and how the call should be routed.

You can configure location policies from the **Network Configuration** group in Lync Server 2013 Control Panel. From Lync Server Control Panel you can view, create, modify, or delete location policies. Use the following procedures delete a location policy. For details on creating or modifying location policies, see Creating or Modifying a Location Policy.

⊟To delete a location policy

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or is assigned to the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Network Configuration** and then click **Location Policy**.
4. On the **Location Policy** page, select the location policy that you want to delete.

   > **Note:**
   > You can delete more than one location policy at a time. To do this, press CTRL and select multiple policies while holding down the CTRL key. Or, to select all policies, click **Select all** on the **Edit** menu.

5. On the **Edit** menu, click **Delete**.
6. Click **OK**.

   > **Important:**
   > You cannot delete the Global location policy. If you attempt to delete the Global policy you will receive a warning message and that policy will be reset to its default values.

Tasks

Creating or Modifying a Location Policy
Viewing Location Policy Information

1.7.16 Managing Lync Server 2013 Services and Server Roles

Managing Lync Server 2013 Services and Server Roles

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-10-15*

You can use the procedures in this section to manage the various services and server roles in Lync Server 2013.

- Audio/Video (A/V) Edge Servers
- Configure a New Trusted Application Server
- Managing Lync Server 2013 Services
- Administering the Address Book Service
- Change the Web Services URL

1.7.16.1 Audio/Video (A/V) Edge Servers

Audio/Video (A/V) Edge Servers

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Services and Server Roles >

Topic Last Modified: *2012-11-01*

The A/V Edge service provide a way for your internal users (users who are logged on to your organizational network) to share audio and video with external users (users who are not logged on to your organizational network). In addition to audio and video, the A/V Edge service also provides support for such things desktop sharing and file transfer.

The A/V Edge service is primarily managed by using A/V Edge configuration; these settings enable you to manage the maximum amount of bandwidth to be allocated per port and per user, and to specify the length of time that an authentication token can be used before that token must be renewed. A/V Edge configuration settings can be applied to sites or to individual A/V Edge servers. When determining which collection of settings will take priority, use the following guide:

- Settings configured at the service scope (that is, on an individual server) take priority over everything.
- Settings configured at the site scope take priority over settings configured at the global scope. However, service scope settings will also supersede site-scope settings.
- Settings at the global scope will be used only if there are no service settings configured on the individual server and if there are no site settings for the site where that server is located.

The A/V Edge service can only be managed by using Lync Server PowerShell and the CsAVEdgeConfiguration cmdlets.

- Return A/V Edge Server Configuration Information
- Create or Modify a Collection of A/V Edge Server Configuration Settings
- Delete an Existing Collection of A/V Edge Server Configuration Settings

1.7.16.1.1 Return A/V Edge Server Configuration Information

Return A/V Edge Server Configuration Information

See Also

Operations > Managing Lync Server 2013 Services and Server Roles > Audio/Video (A/V) Edge Servers >

Topic Last Modified: *2012-11-01*

The A/V Edge service provide a way for your internal users (users who are logged on to your organizational network) to share audio and video with external users (users who are not logged on to your organizational network). The A/V Edge service is primarily managed by using A/V Edge configuration settings, setting that can be configured at the site scope or at the service scope (that is, can be configured for an individual A/V Edge server).

To return information about the A/V Edge configuration settings in use in your organization, you must use Windows PowerShell and the Get-CsAVEdgeConfiguration cmdlet. For more information, see the help topic for the Get-CsAVEdgeConfiguration cmdlet.

Information returned from the Get-CsAVEdgeConfiguration cmdlet will look similar to this:

```
Identity                 : Global
MaxTokenLifetime         : 08:00:00
MaxBandwidthPerUserKb : 10000
MaxBandwidthPerPortKb : 3000
```

To return information for all your A/V Edge configuration settings

- The following command returns information about all the A/V Edge configuration settings currently in use in your organization:

```
Get-CsAVEdgeConfiguration
```

To return information for site-scoped A/V Edge configuration settings

- To return information about a specific collection of A/V Edge configuration settings, specify the Identity of that collection when running the Get-CsAVEdgeConfiguration cmdlet. For example, this command returns information only for the settings applied to the Redmond site:

```
Get-CsAVEdgeConfiguration -Identity "site:Redmond"
```

To return information for service-scoped A/V Edge configuration settings

- And this command returns information only for settings applied the a specific A/V Edge server:

```
Get-CsAVEdgeConfiguration -Identity "service:EdgeServer:atl-edge-001.li
```

Tasks

Create or Modify a Collection of A/V Edge Server Configuration Settings
Delete an Existing Collection of A/V Edge Server Configuration Settings

Other Resources

Audio/Video (A/V) Edge Servers

1.7.16.1.2 Create or Modify a Collection of A/V Edge Server Configuration Settings

Create or Modify a Collection of A/V Edge Server Configuration Settings

See Also

Operations > Managing Lync Server 2013 Services and Server Roles > Audio/Video (A/V) Edge Servers >

***Topic Last Modified:** 2012-11-01*

The A/V Edge service provide a way for your internal users (users who are logged on to your organizational network) to share audio and video with external users (users who are not logged on to your organizational network). The A/V Edge service is primarily managed by using A/V Edge configuration settings, setting that can be configured at the site scope or at the service scope (that is, can be configured for an individual A/V Edge server).

When you install Lync Server, a global collection of A/V Edge configuration settings is created for you. In addition to that, you can use the Windows PowerShell and the New-CsAVEdgeConfiguration cmdlet to create new settings at the site scope or the service scope (that is, for an individual A/V Edge server). If you create new settings keep in mind that:

- Settings configured at the service scope (that is, on an individual server) take priority over everything.
- Settings configured at the site scope take priority over settings configured at the global scope. However, service scope settings will also supersede site-scope settings.
- Settings at the global scope will be used only if there are no service settings configured on the individual server and if there are no site settings for the site where that server is located.

Any of your settings can then be modified by using the Set-CsAVEdgeConfiguration cmdlet. For more information, see the help topics for the New-CsAVEdgeConfiguration and the Set-CsAVEdgeConfiguration cmdlets.

To create new A/V Edge configuration settings at the site scope

- The following command creates a new collection of A/V Edge configuration settings for the Redmond site:

```
New-CsAVEdgeConfiguration -Identity "site:Redmond"
```

To create custom A/V Edge configuration settings at the site scope

- Because no additional parameters were included, these new settings will use the default values for the A/V Edge service. Alternatively, you can add additional parameters and parameter values to create a custom collection. For example, this command sets the MaxTokenLifetime property to 4 hours (04 hours : 00 minutes : 00 seconds):

```
New-CsAVEdgeConfiguration -Identity "site:Redmond" -MaxTokenLifetime "0
```

To create custom A/V Edge configuration settings at the service scope

- This command creates a similar collection applied to the A/V Edge server atl-edge-001.litwareinc.com:

```
New-CsAVEdgeConfiguration -Identity "service:EdgeServer:atl-edge-001.li
```

To modify existing A/V Edge configuration settings

- In this example, the Set-CsAVEdgeConfiguration cmdlet is used to change the maximum token lifetime for the Redmond site to 12 hours:

```
Set-CsAVEdgeConfiguration -Identity "site:Redmond" -MaxTokenLifetime "1
```

Tasks

Return A/V Edge Server Configuration Information
Delete an Existing Collection of A/V Edge Server Configuration Settings

Other Resources

Audio/Video (A/V) Edge Servers
New-CsAVEdgeConfiguration
Set-CsAVEdgeConfiguration

1.7.16.1.3 Delete an Existing Collection of A/V Edge Server Configuration Settings

Delete an Existing Collection of A/V Edge Server Configuration Settings

See Also

Operations > Managing Lync Server 2013 Services and Server Roles > Audio/Video (A/V) Edge Servers >

Topic Last Modified: *2012-11-01*

The A/V Edge service provide a way for your internal users (users who are logged on to your organizational network) to share audio and video with external users (users who are not logged on to your organizational network). The A/V Edge service is primarily managed by using A/V Edge configuration settings, setting that can be configured at the site scope or at the service scope (that is, can be configured for an individual A/V Edge server).

When you install Lync Server, a global collection of A/V Edge configuration settings is created for you. This global collection cannot be deleted. However, you can use the Windows PowerShell and the Remove-CsAVEdgeConfiguration cmdlet to "reset" the global collection; that simply means that all the property values in the global collection will be reset to their default value. For example, if you have set the MaxTokenLifetime property for 16 hours, that property will be reset to its default value of 8 hours.

However, custom settings collections that you have created at either the site scope or the service scope can be deleted by using the Remove-CsAVEdgeConfiguration cmdlet. If you delete site settings then A/V Edge servers in that site will be managed by the global settings. If you delete service-scope settings,, that server will then be managed by its site settings, if they exist, or by the global settings if no site settings are available.

For more information, see the help topic for the Remove-CsAVEdgeConfiguration cmdlet.

⊟To reset the global collection

- The following command resets the global collection of A/V Edge configuration settings:

```
Remove-CsAVEdgeConfiguration -Identity "global"
```

⊟To remove a collection from the site scope

- This command removes the A/V Edge configuration settings applied to the Redmond site:

```
Remove-CsAVEdgeConfiguration -Identity "site:Redmond"
```

⊟To remove a collection from the service scope

- This command removes the settings applied to the A/V Edge server atl-edge-001.litwareinc.com:

```
Remove-CsAVEdgeConfiguration -Identity "service:EdgeServer:atl-edge-001
```

Tasks

Return A/V Edge Server Configuration Information
Create or Modify a Collection of A/V Edge Server Configuration Settings

Other Resources

Audio/Video (A/V) Edge Servers
Remove-CsAVEdgeConfiguration

1.7.16.2 Configure a New Trusted Application Server

Configure a New Trusted Application Server

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Services and Server Roles >

Topic Last Modified: *2012-11-01*

A trusted application is an application based on Microsoft Unified Communications Managed API (UCMA) 3.0 Core SDK that is trusted by Microsoft Lync Server 2013. For details about UCMA applications, see "Unified Communications Managed API 3.0 Core SDK Documentation" at http://go.microsoft.com/fwlink/p/?linkId=210320.

For information about configuring Microsoft Outlook Web Access (OWA) and Lync Server 2013, see "Configure Outlook Web App and Lync Server 2010 Integration" at the Microsoft Exchange Server 2013 documentation.

To successfully publish, enable, or disable a topology when adding or removing a server role, you should be logged on as a user who is a member of the RTCUniversalServerAdmins and Domain Admins groups. It is also possible to delegate the proper administrator permissions and rights for adding server roles. For details, see Delegate Setup Permissions in the Deployment documentation. For other configuration changes, only membership in the RTCUniversalServerAdmins group is required.

⊟To configure a trusted application server

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
3. Select **Download topology from existing deployment**, and then click **OK**.
4. In the **Save Topology As** dialog box, click the Topology Builder file you want to use, and then click **Save**.
5. In the left pane, right-click **Trusted application servers**, and then click **New Trusted Application Pool**.
6. Enter the **Pool FQDN** of the trusted application pool, select whether it will be a single-server or multiple-server, and then click **Next**.
7. On the **Select the next hop** page, from the list, select the Lync Server 2013 Front End pool.
8. Click **Finish**.
9. Select the top node **Lync Server 2013**, and then, from the **Actions** menu, click **Publish Topology**.

   The **Trusted Application Pool** should have been created successfully and associated with the correct Front End pool.

1.7.16.3 Managing Lync Server 2013 Services

Managing Lync Server 2013 Services

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Services and Server Roles >

Topic Last Modified: *2013-02-21*

Use the procedures in this section to manage Lync Server 2013 services from the **Topology** page.

- View the Status of Services Running on a Computer

1.7.16.3.1 View the Status of Services Running on a Computer

View the Status of Services Running on a Computer

See Also

Microsoft Lync Server 2013 > Operations > Managing the Lync Server 2013 Topology >

Topic Last Modified: *2013-02-22*

You can use Lync Server 2013 Control Panel to view all the services that are running on a specific computer in your Lync Server topology and see the status of each service.

To view the status of services running on a computer

1. From a user account that is assigned to the CsUserAdministrator role or the CsAdministrator role, log on to any computer in your internal deployment.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology**.
4. On the **Status** page, sort or search the list, as required, to find the computer you’re interested in, and then click the computer name.
5. Do any of the following:
   - To see the latest status of services running on the computer, click **Get service status**.
   - To see a list of specific services running on the computer and the status of each service, click **Properties**, and then click **Close** to return to the list.

Viewing Service Status by Using Windows PowerShell Cmdlets

You can also view service status by using Windows PowerShell and the **Get-CsWindowsService** cmdlet. You can run this cmdlet from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view service status

- To view service status on a computer, type a command similar to the following in the Lync Server Management Shell and then press Enter:

  ```
  Get-CsWindowsService -ComputerName atl-cs-001.litwareinc.com | Select-C
  ```

  This command returns information similar to the following:

  ```
  RoleName                                  Status
  --------                                  ------
  {W3SVC}                                   Running
  {CentralManagement}                       Running
  {ClsAgent}                                Running
  {Registrar, UserServer, EdgeServer}       Running
  {ApplicationServer}                       Running
  {ConferencingServer}                      Running
  {MediationServer}                         Running
  ```

For details, see Get-CsWindowsService.

See Also

Other Resources

Managing Devices, Phones, and Client Applications

1.7.16.4 Administering the Address Book Service

Administering the Address Book Service

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Services and Server Roles >

***Topic Last Modified:** 2012-11-01*

As a part of the deployment of Lync Server, Enterprise Edition or Standard Edition server, the Address Book Service is installed by default. The database used by the Address Book Service – RTCab – is created on the SQL Server (for Enterprise Edition, this is the back-end SQL Server; for Standard Edition server, the collocated SQL Server).

Address Book Server Phone Number Normalization

Lync Server requires standardized RFC 3966/E.164 phone numbers. To use phone numbers that are unstructured or inconsistently formatted, Lync Server relies on the Address Book Server to preprocess phone numbers before they are handed off to the normalization rules. When a phone number is used from the address book and the normalization rule is applied, clients, such as Lync Phone Edition and Lync Mobile, can use these normalized numbers.

The normalization rules that were used in previous versions may not work properly without some adjustments. Because the white space and non-mandatory characters are removed prior to the normalization rules, if your regex expression is specifically looking for a dash or other character that was removed, your normalization rule might fail. You should review your normalization rules to ensure that either they are not looking for these non-mandatory characters, or that the rule can fail gracefully and continue in the event that the character is not present where the rule anticipates it will be.

User Replicator and Address Book Server

The Address Book Server uses data provided by User Replicator to update the information that it initially obtains from the global address list (GAL). User Replicator writes the Active Directory Domain Services (AD DS) attributes for each user, contact, and group into the AbUserEntry table in the database and the Address Book Server syncs the user data from the database into files in the Address Book Server file store and into the Address Book database RTCab. The schema for the AbUserEntry table uses two columns, **UserGuid** and **UserData**. **UserGuid** is the index column and contains the 16-byte GUID of the Active Directory object. **UserData** is an image column which contains all of the previously mentioned Active Directory Domain Services (AD DS) attributes for that contact.

User Replicator determines which Active Directory attributes to write by reading a configuration table located in the same SQL Server-based instance as the AbUserEntry table. The AbAttribute table contains three columns, **ID**, **Name**, **Flags**, and **Enable**. The table is created during database setup. If the AbAttribute table is empty, User Replicator skips its AbUserEntry table processing logic. Address Book Server attributes are dynamic and are retrieved from the AbAttribute table, which is initially written by the Address Book Server when the Address Book Server is activated.

Address Book Server activation populates the AbAttribute table with the values needed to support Lync Server. The following table shows those current values.

ID	Name	Flags
1	givenName	0x01400000
2	Sn	0x02400000
3	displayName	0x03420000
4	Title	0x04000000
5	mailNickname	0x05400000
6	Company	0x06000000
7	physicalDeliveryOfficeName	0x07000000
8	msRTCSIP-PrimaryUserAddress	0x08520C00
9	telephoneNumber	0x09022800
10	homePhone	0x0A302800
11	Mobile	0x0B622800
12	otherTelephone	0x0C302000
13	ipPhone	0x0D302000
14	Mail	0x0E500000
15	groupType	0x0F010800
16	Department	0x10000000
17	Description	0x11000100
18	Manager	0x12040001
19	proxyAddress	0x00500105
20	msExchHideFromAddressLists	0xFF000003
99	entryID	0x99000000

The numbers in the **ID** column must be unique and should never be reused. Also, keeping the ID values under 256 saves space in the output files written by the Address Book Server. However, the maximum ID value is 65535. The **Name** column corresponds to the Active Directory attribute name that User Replicator should put in the AbUserEntry table for each contact. The value in the **Flags** column is used to define the type of attribute. The following types of Address Book Server attributes are recognized by User Replicator, indicated by the low byte of the value in the **Flags** column.

Attribute	Description
0x0	A string attribute. User Replicator converts this type to UTF-8 before storing it in the AbUserEntry table.
0x1	A binary attribute. User Replicator stores this in the blob without any conversion.

0x2	A string attribute, but is included only if the attribute value begins with "tel:". This is primarily for multi-valued string attributes, specifically **proxyAddresses**. In this case, Address Book Server is interested only in **proxyAddresses** entries that begin with "tel:". Therefore, in the interest of saving space, User Replicator stores only the entries that begin with "tel:".
0x3	A Boolean string attribute, which if TRUE causes User Replicator to not include this contact in the AbUserEntry table. If FALSE, it causes User Replicator to include the attributes for this contact in the AbUserEntry table, but not the particular attribute with this flag. This is another special case type that is primarily for the **msExchHideFromAddressLists** attribute.
0x4	A string attribute, but is included only if the attribute value begins with "smtp:" and includes the "@" symbol.
0x5	A string attribute, but is included only if the attribute value begins with either "tel:" or "smtp:" and includes the "@" symbol.
0x100	If set, this is a multi-valued attribute that can appear more than once for each contact.
0x400	If set, this identifies the email user account name attribute for a contact. Address Book Server uses this flag to identify which attribute value to show in the phone normalization event log entry.
0x800	If set, this identifies a required attribute for a contact. Address Book Server includes a user in the AbUserEntry table only if there is a value for this attribute in Active Directory. If there is more than one required attribute, only one of them is required to have a value to include the user in the AbUserEntry table.
0x1000	If set, Address Book Server always normalizes the value of this attribute.
0x2000	If set, Address Book Server uses the normalized number from **proxyAddresses**, if the **UseNormalizationRules** CMS setting is FALSE; otherwise it behaves the same as when the flag bit is 0x1000.
0x4000	If set, Address Book Server does not include objects in the AbUserEntry table that have this value for the specified attribute. For example, if the **msRTCSIP-PrimaryUserAddress** attribute has this flag bit set, then contacts that have this

	attribute are not written to the database.
0x8000	If set, Address Book Server does not include objects in the AbUserEntry table that do not have this value for the specified attribute. If both the 0x4000 and 0x8000 flag bits are set on an object, the attribute with the flag bit value set to 0x4000 takes precedence, and the object is excluded from the AbUserEntry table.
0x10000	If set, this represents a group object. User Replicator uses this flag bit to include contacts with the **groupType** attribute whose presence indicates a group (for example, a distribution list or security group).
0x20000	If set, User Replicator uses this flag bit to include this attribute in device-specific Address Book Server files (that is, files with a .dabs extension).

In previous versions of Lync Server, when applying a change to Active Directory, the administrator would be required to run **Update -CSUserDatabase** and **Update –CSAddressBook** Windows PowerShell cmdlets to persist the change to the Lync Server user database and RTCab database immediately. In Lync Server 2013, Lync Server User Replicator will pick up the changes from Active Directory and update the Lync Server user database based on a configured interval. Lync Server User Replicator will also propagate the changes to the RTCab database quickly without the administrator having to run Update-CSAddressBook. If Address Book Web query is enabled, then the changes will be reflected in search results by Lync clients. Administrators will only need to run Update -CSAddressBook if the Address Book file download is enabled.

Note:

By default Lync Server User Replicator runs automatically every 5 minutes. You can configure this interval by using Set -CSUserReplicatorConfiguration -ReplicationCycleInterval <>.

Filtering the Address Book

The users populated in the Address Book Server files can be controlled based on certain Active Directory Domain Services (AD DS) attributes listed in the AbAttribute table. One such attribute used for filtering is the **msExchangeHideFromAddressBook** attribute. This is a user attribute added by the Exchange schema. If the value of this attribute is TRUE, Exchange Server uses this attribute to hide the contact from the Outlook Global Address List (GAL). Similarly, if the value of this attribute is TRUE, User Replicator does not include that user in the AbUserEntry table and this user will not be in the Address Book Server files.

You can use some flag bits to define a filter to use on Address Book Server attributes. For example, the presence of certain flag bits can identify an attribute as an include attribute or an exclude attribute. User Replicator filters out contacts that contain an exclude attribute and filters out contains that do not contain an include attribute.

Currently, there are three different filters. The following table lists these filters.

Attribute	Description
0x800	If set, this identifies a required attribute for

	a contact. User Replicator uses this flag bit to filter out contacts that do not contain at least one required attribute. The OuPathId is a required attribute, which is always set. So at least one of other required attributes should be set. Otherwise, contact (that is, with value of required attribute OuPathId) will still not be written to database. For example, if **telephoneNumber** and **homePhone** are defined as required attributes, only the contacts that have at least one of these attributes are written to the database.
0x4000	If set, this identifies an exclude attribute. User Replicator uses this flag bit to filter out contacts that contain this attribute. For example, if **msRTCSIP-PrimaryUserAddress** is defined as an exclude attribute, contacts that have this attribute are not written to the database.
0x8000	If set, this identifies an include attribute. User Replicator uses this flag bit to filter out contacts that do not contain this attribute. For example, if **msRTCSIP-PrimaryUserAddress** is defined as an include attribute, only the contacts that have this attribute are written to the database.

Note:

If both the 0x4000 (exclude attribute) and 0x8000 (include attribute) flag bits are set, the 0x4000 bit overrides the 0x8000 bit and the contact is excluded.

Although you can filter the Address Book to include only certain users, limiting entries does not limit other users' ability to contact the filtered users or to see their presence status. Users can always find, manually send instant messages, or manually initiate calls to users not in the Address Book by entering a user's complete sign-in name. Also, contact information for a user could also be found in Outlook.

While having full contact records in the Address Book files enables you to use Lync 2010 to initiate email, telephone, or Enterprise Voice calls (that is, if Enterprise Voice is enabled on the server) with users that are not configured for Session Initiation Protocol (SIP), some organizations prefer to include only SIP-enabled users in their Address Book Server entries. You can filter the Address Book to include only SIP-enabled users by clearing the 0x800 bit in the **Flags** column of the following required attributes: **mailNickname**, **telephoneNumber**, **homePhone**, and **mobile**. You can also filter the Address Book to include only SIP-enabled users by setting the 0x8000 (include attribute) in the **Flags** column of the **msRTCSIP-PrimaryUserAddress** attribute. This also helps to exclude service accounts from the Address Book files.

After you modify the AbAttribute table, you can refresh the data in the AbUserEntry table by running the cmdlet **Update-CsUserDatabase** command. After UR replication completes, you can update the file in the Address Book Server file store by manually running the cmdlet **UpdateCsAddressBook** command.

Note:

The Front End Server that the Address Book Server is placed is not administratively configurable. One is chosen during deployment—typically, the first Front End Server deployed. In the event of failure, the Address Book Service will move to another Front End Server, and requires no administrative attention.

Important:

If you have consolidated or otherwise modified your infrastructure from a multi-forest deployment or a parent/child deployment (such as consolidating your infrastructure before moving to Lync Server), you may find that the Address Book service download and the Address Book Web Query fails for some users. When in a deployment that had multiple domains or forests, the attribute **MsRTCSIP-OriginatorSid** is populated on the user objects that are exhibiting the issue. The **MsRTCSIP-OriginatorSid** attribute must be set to NULL on these objects to resolve the issue.

1.7.16.4.1 Windows PowerShell Cmdlets for Address Book Management

Windows PowerShell Cmdlets for Address Book Services

See Also

Operations > Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service >

Topic Last Modified: *2012-11-01*

Lync Server provides a number of Windows PowerShell command-line interface cmdlets to manage and configure the Address Book service. Some of these cmdlets are replacements for the ABServer.exe commands used in previous versions of Office Communications Server. In the following topics are the cmdlets that are used to set, create, and retrieve information about the Address Book service, its configuration and information about the Web services that the Address Book service uses when clients retrieve Address Book service files and settings.

All of these cmdlets are issued through the Lync Server Management Shell found in the Lync Server tools on a server or workstation where the administration tools have been installed.

- New-CsAddressBookConfiguration for Address Book Management
- Set-CsAddressBookConfiguration for Address Book Management
- Get-CsAddressBookConfiguration for Address Book Management
- Remove-CsAddressBookConfiguration for Address Book Management
- Test-CsAddressBookService for Address Book Management
- Test-CsAddressBookWebQuery for Address Book Management
- Update-CsAddressBook for Address Book Management
- New-CsClientPolicy for Address Book Management
- Set-CsClientPolicy for Address Book Management
- Get-CsService for Address Book Management
- New-CsWebServiceConfiguration for Address Book Management
- Get-CsWebServiceConfiguration for Address Book Management
- Set-CsWebServiceConfiguration for Address Book Management
- Remove-CsWebServiceConfiguration for Address Book Management

⊟Related Sections

⊟See Also

Other Resources

http://go.microsoft.com/fwlink/p/?linkId=205826

1.7.16.4.1.1 New-CsAddressBookConfiguration for Address Book Management

New-CsAddressBookConfiguration for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the New-CsAddressBookConfiguration cmdlet locally: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "New-CsAddressBookConfiguration
```

The New-CsAddressBookConfiguration cmdlet creates a new configuration to manage the behavior of the Address book. Specific to this cmdlet is the ability to define if the Address Book Service creates the client download files, how and if normalization rules are used, how long to retain delta and compact delta files, delta file size before incorporating a new full file creation, what time of day the full file Address Book is created, and what the internal should be for synchronization of information in the User database.

For example:

```
New-CsAddressBookConfiguration -Identity site:Redmond -KeepDuration 15 -Synchroni
```

Other Resources

New-CsAddressBookConfiguration

1.7.16.4.1.2 Set-CsAddressBookConfiguration for Address Book Management

Set-CsAddressBookConfiguration for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Set-CsAddressBookConfiguration cmdlet locally: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Set-CsAddressBookConfiguration
```

Set-CsAddressBookConfiguration is similar to the New-CsAddressBookConfiguration cmdlet, except it is used to modify an existing configuration.

For example:

```
Set-CsAddressBookConfiguration -identity site:Redmond -RunTimeOfDay 23:00
```

Other Resources

Set-CsAddressBookConfiguration

1.7.16.4.1.3 Get-CsAddressBookConfiguration for Address Book Management

Get-CsAddressBookConfiguration for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

***Topic Last Modified:** 2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Get-CsAddressBookConfiguration cmdlet locally: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Get-CsAddressBookConfiguration
```

The cmdlet Get-CsAddressBookConfiguration returns information about a configuration that already exists.

For example:

```
Get-CsAddressBookConfiguration -Identity site:Redmond
```

Combining the functionality of Get-CsAddressBookConfiguration and Set-CsAddressBookConfiguration allows the administrator to define which configurations to modify and then apply the modifications. For example, this combined:

```
Get-CsAddressBookConfiguration -Filter site:* | Set-CsAddressBookConfiguration -R
```

Returns all configurations in all sites and applies the RunTimeOfDay of 23:00 hours to the configurations.

Other Resources

Get-CsAddressBookConfiguration

1.7.16.4.1.4 Remove-CsAddressBookConfiguration for Address Book Management

Remove-CsAddressBookConfiguration for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

***Topic Last Modified:** 2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Remove-CsAddressBookConfiguration cmdlet locally: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Remove-CsAddressBookConfigurat
```

As the name implies, Remove-CsAddressBookConfiguration will remove the configuration based on the defined Site Identity.

For example:

```
Remove-CsAddressBookConfiguration -Identity site:Redmond
```

Other Resources

Remove-CsAddressBookConfiguration

1.7.16.4.1.5 Test-CsAddressBookService for Address Book Management

Test-CsAddressBookService for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Test-CsAddressBookService cmdlet: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Test-CsAddressBookService"}
```

Lync Server 2013 contains a number of cmdlets that initiate synthetic commands to confirm that a specific function or feature is working properly. Test-CsAddressBookService confirms that a defined user can connect and request the local files from the Address Book Web service.

For example:

```
Test-CsAddressBookService -TargetFqdn atl-cs-001.contoso.com -UserCredential cont
```

Other Resources

Test-CsAddressBookService

1.7.16.4.1.6 Test-CsAddressBookWebQuery for Address Book Management

Test-CsAddressBookWebQuery for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Test-CsAddressBookWebQuery cmdlet: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Test-CsAddressBookService"}
```

Similar to the Test-CsAddressBookService synthetic transaction, Test-CsAddressBookWebQuery performs a query against the Address Book Web Query to ensure that it is operating properly. The cmdlet will connect to the Web Ticket authentication and present the credentials specified in –UserCredential. If authenticated, the cmdlet then present the –TargetSipAddress information. The cmdlet should report success if it was able to retrieve the information about the contact.

For example:

```
Test-CsAddressBookWebQuery -TargetFqdn atl-cs-001.contoso.com -UserCredential con
```

Other Resources

Test-CsAddressBookWebQuery

1.7.16.4.1.7 Update-CsAddressBook for Address Book Management

Update-CsAddressBook for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Update-CsAddressBook cmdlet locally: RTCUniversalUserAdmins, RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Update-CsAddressBook"}
```

The Update-CsAddressBook cmdlet replaces the **abserver.exe –syncNow** command from Office Communications Server. The cmdlet's purpose is to initiate a synchronization immediately rather than waiting for the scheduled time. The first example command updates all Address Books in the organization. The second updates only the Address Book associated with the defined server.

Note:

In Lync Server 2013, Lync Server User Replicator will pick up the changes from Active Directory and update the Lync Server user database based on a configured interval. Lync Server User Replicator will also propagate the changes to the RTCab database quickly without the administrator having to run Update-CSAddressBook. Administrators will only need to run Update -CSAddressBook if the Address Book file download is enabled.

For example:

```
Update-CsAddressBook
```

```
Update-CsAddressBook -Fqdn atl-abs-001.contoso.com
```

Other Resources

Update-CsAddressBook

1.7.16.4.1.8 New-CsClientPolicy for Address Book Management

New-CsClientPolicy for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the New-CsClientPolicy cmdlet: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "New-CsClientPolicy"}
```

The cmdlet New-CsClientPolicy defines a large number of settings for provisioning clients for features that are available in Lync Server 2013. For the Address Book Service, the parameter AddressBookAvailability is of interest. This parameter, which directly impacts the options available to clients, has three possible options:

- WebSearchAndFileDownload
- WebSearchOnly
- FileDownloadOnly

When defined, it determines how the Address Book is accessed by clients. If you define this parameter, you must define one of the options. If you do not modify this setting, the default WebSearchAndFileDownload remains in effect.

For example:

```
New-CsClientPolicy -Identity RedmondClientPolicy -DisableCalendarPresence $True -
```

Other Resources

New-CsClientPolicy

1.7.16.4.1.9 Set-CsClientPolicy for Address Book Management

Set-CsClientPolicy for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Set-CsClientPolicy cmdlet locally: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Set-CsClientPolicy"}
```

Similar to New-CsClientPolicy, the Set-CsClientPolicy cmdlet allows you to modify client settings that are already in place.

For example:

```
Set-CsClientPolicy -Identity RedmondClientPolicy -WebServicePollInterval "00:15:0
```

Other Resources

Set-CsClientPolicy

1.7.16.4.1.10 Get-CsService for Address Book Management

Get-CsService for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Get-CsService cmdlet locally: RTCUniversalUserAdmins, RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Get-CsService"}
```

Get-CsService is valuable to retrieve and display the current configuration of your infrastructure’s defined Web Services. By defining the pool’s fully qualified domain name (FQDN) and the parameter WebServer, the cmdlet returns the web-based services offered by your server, including the Address Book handler and distribution list expansion URIs.

For example:

```
Get-CsService -PoolFqdn "fe01.contoso.net" -WebServer
```

This cmdlet returns the following:

Identity : WebServer:pool01.contoso.net

FileStore : FileStore:dc01.contoso.net

UserServer : UserServer:pool01.contoso.net

PrimaryHttpPort : 80

PrimaryHttpsPort : 443

ExternalHttpPort : 8080

ExternalHttpsPort : 4443

PublishedPrimaryHttpPort : 80

PublishedPrimaryHttpsPort : 443

PublishedExternalHttpPort : 80

PublishedExternalHttpsPort : 443

ReachPrimaryPsomServerPort : 8060

ReachExternalPsomServerPort : 8061

```
AppSharingPortStart : 49152

AppSharingPortCount : 16383

LIServiceInternalUri : https://internalweb.contoso.net/locationinformation/liservice.svc

ABHandlerInternalUri : https://internalweb.contoso.net/abs/handler

ABHandlerExternalUri : https://csweb.contoso.com/abs/handler

DLExpansionInternalUri : https://internalweb.contoso.net/groupexpansion/service.svc

DLExpansionExternalUri : https://csweb.contoso.com/groupexpansion/service.svc

CAHandlerInternalUri : https://internalweb.contoso.net/CertProv/
CertProvisioningService.svc

CAHandlerInternalAnonUri : http://internalweb.contoso.net/CertProv/
CertProvisioningService.svc

CollabContentInternalUri : https://internalweb.contoso.net/CollabContent

CollabContentExternalUri : https://csweb.contoso.com/CollabContent

CAHandlerExternalUri : https://csweb.contoso.com/CertProv/CertProvisioningService.svc

DeviceUpdateDownloadInternalUri : https://internalweb.contoso.net/RequestHandler/
ucdevice.upx

DeviceUpdateDownloadExternalUri : https://csweb.contoso.com/RequestHandlerExt/
ucdevice.upx

DeviceUpdateStoreInternalUri : http://internalweb.contoso.net/RequestHandler/Files

DeviceUpdateStoreExternalUri : https://csweb.contoso.com/RequestHandlerExt/Files

RgsAgentServiceInternalUri : https://internalweb.contoso.net/RgsClients/AgentService.svc

RgsAgentServiceExternalUri : https://csweb.contoso.com/RgsClients/AgentService.svc

MeetExternalUri : https://csweb.contoso.com/Meet

DialinExternalUri : https://csweb.contoso.com/Dialin

CscpInternalUri : https://internalweb.contoso.net/Cscp

ReachExternalUri : https://csweb.contoso.com/Reach

ReachInternalUri : https://internalweb.contoso.net/Reach

WebTicketExternalUri : https://csweb.contoso.com/WebTicket/WebTicketService.svc

WebTicketInternalUri : https://internalweb.contoso.net/WebTicket/WebTicketService.svc

ExternalFqdn : csweb.contoso.com

InternalFqdn : internalweb.contoso.net

DependentServiceList : {Registrar:pool01.contoso.net,
ConferencingServer:pool01.contoso.net}

ServiceId : 1-WebServices-1

SiteId : Site:Redmond

PoolFqdn : pool01.contoso.net

Version : 5

Role : WebServer
```

Other Resources

Get-CsService

1.7.16.4.1.11 New -CsWebServiceConfiguration for Address Book Management

New-CsWebServiceConfiguration for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the New-CsWebServiceConfiguration cmdlet locally: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "New-CsWebServiceConfiguration"}
```

The cmdlet New-CsWebServiceConfiguration defines a new configuration for Web Services in your organization. The scope for the Web Services configuration can only be at the site or service level. It cannot create a new Web Services configuration at the global level. Specifically of interest to the Address Book is the EnableGroupExansion attribute. If set to True, the Web Services can respond to requests for group expansion.

For example:

```
New-CsWebServiceConfiguration -Identity site:Redmond -EnableGroupExpansion $False
```

Other Resources

New-CsWebServiceConfiguration

1.7.16.4.1.12 Get-CsWebServiceConfiguration for Address Book Management

Get-CsWebServiceConfiguration for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Get-CsWebServiceConfiguration cmdlet locally: RTCUniversalUserAdmins, RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Get-CsWebServiceConfiguration"}
```

Get-CsWebServiceConfiguration returns information of the Web Services configuration currently in use in your organization. Of interest to the Address Book Services is the status of Distribution List Expansion function. If the attribute EnableGroupExpansion is True, your organization currently allows group expansion.

For example:

```
Get-CsWebServiceConfiguration -Identity site:Redmond
```

Other Resources

Get-CsWebServiceConfiguration

1.7.16.4.1.13 Set-CsWebServiceConfiguration for Address Book Management

Set-CsWebServiceConfiguration for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Set-CsWebServiceConfiguration cmdlet locally: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Set-CsWebServiceConfiguration"}
```

The Set-CsWebServiceConfiguration cmdlet allows the administrator to redefine an existing attribute in the configuration of the Web Services.

For example:

```
Set-CsWebServiceConfiguration -Identity site:Redmond -EnableGroupExpansion $True
```

Other Resources

Set-CsWebServiceConfiguration

1.7.16.4.1.14 Remove-CsWebServiceConfiguration for Address Book Management

Remove-CsWebServiceConfiguration for Address Book Management

See Also

Managing Lync Server 2013 Services and Server Roles > Administering the Address Book Service > Windows PowerShell Cmdlets for Address Book Services >

Topic Last Modified: *2012-11-01*

Who can run this cmdlet: By default, members of the following groups are authorized to run the Remove-CsWebServiceConfiguration cmdlet locally: RTCUniversalServerAdmins. To return a list of all the role-based access control (RBAC) roles this cmdlet has been assigned to (including any custom RBAC roles you have created yourself), run the following command from the Windows PowerShell prompt:

```
Get-CsAdminRole | Where-Object {$_.Cmdlets -match "Remove-CsWebServiceConfigurati
```

The Remove-CsWebServiceConfiguration cmdlet allows an administrator to remove a previously created Web Services configuration. The cmdlet cannot remove the global Web Services configuration.

For example:

```
Remove-CsWebServiceConfiguration -Identity site:Redmond
```

Other Resources

Remove-CsWebServiceConfiguration

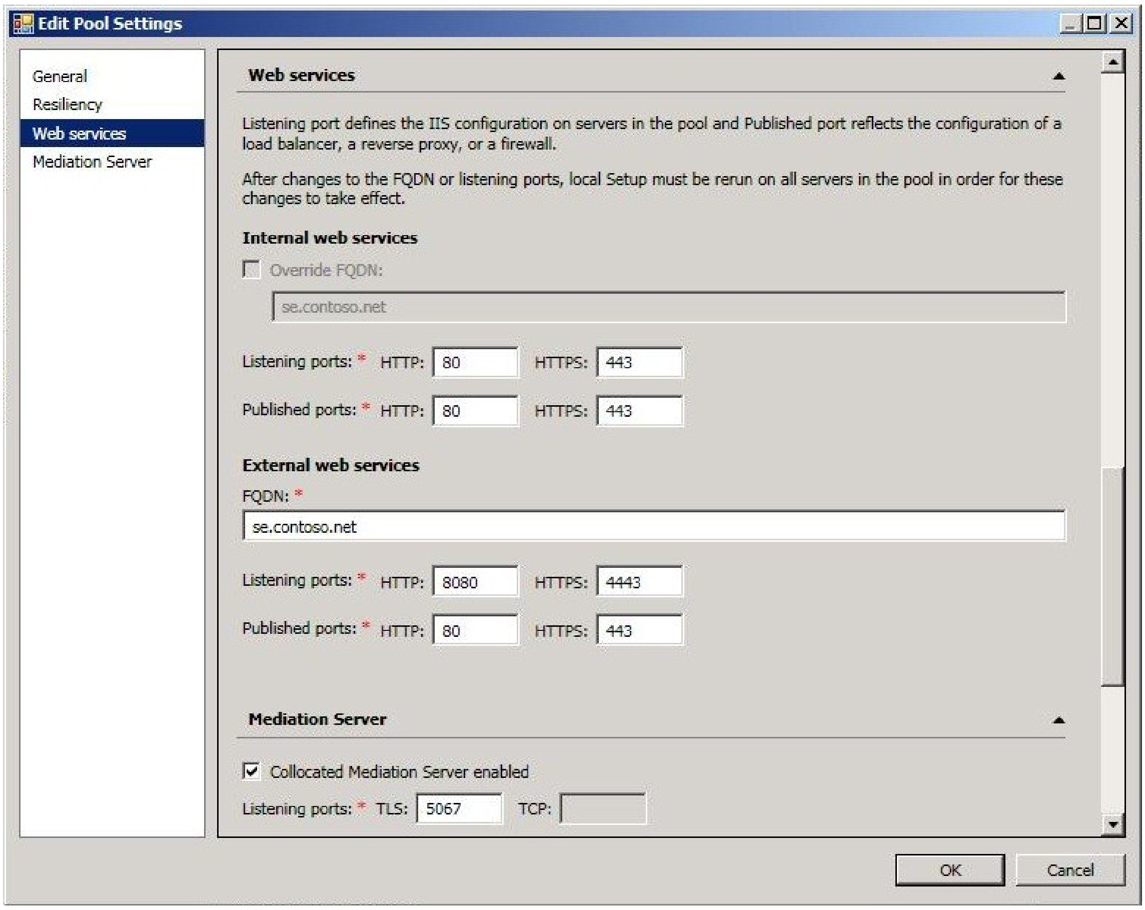
1.7.16.5 Change the Web Services URL

Change the Web Services URL

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Services and Server Roles >

Topic Last Modified: *2012-11-01*

When you set up your Front End pools and Standard Edition servers, you have the option to configure an external Web farm fully qualified domain name (FQDN) and associated ports. If you did not configure this URL when you ran the Lync Server Deployment Wizard, you need to manually configure these settings. An administrator typically does not need to modify these settings, as these are the recommended and default ports.



Web services

Listening port defines the IIS configuration on servers in the pool and Published port reflects the configuration of a load balancer, a reverse proxy, or a firewall.

After changes to the FQDN or listening ports, local Setup must be rerun on all servers in the pool in order for these changes to take effect.

Internal web services

□ Override FQDN:

se.contoso.net

Listening ports: * HTTP: 80 HTTPS: 443

Published ports: * HTTP: 80 HTTPS: 443

External web services

FQDN: *

se.contoso.net

Listening ports: * HTTP: 8080 HTTPS: 4443

Published ports: * HTTP: 80 HTTPS: 443

Mediation Server

☑ Collocated Mediation Server enabled

Listening ports: * TLS: 5067 TCP:

To configure web services

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
3. In Topology Builder, in the console tree under **Standard Edition Front End Servers**, **Enterprise Edition Front End pools**, and **Directory pools**, select the pool name. Right-click the name, click **Edit Properties**, and then click **Web Services**.
4. Add or edit the **External Web Services FQDN**, and then click **OK**.

Warning:

If you have more than one Front End pool or Front End Server the external Web services FQDN must be unique. For example, if you define the external Web services FQDN of a Front End Server as **pool01.contoso.com**, you cannot use **pool01.contoso.com** for another Front End pool or Front End Server. If you are also deploying Directors, the external Web services FQDN defined for any Director or Director pool must be unique from any other Director or Director pool as well as any Front End pool or Front End Server.

5. Verify the listening and published ports are configured correctly for your environment.
6. Repeat these steps for all Standard Edition servers, Front End Pools, and Director pools in your environment.
7. In the console tree, click **Lync Server 2013**, and then, in the **Actions** pane, click **Publish Topology**.

There are a few requirements you should be aware of when configuring the Listening and Publishing ports:

- The listening ports shown are the ports that are configured for Internet Information Server (IIS) on each Front End Server.
- The internal and external listening ports must be different for IIS. For the external listening ports, these are typically the same because one represents the hardware load balancer for internal web traffic and one represents the reverse proxy server for external web traffic.
- You can override the Internal web services on a Front End pool, Director or a Director pool and define your own FQDN.

  ⚠**Warning:**

  If decide to override the Internal web services with a self-defined FQDN, each FQDN must be unique from any other Front End pool, Director or a Director pool.

- The published ports must be configured on the reverse proxy or hardware load balancer as listening ports.
- For an Front End pool (not shown in the example), the internal SIP pool FQDN must be different from the internal web services FQDN, because web traffic comes through the hardware load balancer and the internal SIP pool traffic travels comes through the DNS load balancer. This requirement must be met.
- A Lync Server Standard Edition deployment does not need or allow an internal web services FQDN to be overridden because this server cannot be load balanced.
- If you have a hardware load balancer in your environment that you use for both internal SIP and web traffic, the Topology Builder cannot make the distinction.

The external web services works in conjunction with a reverse proxy in the perimeter network. It provides clients external access to by using these web services. The FQDNs configured here are sent to clients when they log on, and are used to make an HTTPS connection back to the reverse proxy when connecting remotely. The reverse-proxy server forwards the external web service FQDN to an internal hardware load balancer, or directly to the pool. The reverse proxy must be able to resolve the external web services FQDN to the IP address of the internal Web server. The external web services FDQN must be resolvable in the public Internet.

If your internal server is a Standard Edition server, the internal FQDN is the Standard Edition server FQDN. If your internal server is a Front End pool, the FQDN is a hardware load balancer virtual IP (VIP) that load balances the internal web farm servers. A hardware load balancer is required in a Front End pool with more than one Enterprise Edition server. A load balancer is not required for a Standard Edition server or a single Enterprise Edition Front End Server.

1.7.17 Managing Applications

Managing Applications

See Also

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-11-01*

Use the procedures in this section to manage applications for Lync Server 2013.

- Configure a New Trusted Application Server
- Trusted Applications (Application/Computer/Endpoint/Pool)

⊟See Also

Other Resources

Managing Lync Server 2013 Services and Server Roles

1.7.17.1 Configure a New Trusted Application Server

Configure a New Trusted Application Server

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Services and Server Roles >

Topic Last Modified: *2012-11-01*

A trusted application is an application based on Microsoft Unified Communications Managed API (UCMA) 3.0 Core SDK that is trusted by Microsoft Lync Server 2013. For details about UCMA applications, see "Unified Communications Managed API 3.0 Core SDK Documentation" at http://go.microsoft.com/fwlink/p/?linkId=210320.

For information about configuring Microsoft Outlook Web Access (OWA) and Lync Server 2013, see "Configure Outlook Web App and Lync Server 2010 Integration" at the Microsoft Exchange Server 2013 documentation.

To successfully publish, enable, or disable a topology when adding or removing a server role, you should be logged on as a user who is a member of the RTCUniversalServerAdmins and Domain Admins groups. It is also possible to delegate the proper administrator permissions and rights for adding server roles. For details, see Delegate Setup Permissions in the Deployment documentation. For other configuration changes, only membership in the RTCUniversalServerAdmins group is required.

⊟To configure a trusted application server

1. Log on to the computer where Topology Builder is installed as a member of the Domain Admins group and the RTCUniversalServerAdmins group.
2. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
3. Select **Download topology from existing deployment**, and then click **OK**.
4. In the **Save Topology As** dialog box, click the Topology Builder file you want to use, and then click **Save**.
5. In the left pane, right-click **Trusted application servers**, and then click **New Trusted Application Pool**.
6. Enter the **Pool FQDN** of the trusted application pool, select whether it will be a single-server or multiple-server, and then click **Next**.
7. On the **Select the next hop** page, from the list, select the Lync Server 2013 Front End pool.
8. Click **Finish**.
9. Select the top node **Lync Server 2013**, and then, from the **Actions** menu, click **Publish Topology**.

   The **Trusted Application Pool** should have been created successfully and associated with the correct Front End pool.

1.7.17.2 Trusted Applications (Application/Computer/Endpoint/Pool)

Trusted Applications (Application/Computer/Endpoint/Pool)

See Also

Microsoft Lync Server 2013 > Operations > Managing Applications >

Topic Last Modified: *2012-11-01*

Use the procedures in this section to manage trusted applications for Lync Server 2013.

- Managing Trusted Applications

⊟Related Sections

Trusted Applications Cmdlets

⊟See Also

Other Resources

Managing Trusted Applications

1.7.17.2.1 Managing Trusted Applications

Managing Trusted Applications

Operations > Managing Applications > Trusted Applications (Application/Computer/Endpoint/Pool) >

Topic Last Modified: *2012-11-01*

Use the procedures in this section to view either a list of trusted applications or view information about a trusted application in Lync Server 2013. You can do these procedures in Lync Server 2013 Control Panel or Lync Server Management Shell.

- View a List of Trusted Applications
- View Trusted Application Information

1.7.17.2.1.1 View a List of Trusted Applications

View a List of Trusted Applications

See Also

Managing Applications > Trusted Applications (Application/Computer/Endpoint/Pool) > Managing Trusted Applications >

Topic Last Modified: *2012-09-21*

You can use Lync Server 2013 Control Panel to view a list of the trusted applications that you have deployed in your Lync Server 2013 environment. A trusted application is an application based on Microsoft Unified Communications Managed API (UCMA) 3.0 Core SDK that is trusted by Lync Server 2013. This trust relationship is summarized in the following list:

- Trusted applications are not challenged for authentication by Lync Server.
- Trusted applications are not throttled by Lync Server for SIP transactions, connections or outgoing Voice over Internet Protocol (VoIP) calls.
- Trusted applications can impersonate any user and can join conferences without appearing in rosters.
- Trusted applications are highly available and resilient.

In Lync Server Control Panel, you can see the name of the applications, the pool where they run, and the port they use.

⊟To view a list of trusted applications

1. From a user account that is assigned to the CsServerAdministrator, CsAdministrator, CsHelpDesk, or CsViewOnlyAdministrator role, log on to any

computer in your internal deployment. For details about the predefined administrative roles available in Lync Server 2013, see Planning for Role-Based Access Control.

2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Topology** and the click **Trusted Application**.
4. On the **Trusted Application** page, click a column heading to sort the applications, if needed.

Other Resources

Managing the Lync Server 2013 Topology

1.7.17.2.1.2 View Trusted Application Information

View Trusted Application Information

Managing Applications > Trusted Applications (Application/Computer/Endpoint/Pool) > Managing Trusted Applications >

Topic Last Modified: *2013-02-23*

You can view information about your trusted applications by using Windows PowerShell and the **Get-CsTrustedApplication** cmdlet. This cmdlet can be run either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

⊟To view trusted applications

- To view all of your trusted applications, type the following command in the Lync Server Management Shell and then press ENTER:

```
Get-CsConferenceDisclaimer
```

This command returns information similar to the following for each trusted application:

```
Identity                : CN={5dedf4b0-a590-49b3-80cf-f16f914bbef9},CN=A
                          Service,CN=Services,CN=Configuration,DC=litwar
RegistrarPool           : 487279971
HomeServer              : CN=Lc Services,CN=Microsoft,CN=co1:2,CN=Pools,
                          Service,CN=Services,CN=Configuration,DC=litwar
OwnerUrn                : urn:application:helpdesk
SipAddress              : sip:RtcApplication-dbf5142f-2bb2-4c4f-9531-b7f
DisplayName             :
DisplayNumber           :
LineURI                 :
PrimaryLanguage         : 0
SecondaryLanguages      : {}
EnterpriseVoiceEnabled  : True
ExUmEnabled             : False
Enabled                 : True
```

For details, see Get-CsTrustedApplication.

1.7.18 Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service

Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service

See Also

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-11-12*

This section contains procedures for disaster recovery operations, as well as for maintaining the Backup Service which synchronizes the data in paired Front End pools.

Disaster recovery procedures, both failover and failback, are manual. If there is a disaster, the administrator must manually invoke the failover procedures. The same applies to failback after the pool is repaired.

The disaster recovery procedures in the rest of this section assume the following:

- You have a deployment with paired Front End pools, located in different sites, as described in Planning for High Availability and Disaster Recovery. The Backup Service has been running on these paired pools to keep them synchronized.
- If the Central Management store is hosted on either pool, it is installed and running on both of the paired pools, with one of those pools hosting the active master and the other pool hosting the standby.

> **Important:**
>
> In the following procedures, the *PoolFQDN* parameter refers to the FQDN of the pool that is affected by disaster, not the pool that affected users are being redirected from. For the same set of affected users, it refers to the same pool in both failover and failback cmdlets (that is, the pool that first homed the users before the failover).
> For example, assume a case in which all users homed on a pool P1 were failed over to the backup pool, P2. If the administrator wants to move all the users currently serviced by P2 to be serviced by P1, the administrator must perform the following steps:
>
> 1. Fail back all the users originally homed on P1 from P2 to P1 using the failback cmdlet. In this case, the *PoolFQDN* is P1’s FQDN.
> 2. Fail over all the users originally homed on P2 to P1 using the failover cmdlet. In this case, the *PoolFQDN* is P2’s FQDN.
> 3. If the administrator later wants to fail back those P2 users back to P2, the *PoolFQDN* is P2’s FQDN.
>
> Note that step 1 above must be performed before step 2 to preserve pool integrity. If you try step 2 before step 1, the step 2 cmdlet will fail.

- Configuring and Monitoring the Backup Service
- Failing Over a Pool
- Failing Back a Pool
- Failing Over a Mirrored Database
- Failing Over the Edge Pool Used for Lync Server Federation
- Failing Over the Edge Pool Used for XMPP Federation
- Failing Back the Edge Pool Used for Lync Server Federation or XMPP Federation
- Changing the Edge Pool Associated with a Front End Pool
- Restoring Conference Contents Using the Backup Service

⊟See Also

Concepts

Planning for High Availability and Disaster Recovery

1.7.18.1 Configuring and Monitoring the Backup Service

Configuring and Monitoring the Backup Service

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service >

Topic Last Modified: *2012-11-01*

You can use the following Lync Server Management Shell commands to configure and monitor the Backup Service.

Note:

The RTCUniversalServerAdmins group is the only group that has permissions to run **Get-CsBackupServiceStatus** by default. To use this cmdlet, log on as a member of this group. Or, you can grant access to this command to other groups (for example, CSAdministrator) by using the **Set-CsBackupServiceConfiguration** cmdlet.

To see the Backup Service configuration

Run the following cmdlet:

```
Get-CsBackupServiceConfiguration
```

The default for SyncInterval is two minutes.

To set the Backup Service sync interval

Run the following cmdlet:

```
Set-CsBackupServiceConfiguration -SyncInterval interval
```

For example, the following sets the interval to three minutes.

```
Set-CsBackupServiceConfiguration -SyncInterval 00:03:00
```

Important:

Although you can use this cmdlet to change the default sync interval for the Backup Service, you should not do so unless it is absolutely necessary, as the sync interval has a great impact on the Backup Service performance and the recovery point objective (RPO).

To get the Backup Service status for a particular pool

Run the following cmdlet:

```
Get-CsBackupServiceStatus -PoolFqdn <pool-FQDN>
```

Note:

The Backup Service sync status is defined unidirectionally from a pool (P1) to its backup pool (P2). The sync status from P1 to P2 can be different than the one from P2 to P1. For P1 to P2, Backup Service is in a “steady” state if all the changes made in P1 are completely replicated over to P2 within the sync interval. It is in the “final” state if there are no more changes to be synchronized from P1 to P2. Both states indicate a snapshot of the Backup Service at the time the cmdlet is executed. It does not imply that the state returned will stay as is afterwards. In particular, the “final” state will continue to hold only if P1 does not generate any changes after the cmdlet is executed. This is true in the case of failing P1 over to P2 after P1 is placed into the read-only mode as part of the

Invoke-CsPoolfailover execution logic.

To get information about the backup relationship for a particular pool

Run the following cmdlet:

```
Get-CsPoolBackupRelationship -PoolFQDN <poolFQDN>
```

To force a Backup Service sync

Run the following cmdlet:

```
Invoke-CsBackupServiceSync -PoolFqdn <poolFqdn> [-BackupModule  {All|PresenceFocu
```

1.7.18.2 Failing Over a Pool

Failing Over a Pool

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service >

Topic Last Modified: *2012-11-01*

If a single Front End pool has failed and needs to be failed over, use the following procedure. In this procedure, Datacenter1 contains Pool1, and Pool1 has failed. You are failing over to Pool2 located in Datacenter2.

Most of the work for the pool failover involves failing over the Central Management store, if it is required. This is important because the Central Management store must be functional when the pool's users are failed over.

Additionally, if a Front End pool fails but the Edge pool at that site is still running, you must know whether the Edge pool uses the failed pool as a next hop pool. If it does, you must change the Edge pool to use a different Front End pool before failing over the failed Front End pool. How you change the next hop setting depends on whether the Edge will use a pool at the same site as the Edge pool, or a different site.

To Set an Edge Pool to Use a Next Hop Pool at the Same Site

1. Open Topology Builder, right-click the Edge pool that needs to be changed, and click **Edit Properties**.
2. Click **Next Hop**. From the **Next hop pool:** list, select the pool which will now serve as the next hop pool.
3. Click **OK**, and then publish the changes.

To Set an Edge Pool to Use a Next Hop Pool at a Different Site

1. Open a Lync Server Management Shell window and type the following cmdlet:

   ```
   Set-CsEdgeServer -Identity EdgeServer:<edge server FQDN> -Registrar Re
   ```

To Fail Over a Pool in a Disaster

1. Find which pool is the host for the Central Management Server by typing the following cmdlet on a Front End server in Pool2:

   ```
   Invoke-CsManagementServerFailover -Whatif
   ```

   The results of this cmdlet show which pool currently hosts the Central Management Server. In the rest of this procedure, this pool is known as CMS_Pool.
2. Use Topology Builder to find the version of Lync Server running on the CMS_Pool. If it is running Lync Server 2013, use the following cmdlet to find the backup pool of Pool 1.

```
Get-CsPoolBackupRelationship -PoolFQDN <CMS_Pool FQDN>
```

Let Backup_Pool be the backup pool.

3. Check the status of the Central Management store with the following cmdlet:

   ```
   Get-CsManagementStoreReplicationStatus -CentralManagementStoreStatus
   ```

   This cmdlet should show that both ActiveMasterFQDN and ActiveFileTransferAgents are pointing to the FQDN of CMS_Pool. If they are empty, the Central Management Server is not available and you must fail it over.
4. If the Central Management store is not available or if the Central Management store was running on Pool1 (that is, the pool that has failed), you must fail over the Central Management Server before failing over the pool. If you need to fail over the Central Management Server that was hosted on a pool running Lync Server 2013, use the cmdlet in step 5 of this procedure. If you need to fail over the Central Management Server that was hosted on a pool running Lync Server 2010, use the cmdlet in step 6 of this procedure. If you do not need to fail over the Central Management Server, skip to step 7 of this procedure.
5. To fail over the Central Management store on a pool running Lync Server 2013, do the following:
   - First, check which Back End Server in Backup_Pool runs the principal instance of the Central Management store by typing the following:

     ```
     Get-CsDatabaseMirrorState -DatabaseType CMS -PoolFqdn <Backu
     ```

   - If the primary Back End Server in Backup_Pool is the principal, type:

     ```
     Invoke-CSManagementServerFailover -BackupSQLServerFqdn <Back
     ```

     If the mirror Back End Server in Backup_Pool is the principal, type:

     ```
     Invoke-CSManagementServerFailover -MirrorSQLServerFqdn <Back
     ```

   - Validate that the Central Management Server failover is complete. Type the following:

     ```
     Get-CsManagementStoreReplicationStatus -CentralManagementSto
     ```

     Check that both ActiveMasterFQDN and ActiveFileTransferAgents are pointing to the FQDN of Backup_Pool.
   - Finally, check the replica status for all Front End Servers by typing the following:

     ```
     Get-CsManagementStoreReplicationStatus
     ```

     Check that all replicas have a value of True.
     Skip to step 7 in this procedure.
6. Install the Central Management store on the Back End Server of Backup_Pool.
   - First, run the following command:

     ```
     Install-CsDatabase -CentralManagementDatabase -Clean -SqlSer
     ```

   - Run the next command on one of the Front End Servers of Backup_Pool to force the move of the Central Management store:

     ```
     Move-CsManagementServer -ConfigurationFileName c:\CsConfigur
     ```

   - Validate the move is complete:

     ```
     Get-CsManagementStoreReplicationStatus -CentralManagementSto
     ```

     Check that both ActiveMasterFQDN and ActiveFileTransferAgents are pointing to the FQDN of Backup_Pool.
   - Check the replica status for all Front End Servers by typing the following:

     ```
     Get-CsManagementStoreReplicationStatus
     ```

     Check that all replicas have a value of True.

- Install the Central Management Server service on the rest of the Front End Servers in Backup_Pool. To do so, run the following command on all the Front End Servers, except the one you used when forcing the Central Management store move earlier in this procedure:

```
Bootstrapper /Setup
```

7. Fail over the users from Pool1 to Pool2 by running the following cmdlet in a Lync Server Management Shell window:

```
Invoke-CsPoolFailover -PoolFQDN <Pool1 FQDN> -DisasterMode -Verbose
```

Because the steps taken in the previous parts of this procedure to check the Central Management store status are not universal, there is still a chance this cmdlet will fail because the Central Management store is not yet fully failed over. In this case, you must fix the Central Management store based on the error messages that you see, and then run this cmdlet again.

If you see the following error message, then you need to change the Edge pool at this site to use a different pool as its next hop before failing over the pool. For details, see the procedures at the beginning of this topic.

```
Invoke-CsPoolFailOver : This Front-end pool "pool1.contoso.com" is spe
topology as the next hop for the Edge server. Failing over this pool m
access/Federation/Split-domain/XMPP features to stop working. Please u
change the Edge internal next hop setting to point to a different Fron


proceed.
```

1.7.18.3 Failing Back a Pool

Failing Back a Pool

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service >

Topic Last Modified: *2012-11-01*

After the pool that experienced the disaster is back online (that is, Pool1 in this example), take the following steps to restore your deployment to regular working status.

Note that the failback process takes several minute to complete. For reference, it is expected to take up to 60 minutes for a pool of 20,000 users.

1. Fail back the users who were originally homed in Pool1 and have been failed over to Pool2 by typing the following cmdlet:

```
Invoke-CsPoolFailback -PoolFQDN <Pool1 FQDN> -Verbose
```

No other steps are necessary. If you failed over the Central Management Server, you can leave it in Pool2.

1.7.18.4 Failing Over a Mirrored Database

Failing Over a Mirrored Database

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service >

Topic Last Modified: *2012-11-01*

If you have configured your back-end database to use synchronized mirroring with a witness, failover is automatic. If you have configured synchronized mirroring without a witness, you can use the following procedures to failover and failback your database. You can also use these procedures to manually failover and failback your databases even if you have configured a witness.

To fail over your back-end database

1. Before failing over, determine which back-end database is the principal and which is the mirror by typing the following cmdlet:

   ```
   Get-CsDatabaseMirrorState -PoolFqdn <poolFQDN> -DatabaseType User
   ```

2. If the Central Management store is hosted in this pool, type the following cmdlet to determine which is the principal and which is the mirror for the Central Management store:

   ```
   Get-CsDatabaseMirrorState -PoolFqdn <poolFQDN> -DatabaseType CMS
   ```

3. Perform the failover of the user database:
   - If the primary has failed and you are failing over to the mirror, type:

     ```
     Invoke-CsDatabaseFailover -PoolFqdn <poolFQDN> -DatabaseType
     ```

   - If the mirror has failed and you are failing over to the primary, type:

     ```
     Invoke-CsDatabaseFailover -PoolFqdn <poolFQDN> -DatabaseType
     ```

4. If the pool hosts the Central Management Server, perform the failover of the Central Management store.
   - If the primary has failed and you are failing over to the mirror, type:

     ```
     Invoke-CsDatabaseFailover -PoolFqdn <poolFQDN> -DatabaseType
     ```

   - If the mirror has failed and you are failing over to the primary, type:

     ```
     Invoke-CsDatabaseFailover -PoolFqdn <poolFQDN> -DatabaseType
     ```

1.7.18.5 Failing Over the Edge Pool Used for Lync Server Federation

Failing Over the Edge Pool Used for Lync Server Federation

See Also

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service >

Topic Last Modified: *2012-09-17*

If the Edge pool where you have Lync Server federation configured goes down, you must change federation to use a different Edge pool for federation to work.

⊟Failing Over the Edge Pool Used for Lync Server Federation

1. On a Front End server, open Topology Builder. Expand **Edge pools**, then right click the Edge server or Edge server pool that is currently configured for Federation. Select **Edit properties**.
2. In **Edit Properties** under **General**, clear **Enable federation for this Edge pool (Port 5061)**. Click **OK**.
3. Expand **Edge pools**, then right click the Edge server or Edge server pool that you now want to use for Federation. Select **Edit properties**.
4. In **Edit Properties** under **General**, select **Enable federation for this Edge pool (Port 5061)**. Click **OK**.
5. Click **Action**, select **Topology**, select **Publish**. When prompted on **Publish the topology**, click **Next**. When the Publish is finished, click **Finish**.
6. On the Edge server, open the Lync Server Deployment wizard. Click **Install or Update Lync Server System**, then click **Setup or Remove Lync Server**

Components. Click **Run Again**.

7. At Setup Lync Server components, click **Next**. The summary screen will show actions as they are executed. Once the deployment is done, click **View Log** to view available log files. Click **Finish** to complete the deployment.

   If the site containing the failed Edge pool contains Front End Servers that are still running, you must update the Web Conferencing Service and A/V Conferencing Service on these Front End pools to use an Edge pool in a remote site that is still running. For more information, see Changing the Edge Pool Associated with a Front End Pool.

Tasks

Failing Over the Edge Pool Used for XMPP Federation
Failing Back the Edge Pool Used for Lync Server Federation or XMPP Federation

Concepts

Edge Server High Availability and Disaster Recovery

1.7.18.6 Failing Over the Edge Pool Used for XMPP Federation

Failing Over the Edge Pool Used for XMPP Federation

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service >

Topic Last Modified: *2012-10-19*

In your organization, there is one Edge pool designated as the pool to use for XMPP federation. If this pool goes down, you must fail over XMPP federation to use a different Edge pool before XMPP federation can work again.

When you first install Edge pools and enable XMPP Federation, you can simplify the disaster recovery process by setting up external DNS SRV records for all of your Edge pools for XMPP federation, instead of just one. Each of these SRV records must have a different priority set. All XMPP federation traffic goes through the pool with the SRV record with the highest priority. For more information on enabling and setting up XMPP federation, see Setting Up XMPP Federation.

In the following procedure, EdgePool1 is the pool which originally hosted XMPP federation, and EdgePool2 is the pool which will now host XMPP federation.

⊟Failing Over the Edge Pool Used for XMPP Federation

1. If you don't already have another Edge pool deployed (besides the one which is currently down), deploy that pool. For details, see Deploying External User Access.
2. On each Edge Server in the new Edge pool which will now host XMPP federation (EdgePool2), run the following cmdlet:

   ```
   Stop-CsWindowsService
   ```

3. Run the following cmdlet to repoint the XMPP federation route to EdgePool2:

   ```
   Set-CsSite Site2 -XmppExternalFederationRoute EdgeServer2.contoso.com
   ```

   In this example, Site2 is the site containing the Edge pool which will now host the XMPP federation route, and EdgeServer2.contoso.com is the FQDN of an Edge Server in that pool.
4. On the external DNS server, change the DNS A record for XMPP federation to point to EdgeServer2.contoso.com.
5. If you do not already have a DNS SRV record for XMPP federation which resolves to the Edge pool which will now host XMPP federation, you must add it, as in the following example. This SRV record must have a port value of 5269.

```
_xmpp-server._tcp.contoso.com
```

6. Verify that the Edge pool which will now host XMPP federation has port 5269 open externally.
7. Start the services on all Edge Servers in the Edge pool which will now host XMPP federation:

```

Start-CsWindowsService
```

1.7.18.7 Failing Back the Edge Pool Used for Lync Server Federation or XMPP Federation

Failing Back the Edge Pool Used for Lync Server Federation or XMPP Federation

See Also

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service >

Topic Last Modified: *2012-11-01*

After a failed Edge pool that used to host federation has been brought back online, use this procedure to fail back the Lync Server federation route and/or the XMPP federation route to again use this restored Edge pool.

Failing Back Federation to a Restored Edge Pool

1. On the Edge pool that is now available again, start the Edge Services.
2. If you want to fail back the Lync Server federation route to use the restored Edge Server, do the following:
   - On a Front End server, open Topology Builder. Expand **Edge pools**, then right click the Edge server or Edge server pool that is currently configured for Federation. Select **Edit properties**.
   - In **Edit Properties** under **General**, clear **Enable federation for this Edge pool (Port 5061)**. Click **OK**.
   - Expand **Edge pools**, then right click the original Edge server or Edge server pool that you again want to use for Federation. Select **Edit properties**.
   - In **Edit Properties** under **General**, select **Enable federation for this Edge pool (Port 5061)**. Click **OK**.
   - Click **Action**, select **Topology**, select **Publish**. When prompted on **Publish the topology**, click **Next**. When the Publish is finished, click **Finish**.
   - On the Edge server, open the Lync Server Deployment wizard. Click **Install or Update Lync Server System**, then click **Setup or Remove Lync Server Components**. Click **Run Again**.
   - At Setup Lync Server components, click **Next**. The summary screen will show actions as they are executed. Once the deployment is done, click **View Log** to view available log files. Click **Finish** to complete the deployment.
3. If you want to fail back the XMPP federation route to use the restored Edge Server, do the following:
   - Run the following cmdlet to repoint the XMPP federation route to the Edge pool which will now host XMPP federation (in this example, EdgeServer1):

     ```
     Set-CsSite Site1 -XmppExternalFederationRoute EdgeServer1.c
     ```

     In this example, Site1 is the site containing the Edge pool which will now host the XMPP federation route, and EdgeServer1.contoso.com is the FQDN of an Edge Server in that pool.
   - If you do not already have a DNS SRV record for XMPP federation which

resolves to the Edge pool which will now host XMPP federation, you must add it, as in the following example. This SRV record must have a port value of 5269.

```
_xmpp-server._tcp.contoso.com
```

- On the external DNS server, change the DNS A record for XMPP federation to point to EdgeServer2.contoso.com.
- Verify that the Edge pool which will now host XMPP federation has port 5269 open externally.

4. If the Front End pools remained running in the site containing the Edge pool that failed and has been restored, you should update the Web Conferencing Service and A/V Conferencing Service on these Front End pools to again use the Edge pools at their local site. For more information, see Changing the Edge Pool Associated with a Front End Pool.
5. If the Front End pool at the same site as the failed Edge pool also failed, you can now use Invoke–CsPoolFailback to fail back the Front End pool.

Tasks

Failing Over the Edge Pool Used for Lync Server Federation
Failing Over the Edge Pool Used for XMPP Federation

Concepts

Edge Server High Availability and Disaster Recovery

1.7.18.8 Changing the Edge Pool Associated with a Front End Pool

Changing the Edge Pool Associated with a Front End Pool

See Also

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service >

Topic Last Modified: *2012-09-21*

If an Edge pool goes down but the Front End pool at the same site is still running, you will need to set the Front End pool to use an Edge pool at a different site until the failed Edge pool is restored.

Changing the Edge Pool Associated with a Front End Pool

1. In Topology Builder, navigate to the name of the Front End pool you need to change.
2. Right-click the pool, and then click **Edit Properties**.
3. In the **Associations** section, under **Associate Edge Pool (for media components)**, use the drop down box to select the Edge pool you want to associate this Front End pool with.
4. Click **OK**.

Concepts

Edge Server High Availability and Disaster Recovery

1.7.18.9 Restoring Conference Contents Using the Backup Service

Restoring Conference Contents Using the Backup Service

Microsoft Lync Server 2013 > Operations > Managing Lync Server 2013 Disaster Recovery, High Availability, and Backup Service >

Topic Last Modified: *2012-11-01*

If the conference information stored in the file store of a Front End pool becomes unavailable. you must restore this information so that users homed on the pool retain their conference data. If the Front End pool which has lost conference data is paired with another Front End pool, you can use the Backup Service to restore the data.

You must also perform this task if an entire pool has failed and you have to fail over its users to a backup pool. When these users are failed back over to their original pool, you must use this procedure to copy their conference content back to their original pool as well.

Assume that Pool1 is paired with Pool2, and the conference data in Pool1 is lost. You can use the following cmdlet to invoke the Backup Service to restore the contents:

```
Invoke-CsBackupServiceSync -PoolFqdn <Pool2 FQDN> -BackupModule ConfServices.Data
```

Restoring the conference contents may take some time, depending on their size. You can use the following cmdlet to check the process status:

```
Get-CsBackupServiceStatus -PoolFqdn <Pool2 FQDN> -BackupModule ConfServices.DataC
```

The process is done when this cmdlet returns a value of Steady State for the data conference module.

1.7.19 Backing Up and Restoring Lync Server 2013

Backing Up and Restoring Lync Server 2013

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2013-02-21*

In this section, you'll find the best practices for backing up your Lync Server 2013 data, and for restoring it if you have a failure. These best practices apply to the following situations:

- An entire Lync Server pool of any type (Front End Server, Edge Server, Mediation Server, Persistent Chat Server, or Director), or an individual server in one of these pools.
- The Central Management Server
- A Standard Edition server
- An Enterprise Edition Back End Server
- A File Store
- An Archiving database, Monitoring database, or Persistent Chat database

This section does not include information about restoring an entire site or for developing a standby site. For details about developing a disaster recovery solution with paired Front End pools, see Planning for High Availability and Disaster Recovery. This is the recommended method for planning for disaster recovery.

If you have deployed paired Front End pools, if one of these pools fails and becomes unrecoverable, you can restore this pool with a new fully qualified domain name (FQDN) from its paired pool. For details on the steps to perform this recovery, see Failing Over a Pool. Additionally, if you later want to recreate a failed and unrecoverable pool that was part of a Front End pair, you can use the steps in Performing an ABC Front End Pool Failover.

The methodology described in this document involves special considerations during the planning phase. For details, see Establishing a Backup and Restoration Plan.

- Preparing for Lync Server Backup and Restoration
- Backing Up Data and Settings
- Restoring Data and Settings
- Backup and Restoration Worksheets

1.7.19.1 Preparing for Lync Server Backup and Restoration

Preparing for Lync Server Backup and Restoration

Microsoft Lync Server 2013 > Operations > Backing Up and Restoring Lync Server 2013 >

Topic Last Modified: *2013-02-17*

The following topics describe the settings, configuration, and other data that you need to back up, in order to be able to restore servers and databases in the event of a failure or outage.

- Backup and Restoration Requirements: Data
- Backup and Restoration Requirements: Tools and Permissions
- Backup and Restoration Process Overview
- Developing a Backup and Restoration Strategy and Plan
- Best Practices for Backup and Restoration

1.7.19.1.1 Backup and Restoration Requirements: Data

Backup and Restoration Requirements: Data

Operations > Backing Up and Restoring Lync Server 2013 > Preparing for Lync Server Backup and Restoration >

Topic Last Modified: *2013-02-21*

Lync Server uses settings and configuration information that are stored in databases, and data that is stored in databases and file stores. This topic describes the data that you need to back up to be able to restore service if your organization experiences a failure or outage, and also identifies the data and components used by Lync Server that you need to back up separately.

Settings and Configuration Requirements

This topic includes procedures for backing up and restoring the settings and configuration information that is required for recovery of Lync Server service. The configuration information is located in the Central Management store or on another back-end database or on Standard Edition server.

The following table identifies the settings and configuration information that you need to back up and restore.

Settings and Configuration Data

Type of data	Where stored	Description / When to back up
Topology configuration information	Central Management store (database: Xds.mdf)	Topology, policy, and configuration settings.

		Back up with your regular backups and after you use Lync Server Control Panel or cmdlets to modify your configuration or policies.
Location information	Central Management store (database: Lis.mdf)	Enterprise Voice Enhanced 9-1-1 (E9-1-1) configuration information. This information is generally static. Back up with your regular backups.
Response Group configuration information	Back End Server or Standard Edition server (database: RgsConfig.mdf)	Response Group agent groups, queues, and workflows. Back up with your regular backups and after you add or change agent groups, queues, or workflows.

Data Requirements

Here is a list of the Lync Server data that you need to back up so that you can restore Lync Server service in the event of a failure.

Note that some types of data are not required for recovery. This topic does not contain procedures for backing up these types of data, which include the following:

- Transient user data, such as endpoints and subscriptions, active conferencing servers, and transient conferencing states (database: RtcDyn.mdf)
- Address Book data (databases: Rtcab.mdf and Rtcab1.mdf). The Address Book database is regenerated automatically from Active Directory Domain Services (AD DS).
- Dynamic information for the Call Park application (database: CpsDyn.mdf)
- Transient Response Group data, such as agent sign-in state and call waiting information (database: RgsDyn.mdf)
- The compliance database for Persistent Chat (database: MgcComp.mdf). If you have Persistent Chat compliance enabled, the information in the Persistent Chat Compliance database is transient as long as you have an adapter configured to read information from the database and convert it to an alternate format. Hence the compliance database for Persistent Chat is considered transient.
  Lync Server 2013 Persistent Chat Server ships with an XML adapter. You can also install custom adapters that take this data and move it to other sources, such as Exchange Hosted Archives.

The following table identifies the data that you need to back up and restore.

Data Stored in Databases

Type of data	**Where stored**	**Description / When to back up**
Persistent user data	Back End Server or Standard Edition server (database: RTCXDS.mdf)	User rights, user Contacts lists, server or pool data, scheduled conferences, and

		so on. This user data does not include content uploaded to a conference. Back up with your regular backups. This information is dynamic, but the loss of updates is not catastrophic to Lync Server if you need to restore to your last regular backup. If Contacts lists are critical to your organization, you can back up this data more frequently.
Archiving data	Archiving database (database: LcsLog.mdf) This data may be stored on Exchange 2013, if you have enabled the Microsoft Exchange integration option. Otherwise, this data is kept in a Lync Server Archiving database, which may be collocated with another Lync Server database, or stand-alone on a separate database server.	Instant messaging (IM) and meeting content. This data is not critical to Lync Server, but it may be critical to your organization for regulatory purposes. Determine your back up schedule accordingly. Lync Server supports only the Simple Recovery model for Archiving databases. With the Simple Recovery model, databases are recovered to the point of last full backup, which means that you cannot restore a database to the point of failure or to a specific point in time.
Monitoring data	Monitoring databases (LcsCDR.mdf and QoeMetrics.mdf) These databases may be collocated with another Lync Server database, or stand-alone on a separate database server.	Call detail records (LcsCDR.mdf) and Quality of Experience (QoE) metrics (QoeMetrics.mdf). Call detail records are dynamic and may be critical to your business. Determine your back up schedule by considering whether you need these records for regulatory reasons. Quality of experience information is dynamic. Loss of QoE data is not critical for the operation of Lync Server, but it may be critical to your business. Determine your back up schedule based on how critical this information is to your organization.

		Lync Server supports only the Simple Recovery model for Monitoring databases. With the Simple Recovery model, databases are recovered to the point of last full backup, which means that you cannot restore a database to the point of failure or to a specific point in time.
Persistent Chat data	Persistent Chat database (mgd.mdf). This database may be collocated with another Lync Server database, or stand-alone on a separate database server.	Persistent Chat Data is actual chat content being posted in chat rooms. This data is often business critical. You can choose to use SQL Server backup, or export the database by using the **Export-CsPersistentChatData** cmdlet that is provided in Lync Server. For recovery of the data, you can import and restore the database to the point of the last full backup, which means you cannot restore the database to the point of failure.

File Store Data Requirements

In an Enterprise Edition deployment, the Lync Server file store is typically located on a file server. In a Standard Edition deployment, the Lync Server file store is located by default on the Standard Edition server. Typically, there is one Lync Server file store that is shared for a site. The Persistent Chat file store uses the same file share as the Lync Server file store.

File store locations are identified as \\server\share name. To find the specific locations of your file stores, open Topology Builder and look in the **File stores** node.

The following table identifies the file stores you need to back up and restore.

File Stores

Type of data	Where stored	Description / when to back up
Lync Server file store	Typically on a file server, file cluster, or a Standard Edition server	Meeting content, meeting content metadata, meeting compliance logs, application data files, update files for device updates, audio files for Response Group, Call Park, and Announcement applications, and files posted into Persistent Chat rooms.

		Back up with your regular backups.

Additional Backup Requirements

To help ensure your ability to restore Lync Server services in the event of a failure, you must back up some necessary components that are not part of Lync Server itself. The following components are not backed up or restored as part of the Lync Server backup and restoration process described in this document:

- **Active Directory Domain Services (AD DS)** You need to back up AD DS by using Active Directory tools at the same time that you back up Lync Server. It is important to keep AD DS synchronized with Lync Server, to avoid problems that can occur when Lync Server expects contact objects that do not match those in AD DS. AD DS stores the following settings which are used by Lync Server:
  - User SIP URI and other user settings.
  - Contact objects for applications such as Response Group and Conferencing Attendant.
  - A pointer to the Central Management Store.
  - Kerberos Authentication Account (an optional computer object) and Lync Server security groups.

  For details about backing up and restoring AD DS in Windows Server 2008, see "AD DS Backup and Recovery Step-by-Step Guide" at http://go.microsoft.com/fwlink/p/?linkId=209105.
- **Certification authority and certificates** Use your organization's policy for backing up your certification authority (CA) and certificates. If you use exportable private keys, you can back up the certificate and the private key, and then export them if you use the procedures in this document to restore Lync Server. If you use an internal CA, you can re-enroll if you need to restore Lync Server. It is important that you retain the private key in a secure location where it will be available if a computer fails.
- **System Center Operations Manager** If you use Microsoft System Center Operations Manager (formerly Microsoft Operations Manager) to monitor your Lync Server deployment, you can optionally back up the data it creates while it is monitoring Lync Server. Use your standard SQL Server backup process to back up System Center Operations Manager files. These files are not restored during recovery.
- **Public switched telephone network (PSTN) gateway configuration** If you use Enterprise Voice or Survivable Branch Appliances, you need to back up the PSTN gateway configuration. See your vendor for details about backing up and restoring PSTN gateway configurations.
- **Coexisting versions of Lync Server or Office Communications Server** If your Lync Server 2013 deployment coexists with Lync Server 2010 or an earlier version of Office Communications Server, you can’t use the procedures in this document for backing up or restoring the earlier version. Instead, you must use the backup and restoration procedures documented specifically for your earlier version. For details about backing up and restoring Lync Server 2010, see http://go.microsoft.com/fwlink/p/?linkId=265417 . For details about backing up and restoring Microsoft Office Communications Server 2007 R2, see http://go.microsoft.com/fwlink/p/?linkId=168162.
- **Infrastructure information** You need to back up information about your infrastructure, such as your firewall configuration, load balancing configuration, Internet Information Services (IIS) configuration, Domain Name System (DNS) records and IP addresses, and Dynamic Host Configuraton Protocol (DHCP) configuration. For details about backing up these components, check with their respective vendors.
- **Microsoft Exchange and Exchange Unified Messaging (UM)** Backup and

restore Microsoft Exchange and Exchange UM as described in the Microsoft Exchange documentation. For details about backing up and restoring Exchange Server 2013, see http://go.microsoft.com/fwlink/?LinkId=285384. For details about backing up and restoring Exchange Server 2010, see http://go.microsoft.com/fwlink/p/?linkId=209179.
Note that Lync Server 2013 introduces the ability to have user contact lists, high definition user photos, and archiving data stored in Exchange 2013. See the following list to see how to back up these types of data:

- **High definition photos** are backed up as part of the Exchange Server backup.
- **Unified contact store** is introduced in Lync Server 2013. Unified contact store enables users to keep all their contact information in Exchange 2013.

  You should make sure that backups are up-to-date for users in terms of whether their user contacts are stored in the unified contact store or on the Lync Back End Server. The following scenarios illustrate where migrating user contacts to the unified contact store can cause issues for the backup and restore process.
  Scenario 1: User contacts are migrated to the unified contact store, and a restore is performed from a Lync Server backup taken prior to the migration of user contacts. In this scenario, the user will have a state of outdated contacts for up to one day until Lync Server Migration Task begins migrating user contacts to Exchange. (Note that because the user contacts were previously migrated to the unified contact store, the Exchange contact information will be used). No administrator intervention is needed in this scenario.
  Scenario 2: User contacts were previously stored in the unified contact store, but then rolled back. A restore is performed from a Lync Server backup taken when the user contacts were stored in the unified contact store. In this scenario, an error message of `Error: Incorrect Exchange Version` in the client or Lyss server logs may indicate this as an issue. The user will be able to access their contact list in Lync 2013 directly from Exchange, but client's state will not match the Lync Server state. To fix this, an administrator will need to run the **Invoke-CsUCSRollback** cmdlets for the affected users.
- **Archiving Data** can be stored in Exchange 2013. This data is not critical to Lync Server, but it may be critical to your organization for regulatory purposes. If archiving data is stored in Exchange and is critical to your organization, then follow Exchange backup and restore procedures. Note that archiving data stored in Exchange cannot be moved back to Lync Server. Additionally, there is no way to move data already stored in the Lync archiving database to Exchange.

1.7.19.1.2 Backup and Restoration Requirements: Tools and Permissions

Backup and Restoration Requirements: Tools and Permissions

Operations > Backing Up and Restoring Lync Server 2013 > Preparing for Lync Server Backup and Restoration >

Topic Last Modified: *2013-02-17*

This topic identifies the tools that you can use to back up and restore Lync Server 2013, the permissions that you need, and whether you can run commands remotely or locally. Specifically, this topic focuses on tools that are provided with Lync Server for backup and restoration.

Backups

To back up Lync Server, use the tools identified in the following table. All the commands that you need to back up Lync Server can be scripted and can be run remotely.

Tools for Backing Up Lync Server

To back up this:	**Use this tool or cmdlet:**
Topology configuration data (Xds.mdf)	Export-CsConfiguration
Location information service (E9-1-1) data (Lis.mdf)	Export-CsLisConfiguration
Response Group configuration data (RgsConfig.mdf)	Export-CsRgsConfiguration
Persistent user data (Rtcxds.mdf database) Conference IDs	Export-CsUserData
• Archiving database (LcsLog.mdf) • Monitoring call detail record database (LcsCDR.mdf) • Monitoring QoE database (QoEMetrics.mdf)	SQL Server database tool, such as SQL Server Management Studio
Persistent Chat database (Mgc.mdf)	SQL Server backup procedures or Export-CsPersistentChatData. Export-CsPersistentChatData exports Persistent Chat data as a file.
All file stores: Lync Server file store, Archiving file store **Note:** Files named **Meeting.Active** should not be backed up. These files are in use and locked while a meeting takes place.	Standard file system management tool, such as Robocopy.

Restoration

To restore Lync Server, use the tools in the following table. All the commands that you need to restore Lync Server can be scripted. Some can be run remotely, but others need to be run locally, as specified in the following table.

Tools for Restoring Lync Server

To do this:	**Use this tool or cmdlet:**
Build a new or clean computer	• Windows operating system installation software • SQL Server installation software • Certificates Microsoft Management Console (MMC) snap-in, if restoring certificates with an exportable private key
Restore file store data	Standard file system management tool, such as Robocopy

Recreate empty databases and set permissions for the following: • Central Management store • Back End Server • Monitoring database • Archiving database	Install-CsDatabase
Restore the Active Directory Domain Services (AD DS) pointer to the Central Management store **Note:** If you lose the service connection point at any time, you can rerun this cmdlet.	Set-CsConfigurationStoreLocation
Import the topology, policies, and configuration settings to the Central Management store (Xds.mdf)	Import-CsConfiguration
Publish and enable the topology	Topology Builder -or- Publish-CsTopology and Enable-CsTopology
Enable the last published topology	Enable-CsTopology
Reinstall Lync Server components	Lync Server Setup **Note:** Located in the Lync Server installation folder or media at \setup\amd64\Setup.exe.
Restore location information (E9-1-1) data (Lis.mdf)	Import-CsLisConfiguration
Restore persistent user data (Rtcxds.mdf)	Import-CsUserData
Restore Response Group configuration data (RgsConfig.mdf)	Import-CsRgsConfiguration **Note:** If the configuration is being restored in a newly deployed pool that has no Response Group data in the database, then you should use the –OverwriteOwner option. Use this option even if the data being restored is in a pool with the same fully qualified domain name (FQDN). Otherwise, the import will not succeed, due to the contact objects to the Response Groups already existing in Active Directory.
Restore the following databases: • Archiving database (LcsLog.mdf) • Monitoring databases: call detail record database (LcsCDR.mdf) and QoE database (QoEMetrics.mdf)	SQL Server database management tools
Persistent Chat database (Mgs.mdf)	SQL Server restore procedures or Import-CsPersistentChatData. You can use Import-CsPersistentChatData with a file created by Export-CsPersistentChatData, and the data will be imported into the Persistent Chat

	database.

Required Permissions

Users must be a member of the **RTCUniversalServerAdmins** group to perform all the commands described in this topic. Most backup and restore commands do not support role-based access control (RBAC). Two exceptions are the Persistent Chat cmdlets Export-CsPersistentChatData and Import-CsPersistentChatData, which must be run by a user who is a member of the CsPersistentChatAdministrator group. To run Lync Server Deployment Wizard, a user must also be a member of the Local Adminstrators group.

1.7.19.1.3 Backup and Restoration Process Overview

Backup and Restoration Process Overview

Operations > Backing Up and Restoring Lync Server 2013 > Preparing for Lync Server Backup and Restoration >

Topic Last Modified: *2013-02-21*

This section provides an overview of how the backup and restoration process works for Lync Server 2013. You use the same process for all Standard Edition servers and Enterprise Edition servers, regardless of their location.

In general, the backup process works as follows:

- You create a backup location as a shared folder on a stand-alone computer that is not part of any pool. The location of the backup is referenced in **$Backup**.
- On a regular, scheduled basis, you back up all the Lync Server databases and all the file stores that are described in Backup and Restoration Requirements: Data by following the procedures described in Backing Up Lync Server The Central Management store includes all the server settings and configurations.
- Each time you run a subsequent backup, you create a new shared folder and change the path that **$Backup** references.

In general, the restoration process works as follows:

- When a failure or outage occurs, you restore the data in the location referenced by **$Backup** to new or clean computers.

Important:
This restoration process does not restore data onto an existing server state. That is, this process requires that the server is clean or new.

- To enable your user and conference information to be recoverable to the point of failure, you can implement a disaster recovery topology with paired Front End pools, as described in Planning for High Availability and Disaster Recovery. Aside from this option, Lync Server supports only the Simple Recovery model for its databases. With the Simple Recovery model, databases are recovered to the point of last full backup, which means that you cannot restore a database to the point of failure or to a specific point in time. For many organizations the Simple Recovery model is optimal, because the Lync Server back-end database (RTCXDS.mdf) is actually smaller than the transaction log files, and is significantly smaller than those of typical line-of-business database applications.
- All Domain Name System (DNS) configuration, Dynamic Host Configuration Protocol (DHCP) configuration, domain names, computer fully qualified domain names (FQDNs), file store paths, and so on must be the same at the time of

restoration that they were at the time of back up.

If a server running Lync Server fails, recovery includes the following steps:

- Install the operating system on a new or clean computer with the same FQDN as the failed computer.
- Reinstall certificates.
- If the server hosted a database, install Microsoft SQL Server 2012 or Microsoft SQL Server 2008 R2.
- In general, if the server hosted a database, run Topology Builder to create and install the database and set up access control lists (ACLs).
- In general, if the server hosted a server role, run step 1 through step 4 of the Lync Server Deployment Wizard to install the local configuration files, install the server role components, assign certificates, and start the services.

  Note:

  If the server hosted a database collocated with the server role, running step 2 of the Lync Server Deployment Wizard recreates the database.
- If the server hosted a database, restore the backed up data.

1.7.19.1.4 Developing a Backup and Restoration Strategy and Plan

Developing a Backup and Restoration Strategy and Plan

Operations > Backing Up and Restoring Lync Server 2013 > Preparing for Lync Server Backup and Restoration >

Topic Last Modified: *2013-02-17*

The effectiveness of your Lync Server backup and restoration operations depends on your backup and restoration strategy and plan. You should establish a strategy for backing up and restoring Lync Server that fits with your organization's overall strategy, and a comprehensive, concise plan for backing up data and settings, and, in the event of an outage, a plan for restoring service.

For the most robust disaster recovery of a Front End Pool, use the paired-pool disaster recovery topology introduced in Lync Server 2013. For more information, see Planning for High Availability and Disaster Recovery.

- Establishing a Backup and Restoration Strategy
- Establishing a Backup and Restoration Plan
- Setting Up a Backup Location

1.7.19.1.4.1 Establishing a Backup and Restoration Strategy

Establishing a Backup and Restoration Strategy

Backing Up and Restoring Lync Server 2013 > Preparing for Lync Server Backup and Restoration > Developing a Backup and Restoration Strategy and Plan >

Topic Last Modified: *2013-02-17*

Before you can develop a backup and restoration plan for Lync Server, you need to develop a strategy that fits with your organization's goals. To develop an effective backup and restoration strategy, you will need to:

- Establish business priorities.
- Identify backup and restoration requirements.

Establishing Business Priorities

Evaluate the business priorities of your organization. Typically, the primary business priorities that affect your backup and restoration strategy are the following:

- Business continuity requirements
- Data completeness
- Data criticality
- Portability requirements
- Cost constraints

Business needs such as these help to determine the service level agreements (SLAs) that you develop with your customers. Service level agreements greatly influence your backup and recovery strategy.

Identifying Backup and Restoration Requirements

Your business priorities and service level agreements act in determining your organizations' requirements for backing up and restoring Lync Server. Identify and document your requirements for the following:

- **Frequency of backups** Keep in mind that, except for Front End pools in paired relationships as described in Planning for High Availability and Disaster Recovery, Lync Server supports only the Simple Recovery model, which means that you restore to the last full backup. Plan thoroughly for how often you need to take a full backup. For details about best practices for backup frequency, see Best Practices for Backup and Restoration.
- **Backup and restoration tools** Include who is to use the tools, and on which computers. For details about the tools discussed in this topic and necessary permissions, see Backup and Restoration Requirements: Tools and Permissions.
- **Backup location** Identify whether the backups are kept locally or remotely, taking security and accessibility into consideration. Specify the media to be used for the backups.
- **Hardware and software requirements** Identify and document your specific hardware and software requirements, including the hardware for backup storage and restoration of specific components and any software and network connectivity required to support backup and restoration. As you develop your hardware and software requirements, keep in mind the various restoration scenarios that follow.
- **Restoration scenarios** Here are the restoration processes for the following scenarios:
  - A Lync Server pool fails. This scenario requires rebuilding each server in the pool.
  - A Standard Edition server fails. This scenario requires rebuilding the server on a new or clean computer and restoring databases.
  - Loss of the Central Management store. At a minimum, this scenario requires restoring and publishing the Central Management store.
  - Loss of a Back End Server when the Central Management store is still functioning normally. This scenario requires rebuilding the server on a new or clean computer and restoring databases.
  - A server that is a member of a Lync Server pool fails. This scenario requires rebuilding the server on a new or clean computer.
  - A File Store fails. This scenario requires restoring the file server or file cluster.
  - An Archiving, Monitoring, or Persistent Chat database fails. This scenario requires recreating the databases, and, if the data is critical to your

organization, restoring the data. Archiving, Monitoring, and Persistent Chat data is not required to get Lync Server back up and running.

1.7.19.1.4.2 Establishing a Backup and Restoration Plan

Establishing a Backup and Restoration Plan

Backing Up and Restoring Lync Server 2013 > Preparing for Lync Server Backup and Restoration > Developing a Backup and Restoration Strategy and Plan >

Topic Last Modified: *2013-02-17*

Creating a backup and restoration plan involves the following steps:

- Developing the plan.
- Implementing the plan.
- Maintaining the plan.

Developing a Backup and Restoration Plan

After you develop your backup and restoration strategy for Lync Server, use it to document a detailed backup and restoration plan. Your plan should clearly convey the priorities and requirements for backing up data and settings. You can use the information in Establishing a Backup and Restoration Strategy and the worksheets in Backup and Restoration Worksheets to facilitate the documentation of your strategy. Your plan should also contain criteria for deciding when and how to restore service.

As you develop your plan, you need to consider, and account for, the following:

- How you will recover servers on new hardware.
- How you will recover services that require action on the part of multiple business areas or departments.
- How you can acquire spare servers quickly.
- The time it takes to recover by using your strategy. Consider your organization’s requirements for recovery time objective (RTO).

Modify the backup and restoration procedures in this topic, adding and deleting procedures as appropriate, to reflect the servers and components in your deployment. You can also add appropriate details, such as the backup schedule, to the appropriate procedures to make sure that the information is not overlooked.

Note:
It is good practice to create scripts for as many steps as possible, to help ensure the quality and reproducibility of procedures.

In your plan, specify who is responsible for reviewing the plan, who is responsible for testing and validating any new procedures or tools, and who must approve any changes to the plan and related procedures.

To make sure that your backup and restoration plan fully meets all established goals and priorities, get the approval of the appropriate business decision makers and technical decision makers in your organization before you implement the plan.

Implementing the Backup and Restoration Plan

Implementing a backup and restoration plan requires the following steps:

- Testing and validating the plan.

- Communicating the plan.
- Validating backup and restoration operations.

Testing and Validating the Plan

The procedures described here have been tested and validated in a lab environment. To make sure that these or any other procedures work in your environment, you should test and validate each procedure you intend to implement. Complete the testing and the validation before you submit your plan for final approval.

Communicating the Plan

Your backup and restoration plan should clearly describe who implements procedures and step-by-step instructions for carrying out the procedures. You should make sure that everyone responsible for any aspect of backup and restoration understands the plan, how it is to be implemented, and what their role is. This includes all implementation requirements for the following:

- Pool and server backup.
- Restoration of service.

Pool and server backup

The backup and restoration plan should include all information required to complete backup procedures on an ongoing basis. The primary information to be communicated to responsible team members includes the following:

- Team or person (specified as an individual or role) responsible for backing up each server.
- Specific schedules for backing up each server.
- Backup locations for each type of data (settings, database, and file shares).
- Backup procedures to be used, including the tools required to complete each procedure.
- Information required to complete backups, as covered in Backup and Restoration Worksheets.
- Validation methods to be used to help ensure that data and settings are appropriately backed up and available for restoration, which can include periodic audits and test restorations.

Restoration of service

The backup and restoration plan should include all information required to restore service, in case one or more servers experience a loss that makes service unavailable. The primary information to be communicated to responsible team members includes the following:

- Team or person (specified as an individual or a role) that is responsible for determining when restoration of service is required and the procedures to be used to restore service, and also the team or person responsible for implementing procedures for each restoration scenario.
- Criteria for determining which restoration procedures are most appropriate for a specific situation.
- Time estimates for restoration of service and recovery time objective (RTO) in each restoration scenario.
- Restoration procedures to be used, including the tools required to complete each procedure.
- Information required to restore data and settings. Worksheets are provided in Backup and Restoration Worksheets.

Validating Backup and Restoration Operations

After completing initial backup efforts in your production environment and at specified intervals (as covered in your backup and restoration plan), you should verify the following:

- Backups are occurring as required.

- Backed-up data and settings are accessible.
- Restoration procedures can be performed within the recovery time objective (RTO) times specified in the backup and restoration plan, and the results meet all business requirements.
- Backup worksheets have been completed and verified, and they are stored in a secure location. These worksheets are provided in Backup and Restoration Worksheets.
- Restoration procedures have been tested and verified to work as expected, as specified in your backup and restoration plan.

Maintaining the Backup and Restoration Plan

A Lync Server topology is a dynamic environment that changes with your organization. Reassess your backup and restoration plan as your organization changes, and review it periodically to make sure that it continues to meet the needs of your business.

1.7.19.1.4.3 Setting Up a Backup Location

Setting Up a Backup Location

Backing Up and Restoring Lync Server 2013 > Preparing for Lync Server Backup and Restoration > Developing a Backup and Restoration Strategy and Plan >

Topic Last Modified: *2013-02-17*

Before you take your first backup of Lync Server, set up the hardware and software that you need in order to store and maintain the backups. You need to obtain access to the media and content, as appropriate, and provide network connectivity between each server to be backed up and the backup media. The media and location that you use should be defined in your backup and restoration strategy. The location that you use for regular backups can be local or remote, but it must be secure, and it must be accessible for both backup and restoration. We recommend using a remote location to protect against a catastrophic event at your primary site.

After you set up and test the individual components, verify accessibility to the backups from each server.

1.7.19.1.5 Best Practices for Backup and Restoration

Best Practices for Backup and Restoration

Operations > Backing Up and Restoring Lync Server 2013 > Preparing for Lync Server Backup and Restoration >

Topic Last Modified: *2013-02-21*

This section includes two types of best practices:

- Best practices for backup and restoration.
- Best practices for minimizing the impact of a disaster.

Best Practices for Backup and Restoration

To facilitate your backup and restoration process, apply the following best practices when you back up or restore your data:

- Perform regular backups at appropriate intervals. The simplest and most commonly used backup type and rotation schedule is a full, nightly backup of the entire SQL Server database. Then, if restoration is necessary, the restoration process requires only one backup, and no more than a day's data should be lost.
- If you use cmdlets or the Lync Server Control Panel to make configuration changes, use the **Export-CsConfiguration** cmdlet to take a snapshot backup of the topology configuration file (Xds.mdf) after you make the changes, so that you won't lose the changes if you need to restore your databases. Note that this configuration is backed up in XML format and compressed as a ZIP file.
- Make sure that the shared folder you plan to use for backing up Lync Server has sufficient disk space to hold all the backed up data.
- Schedule backups when Lync Server usage is typically low, to improve server performance and user experience.
- Make sure that the location where you back up data is secure (we recommend a remote location).
- Keep the backup files where they will be available, in case you need to restore the data.
- Plan for and schedule periodic testing of the restoration processes that are supported by your organization.
- Validate your backup and restoration processes in advance to make sure that they work as expected.

Best Practices for Minimizing the Impact of a Disaster

The best strategy for dealing with disastrous service interruptions (caused by unmanageable events such as power outages or sudden hardware failures) is to assume they will happen, and to plan accordingly.

If Lync services, with a minimum of disruption and outage, are business-critical for your organization, you should consider implementing paired pools of Front End Servers, as described in Planning for High Availability and Disaster Recovery. Then, if one of these pools has a disaster, an administrator can switch the users of that pool to be served by the other pool, with a minimum of downtime.

The disaster management plans that you develop as part of your backup and restoration strategy should include the following:

- Keeping your software media, and your software and firmware updates, readily available.
- Maintaining hardware and software records.
- Backing up your data regularly and monitoring the integrity of your backups.
- Training your staff in disaster recovery, documenting procedures, and implementing disaster recovery simulation drills.
- Keeping spare hardware available, or, if you have a service level agreement (SLA), contracting with hardware vendors and suppliers for prompt replacements.
- Separating the location of your transaction log files (.ldf files) and database files (.mdf files).

1.7.19.2 Backing Up Lync Server

Backing Up Lync Server

Microsoft Lync Server 2013 > Operations > Backing Up and Restoring Lync Server 2013 >

Topic Last Modified: *2013-02-17*

The procedures in this section describe how to back up Lync Server so that you can recover service in the event of an outage or failure.

You should develop a backup and recovery strategy and plan for your organization, as described in Developing a Backup and Restoration Strategy and Plan. This strategy and plan should include the specific procedures that you plan to use. Use the procedures included in the topics in this section, along with the worksheets in Backup and Restoration Worksheets, to document how you plan to back up your specific Lync Server deployment.

- Verifying Backup Prerequisites
- Backing Up Data and Settings

1.7.19.2.1 Verifying Backup Prerequisites

Verifying Backup Prerequisites

Operations > Backing Up and Restoring Lync Server 2013 > Backing Up Lync Server >

Topic Last Modified: *2013-02-17*

Before you begin backing up Lync Server, verify that you are prepared with the following:

- Backup tools. For details, see Backup and Restoration Requirements: Tools and Permissions.
- Permissions. For details, see Backup and Restoration Requirements: Tools and Permissions.
- Location for storing backups. For details, see Setting Up a Backup Location.
- Media for the backups. For details, see Setting Up a Backup Location.

1.7.19.2.2 Backing Up Data and Settings

Backing Up Data and Settings

Operations > Backing Up and Restoring Lync Server 2013 > Backing Up Lync Server >

Topic Last Modified: *2013-02-17*

The backup procedures described in the following topics apply to all Enterprise Edition servers and Standard Edition servers, regardless of their location.

- Backing up Core Data and Settings
- Backing Up Archiving and Monitoring Databases
- Backing Up Persistent Chat Databases
- Backing Up File Stores

1.7.19.2.2.1 Backing up Core Data and Settings

Backing up Core Data and Settings

Backing Up and Restoring Lync Server 2013 > Backing Up Lync Server > Backing Up Data and Settings >

Topic Last Modified: *2013-02-17*

The following procedures use Lync Server Management Shell cmdlets to create backup files for settings and data for core services. For details about the tools used in this section, including where they are located, see Backup and Restoration Requirements: Tools and Permissions. For details about backing up Archiving and Monitoring data, see Backing Up Archiving and Monitoring Databases.

Note:
The step in this section to back up the Central Management store includes the settings and configuration for Archiving and Monitoring.

You can run the cmdlets described in this section locally or remotely.

To back up core data and settings

1. From a user account that is a member of the RTCUniversalServerAdmins group, log on to any computer in your internal deployment.
2. To store the backups you create in the following steps, create a new shared folder and update the path referenced by **$Backup** to the new shared folder.
3. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
4. Back up the Central Management store configuration file. At the command line, type the following:

   ```
   Export-CsConfiguration -FileName <path and file name for backup>
   ```

   For example:

   ```
   Export-CsConfiguration -FileName "C:\Config.zip"
   ```

   Note:
   This step exports your Lync Server topology, policies, and configuration settings to a file. No other step is required to backup topology data.
5. Copy the backed-up Central Management store configuration file to $Backup\.
6. Back up Location Information service data. At the command line, type the following:

   ```
   Export-CsLisConfiguration -FileName <path and file name for backup>
   ```

   For example:

   ```
   Export-CsLisConfiguration -FileName "C:\E911Config.zip"
   ```
7. Copy the backed-up Location Information service configuration file to $Backup \.
8. Back up user data on every back-end database of a Front End pool and every Standard Edition server. At the command line, type the following:

   ```
   Export -CsUserData -PoolFQDN <Fqdn> =FileName <String>
   ```

   For example:

   ```
   Export -CsUserData -PoolFQDN "atl-cs-001.litwareinc.com" =FileName "C:
   ```
9. Copy the backed up user file to $Backup\.
10. On every pool that runs the Response Group application, back up the Response Group configuration. Do the following:

    10.a. At the command line, type:

    ```
    Export-CsRgsConfiguration -Source "service:ApplicationServe
    ```

    For example:

    ```
    Export-CsRgsConfiguration -Source ApplicationServer:pool01.
    ```
11. Copy the backed up Response Group configuration file to $Backup\.

1.7.19.2.2.2 Backing Up Archiving and Monitoring Databases

Backing Up Archiving and Monitoring Databases

Backing Up and Restoring Lync Server 2013 > Backing Up Lync Server > Backing Up Data and Settings >

Topic Last Modified: *2013-02-17*

If you deployed Archiving or Monitoring, you need to back up these databases according to your organization's SQL Server backup policy.

Note:
The settings for Archiving and Monitoring are backed up when you back up the Central Management store. For details, see Backing up Core Data and Settings.

For Archiving and Monitoring, you can use a SQL Server tool such as SQL Server Management Studio to perform a manual backup, or you can use SQL Server management tools to schedule regular, automatic backups.

1.7.19.2.2.3 Backing Up Persistent Chat Databases

Backing Up Persistent Chat Databases

Backing Up and Restoring Lync Server 2013 > Backing Up Lync Server > Backing Up Data and Settings >

Topic Last Modified: *2013-02-17*

Persistent Chat room content is stored in the Persistent Chat database (Mgc.mdf). This is business-critical data that should be backed up regularly. In addition to the chat room content, the Persistent Chat database also stores information about the principals (such as users and user groups), and the roles and access that they have to chat rooms and chat room.

There are two ways of backing up Persistent Chat data.

- SQL Server Backup
- The `Export-CsPersistentChatData` cmdlet, which exports Persistent Chat data as a file

Data that is created by using SQL Server backup requires significantly more disk space—possibly 20 times more—than that created by `Export-CsPersistentChatData`, but SQL Server backup is more likely to be a procedure that administrators are familiar with.

1.7.19.2.2.4 Backing Up File Stores

Backing Up File Stores

Backing Up and Restoring Lync Server 2013 > Backing Up Lync Server > Backing Up Data and Settings >

Topic Last Modified: *2013-02-17*

Backing up the Lync Server File Stores includes all the files and folders used by Lync Server components.

⊟To back up File Stores

1. To find the specific locations of your Lync Server File Stores, open Topology Builder and look in the **File stores** node.
2. Use Robocopy or another file system management tool to copy each File Store to $Backup\filestore.

1.7.19.3 Restoring Data and Settings

Restoring Data and Settings

Microsoft Lync Server 2013 > Operations > Backing Up and Restoring Lync Server 2013 >

Topic Last Modified: *2013-02-17*

If you have implemented a disaster recovery topology with paired pools, and one of those Front End pools has gone down and you need to quickly restore service to your users, see Failing Over a Pool. Otherwise, use the information in the following topics, along with the worksheets in Backup and Restoration Worksheets, to restore Lync Server after a failure or outage.

> **Note:**
> To reduce downtime and potential data loss, perform the restoration procedures described in this document only if troubleshooting procedures are not effective in identifying and correcting the problem. During troubleshooting, try to minimize the impact on other servers and components as you shut down and restart servers.

- Preparing to Restore Lync Server
- Restoring a Standard Edition Server
- Restoring the Server Hosting the Central Management Store
- Restoring an Enterprise Edition Back End Server
- Restoring an Enterprise Edition Member Server
- Restoring a Lync Server Pool
- Performing an ABC Front End Pool Failover
- Restoring a File Store
- Restoring Monitoring or Archiving Data
- Restoring Persistent Chat Data

1.7.19.3.1 Preparing to Restore Lync Server

Preparing to Restore Lync Server

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-21*

Before you begin restoring servers and databases after a failure, you need to determine the following:

- What needs to be restored.
- The hardware, software, data, and tools you need for restoration.

Determining What to Restore

This topic describes how to restore Lync Server outages that occur at the server, pool, or Central Management store level. If the Central Management store fails, your Lync Server deployment continues to function, but you cannot make any configuration changes. If a Back End Server or Standard Edition server fails, the user pool stops functioning. If any other server fails, the magnitude of the failure depends on the server role the server is running and whether the server hosts one or more databases.

What to Restore

If this failed	See this section:
Standard Edition server	Restoring a Standard Edition Server

Central Management store	Restoring the Server Hosting the Central Management Store
Enterprise Edition Back End	Restoring an Enterprise Edition Back End Server
Enterprise Edition Mirrored Back End Primary Server	Restoring a Mirrored Enterprise Edition Back End Server - Primary
Enterprise Edition Mirrored Back End Secondary Server	Restoring a Mirrored Enterprise Edition Back End Server - Mirror
Any Enterprise Edition server running a server role, such as a Front End Server, Edge Server, Director, Mediation Server,.or Persistent Chat Server.	Restoring an Enterprise Edition Member Server
An entire Lync Server pool	Restoring a Lync Server Pool
Enterprise Edition File Store	Restoring a File Store
A standalone Monitoring database or Archiving database	Restoring Monitoring or Archiving Data
A stand-alone Persistent Chat database	Restoring Persistent Chat Data

Gathering Hardware, Software, and Tools

When you restore a server, you need to start with a new or clean computer. Additionally, you must have the following hardware and software available:

- A clean or new server with the same fully qualified domain name (FQDN) as the server that failed.

  > **Important:**
  >
  > When you install the operating system, make sure that you do not delete the computer account in Active Directory Domain Services (AD DS), and verify that the group permissions for the account are retained.

- Installation software for the operating system. To install the operating system, use the server deployment procedures and configurations established by your organization. You should have these procedures and configuration requirements available when you restore service.
- Installation software for SQL Server 2012 or SQL Server 2008 R2. To install a database server, use the appropriate version of SQL Server and the database server deployment procedures and configurations established by your organization. You should have these procedures and configuration requirements available when you restore service.

  > **Note:**
  >
  > The Lync Server Deployment Wizard automatically installs SQL Server 2012 Express on each Standard Edition server and on any other Lync Server server when a local configuration store is installed, unless you have preinstalled SQL Server 2012 or SQL Server 2008 R2 on the server.

- Software for taking system images.

  > **Tip:**
  >
  > We recommend that you take an image copy of the system after you install the operating system and SQL Server, and before you start restoration, so that you can use this image as a rollback point in case something goes wrong during restoration.

- Lync Server 2013 installation software. The Lync Server Deployment Wizard is located in the Lync Server installation folder or media at \setup\amd64 \Setup.exe.

During restoration, you use the following tools:

- Lync Server Management Shell cmdlets
- Import-CsUserData
- Tools for restoring Windows folders
- Topology Builder
- SQL Server database utilities, such as SQL Server Management Studio

Preparing to Restore a Server

Before you restore the server, you must perform the following steps:

1. Install the operating system.
2. If the server is a Back End Server, install SQL Server 2012 or SQL Server 2008 R2.
3. Restore or reenroll your certificates. For details about certificates, see "Additional Backup Requirements" in Backup and Restoration Requirements: Data.
4. Take an image of the system before starting restoration to use as a rollback point, in case something goes wrong during restoration.

Note:

The Lync Server Deployment Wizard and cmdlets described in the procedures in this topic, and related topics, set all required access control lists (ACLs).

Verify that the hardware and the software that you need for the components that you plan to restore are available before you start restoration. After you install the operating system and SQL Server, most of the steps in the following restoration procedures can be run remotely. The exceptions are noted in the procedures.

You should also have your organization's backup and restoration plan and the information from your last backup, such as the information in the worksheets in this document (for details, see Backup and Restoration Worksheets), available before you begin restoration.

1.7.19.3.2 Restoring a Standard Edition Server

Restoring a Standard Edition Server

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-21*

If a Standard Edition server that does not host the Central Management store fails, follow the procedures in this section. If the Central Management store fails, see Restoring the Server Hosting the Central Management Store.

Tip:

We recommend that you take an image copy of the system before you start restoration. You can use this image as a rollback point, in case something goes wrong during restoration. You might want to take the image copy after you install the operating system and SQL Server, and restore or re-enroll the certificates.

To restore a Standard Edition server

1. Start with a clean or new server that has the same fully qualified domain name (FQDN) as the failed computer, install the operating system, and then restore or reenroll the certificates.

Note:
Follow your organization's server deployment procedures to perform this step.

2. From a user account that is a member of the RTCUniversalServerAdmins group and the Local Administrators group, log on to the server that you are restoring.
3. Restore the File Store by copying the appropriate File Store from $Backup to the File Store location on the server and share the folder.

Important:
The path and file name for the restored File Store should be exactly the same as the backed up File Store so that components that use the files can access them.

4. Run Topology Builder:
   - 4.a. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
   - 4.b. Click **Download Topology from existing deployment**, and then click **OK**.
   - 4.c. Select the topology, and then click **Save**. Click **Yes** to confirm your selection.
5. Browse to the Lync Server installation folder or media, and then start the Lync Server Deployment Wizard located at \setup\amd64\Setup.exe. Use the Lync Server Deployment Wizard to do the following:
   - 5.a. Run **Step 1: Install Local Configuration Store** to install the local configuration files.
   - 5.b. Run **Step 2: Setup or Remove Lync Server Components** to install the Lync Server server roles.
   - 5.c. Run **Step 3: Request, Install or Assign Certificates** to assign the certificates.
   - 5.d. Run **Step 4: Start Services** to start services on the server.

   For details about running the Deployment Wizard, see the Deployment documentation for the server role you are restoring.
6. Restore user data by performing the following:
   - 6.a. Copy ExportedUserData.zip from $Backup\ to a local directory.
   - 6.b. Before you restore the user data, you must stop Lync services. To do so, type:

     ```
     Stop-CsWindowsService
     ```

   - 6.c. To restore the user data, at the command line, type:

     ```
     Import-CsUserData -PoolFqdn <Fqdn> -FileName <String>
     ```

     For example:

     ```
     Import-CsUserData -PoolFqdn "atl0cs-001.litwareinc.com" -Fi
     ```

   - 6.d. Restart Lync services by typing:

     ```
     Start-CsWindowsService
     ```

7. If you deployed Response Group on this Standard Edition server, restore the Response Group configuration data. For details, see Restoring Response Group Settings.
8. If you deployed Persistent Chat on this Standard Edition server, restore the Persistent Chat database (mgc.mdf).

   If you used SQL Server Backup to back up the Persistent Chat database, use SQL Server restore procedures to restore it.

   If you used the Export-CsPersistentChatData cmdlet to back it up, use the Import-CsPersistentChatData to restore it.

Restoring the Server Hosting the Central Management Store

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

***Topic Last Modified:** 2013-02-21*

A Lync Server deployment has a single Central Management store, a copy of which is replicated to each server running a Lync Server server role. This topic describes how to restore a Back End Server or Standard Edition server that hosts the Central Management store.

To find the pool where the Central Management Server is located, open Topology Builder, click **Lync Server**, and look in the right pane under **Central Management Server**.

If the Back End Server that hosts the Central Management store is in a mirrored setup and the mirror database is still functional, we recommend that you make a backup of this still-functioning mirror, and then perform a full restore on both the primary database and the mirror database, using this backup, by following the restoration procedure below. This is necessary because Back End restore requires modifying and publishing the topology, and this can be done only if the primary database hosting CMS is operational. Also note that the primary and mirror database roles cannot be interchanged if the topology cannot be published.

Note:

If a Back End Server or Standard Edition server that does not host the Central Management store failed, see Restoring an Enterprise Edition Back End Server or Restoring a Standard Edition Server. If a Back End Server that hosts the Central Management store is in a mirrored configuration and only the mirror failed, see Restoring a Mirrored Enterprise Edition Back End Server - Mirror. If any other server failed, see Restoring an Enterprise Edition Member Server.

Tip:

We recommend that you take an image copy of the system before you start restoration. You can use this image as a rollback point, in case something goes wrong during restoration. You might want to take the image copy after you install the operating system and SQL Server, and restore or reenroll the certificates.

⊟To restore the Central Management store

1. Start with a clean or new server that has the same fully qualified domain name (FQDN) as the failed computer, install the operating system, and then restore or reenroll the certificates.

   Note:

   Follow your organization's server deployment procedures to perform this step.

2. From a user account that is a member of the RTCUniversalServerAdmins group and the Local Administrators group, log on to the server that you are restoring.
3. If you are restoring a Standard Edition server, restore the File Store by copying the appropriate File Store from $Backup to the File Store location on the server, and then share the folder.

   Important:

   The path and file name for the restored File Store should be exactly the same as the backed up File Store so that components that use the files can access them.

4. Do one of the following:

- If you are installing a Standard Edition server, browse to the Lync Server installation folder or media, and then start the Lync Server Deployment Wizard located at \setup\amd64\Setup.exe. In the Deployment Wizard, click **Prepare first Standard Edition server** and follow the wizard to install the Central Management store.
- If you are installing an Enterprise Back End Server, install SQL Server 2012 or SQL Server 2008 R2, keeping the instance names the same as before the failure.

> **Note:**
> Depending on the server that you are restoring and on your deployment, the server might include multiple collocated or separate databases. Follow the same procedure to install SQL Server that you used originally to deploy the server, including SQL Server permissions and logins.

5. From a Front End Server, Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
6. Re-create the Central Management store. At the command line, type:

```
Install-CsDatabase -CentralManagementDatabase -Clean -SqlServerFqdn <F
```

For example:

```
Install-CsDatabase -CentralManagementDatabase -Clean -SqlServerFqdn Se
```

7. Set the Active Directory Domain Services (AD DS) control point for the Central Management store. At the command line, type:

```
Set-CsConfigurationStoreLocation -SqlServerFqdn <FQDN> -SqlInstanceNam
```

For example:

```
Set-CsConfigurationStoreLocation -SqlServerFqdn Server01.contoso.com -
```

> **Note:**
> If you lose the connection point, you can rerun this cmdlet.

8. Import the Central Management store data from $Backup. At the command line, type:

```
Import-CsConfiguration -FileName <CMS backup file name>
```

For example:

```
Import-CsConfiguration -FileName "C:\Config.zip"
```

9. Enable the changes you have just made. At the command line, type:

```
Enable-CsTopology
```

> **Note:**
> After you enable the topology, you can find the topology document in the database.

10. If you are restoring an Enterprise Edition Back End Server that also hosted the CMS, or if you need to re-create a mirror of the CMS, then follow this step. Otherwise, skip to step 11.
    Install the stand-alone databases by doing the following:
    - Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
    - Click **Download Topology from existing deployment**, and then click **OK**.
    - Select the topology, and then click **Save**. Click **Yes** to confirm your selection.
    - Right-click the **Lync Server 2013** node, and then click **Install Database**.
    - Follow the **Install Database** wizard. If you are restoring a database other than the Central Management store on this server, on the **Create databases** page, select the databases you want to recreate.

Note:

Only stand-alone databases are displayed on the **Create databases** page. Collocated databases are created when you run the Lync Server Deployment Wizard.

- If you are restoring a mirrored Back End Server, continue to follow the rest of the wizard until you come to a prompt of Create Mirror Database. Select the database you want to install, and complete the process.
- Follow the rest of the wizard, and then click **Finish**.

Tip:

Instead of running Topology Builder, you can use the **Install-CsDatabase** cmdlet to create each database, and the **Install-CsMirrorDatabase** cmdlet to configure mirroring. For details, see Install-CsDatabase and Install-CsMirrorDatabase.

11. If you are restoring a Standard Edition server, browse to the Lync Server installation folder or media, and start the Lync Server Deployment Wizard located at \setup\amd64\Setup.exe. Use the Lync Server Deployment Wizard to do the following:
    - Run **Step 1: Install Local Configuration Store** to install the local configuration files.
    - Run **Step 2: Setup or Remove Lync Server Components** to install the Lync Server server roles.
    - Run **Step 3: Request, Install or Assign Certificates** to assign the certificates.
    - Run **Step 4: Start Services** to start services on the server.

    For details about running the Deployment Wizard, see the Deployment documentation for the server role that you are restoring.
12. Restore user data by performing the following:
    - Copy ExportedUserData.zip from $Backup\ to a local directory.
    - Before you restore the user data, you must stop Lync services. To do so, type:

      ```
      Stop-CsWindowsService
      ```

    - To restore the user data, at the command line, type:

      ```
      Import-CsUserData -PoolFqdn <Fqdn> -FileName <String>
      ```

      For example:

      ```
      Import-CsUserData -PoolFqdn "atl0cs-001.litwareinc.com" -Fi
      ```

    - Restart Lync services by typing:

      ```
      Start-CsWindowsService
      ```

13. Restore Location Information data to the Central Management store. At the command line, type:

    ```
    Import-CsLisConfiguration -FileName <LIS backup file name>
    ```

    For example:

    ```
    Import-CsLisConfiguration -FileName "D:\E911Config.zip"
    ```

14. If you deployed Response Group on this pool or Standard Edition server, restore the Response Group configuration data. For details, see Restoring Response Group Settings.
15. If you are restoring a Back End Server that includes Archiving or Monitoring databases, restore the Archiving or Monitoring data by using a SQL Server management tool, such as SQL Server Management Studio. For details, see Restoring Monitoring or Archiving Data.

Restoring an Enterprise Edition Back End Server

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-18*

Use the procedure described in this topic in the following two cases:

- Both the primary and mirror databases of a mirrored Enterprise Edition Back End Server fail.
- An Enterprise Edition Back End Server that is not mirrored fails.

If you have a mirrored Enterprise Edition Back End and only the mirror or primary database fails, see Restoring a Mirrored Enterprise Edition Back End Server - Primary for restoring the primary database, and Restoring a Mirrored Enterprise Edition Back End Server - Mirror for restoring the mirror.

If the Central Management store fails, see Restoring the Server Hosting the Central Management Store. If an Enterprise Edition member server that is not the Back End Server fails, see Restoring an Enterprise Edition Member Server.

Tip:

We recommend that you take an image copy of the system before you start restoration. You can use this image as a rollback point, in case something goes wrong during restoration. You might want to take the image copy after you install the operating system and SQL Server, and restore or reenroll the certificates.

⊟To restore an Enterprise Edition Back End Server

1. Start with a clean or new server that has the same fully qualified domain name (FQDN) as the failed computer, install the operating system, and then restore or reenroll the certificates.

   Note:

   Follow your organization's server deployment procedures to perform this step.

2. From a user account that is a member of the RTCUniversalServerAdmins group, log on to the server that you are restoring.
3. Install SQL Server 2012 or SQL Server 2008 R2, keeping the instance names the same as before the failure.

   Note:

   Depending on your deployment, the Back End Server might include multiple collocated or separate databases. Follow the same procedure to install SQL Server that you used originally to deploy the server, including SQL Server permissions and logins.

4. After you install SQL Server, perform the following:

   4.a. Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.

   4.b. Click **Download Topology from existing deployment**, and then click **OK**.

   4.c. Select the topology, and then click **Save**. Click **Yes** to confirm your selection.

   4.d. Right-click the **Lync Server 2013** node, and then click **Publish Topology**.

   4.e. Follow the **Publish the Topology** wizard. On the **Create databases** page, select the databases that you want to re-create.

   Note:

   Only stand-alone databases are displayed on the **Create databases** page.

4.f.If you are restoring a Back End that was mirrored, continue to follow the rest of the wizard until the prompt **Create Mirror Database** appears. Select the database that you want to install, and complete the process.
4.g.Follow the rest of the wizard, and then click **Finish**.

Tip:
Instead of running Topology Builder, you can use the **Install-CsDatabase** cmdlet to create each database, and the **Install-CsMirrorDatabase** cmdlet to configure mirroring. For details, see the Lync Server Management Shell documentation.

5. Restore user data by performing the following:
5.a.Copy ExportedUserData.zip from $Backup\ to a local directory.
5.b.Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
5.c.Before you restore the user data, you must stop Lync services. To do so, type:

```
Stop-CsWindowsService
```

5.d.To restore the user data, at the command line, type:

```
Import-CsUserData -PoolFqdn <Fqdn> -FileName <String>
```

For example:

```
Import-CsUserData -PoolFqdn "atl0cs-001.litwareinc.com" -Fi
```

5.e.Restart Lync Services by typing:

```
Start-CsWindowsService
```

6. If you deployed Response Group on this pool, restore the Response Group configuration data. For details, see Restoring Response Group Settings.
7. If you are restoring a Back End Server that included Archiving or Monitoring databases, restore the Archiving or Monitoring data by using a SQL Server tool, such as SQL Server Management Studio. For details, see Restoring Monitoring or Archiving Data.

1.7.19.3.4.1 Restoring a Mirrored Enterprise Edition Back End Server - Primary

Restoring a Mirrored Enterprise Edition Back End Server - Primary

Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings > Restoring an Enterprise Edition Back End Server >

Topic Last Modified: *2013-02-17*

If you have an Enterprise Edition Back End Server in a mirrored configuration and only the primary database fails, follow the procedures in this section. If both the primary database and mirror fail, see Restoring an Enterprise Edition Back End Server. If only the mirror fails, see Restoring a Mirrored Enterprise Edition Back End Server - Mirror. If the database hosting the Central Management store fails, see Restoring the Server Hosting the Central Management Store. If an Enterprise Edition member server that is not the Back End Server fails, see Restoring an Enterprise Edition Member Server.

We recommend that you take an image copy of the system before you start restoration. You can use this image as a rollback point, in case something goes wrong during restoration. You might want to take the image copy after you install the operating system and SQL Server, and restore or reenroll the certificates.

In this topic, the example primary database will have a fully qualified domain name (FQDN) of BE1.contoso.com, and the mirror database will have an FQDN of BE2.contoso.com.

To restore an Enterprise Edition Back End Server Primary Database

1. From a user account that is a member of the RTCUniversalServerAdmins group, log on to a Front End Server.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Force all of the configured databases to fail over to the Mirror. For each of the database types that you have configured on this server, type the following cmdlet:

   ```
   Invoke-CsDataBaseFailover -PoolFqdn <Pool FQDN> -DatabaseType <Configu
   ```

   For example:

   ```
   Invoke-CsDataBaseFailover -PoolFqdn pool0.vdomain.com -DatabaseType Us
   ```

   > ⚠**Warning:**
   >
   > If you have configured your back-end database to use synchronized mirroring with a witness, failover is automatic.

4. After completing failover, perform the following:
   - Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
   - Disable mirroring on the Back End Server: Right-click on the pool under **Enterprise Edition Front End pools** and select **Edit Properties**. On the **General** tab, under **Associations**, clear the **Enable SQL Server store mirroring** check box. Do this for Archiving and Monitoring as necessary. Then click **OK**.
   - Right-click the Lync Server 2013 node, click **Topology**, and then click **Publish**.
   - Select the still functioning backend (BE2.contoso.com) to be the new SQL store. To do this, right-click on the pool under **Enterprise Edition Front End pools** and select **Edit Properties**. On the **General** tab, under **Associations**, type the FQDN of the functioning backend in the **SQL Server store** field (in our example, BE2.contoso.com).
   - Right-click the Lync Server 2013 node, click **Topology**, and then click **Publish**.
   - Restart services so that each server can read the new topology. From a Lync Server Management Shell, run the following cmdlets on each Front End Server that belongs to this pool:

     ```
     Stop-CsWindowsService
     Start-CsWindowsService
     ```

5. Uninstall mirroring. From a Lync Server Management Shell, run the following cmdlet:

   ```
   Uninstall-CsMirrorDatabase -DatabaseType User -SqlServerFqdn <MirrorSe
   ```

   For example:

   ```
   Uninstall-CsMirrorDatabase -DatabaseType User -SqlServerFqdn DB2.conto
   ```

   Do this for all database types on this server.
6. Create a clean or new server that has the same FQDN (in this example, DB1.contoso.com) as the failed computer, install the operating system, and then restore or reenroll the certificates. This server will function as the new mirror.
7. From a user account that is a member of the RTCUniversalServerAdmins group, log on to the new server.
8. Install SQL Server 2012 or SQL Server 2008 R2, keeping the instance names the same as before the failure.
9. From a user account that is a member of the RTCUniversalServerAdmins group, log on to a Front End Server.

10. Use Topology Builder to install mirror DB. Perform the following steps:
    - Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
    - Enable mirroring on the Back End Server. To do so, right-click on the pool under **Enterprise Edition Front End pools** and select **Edit Properties**. On the **General** tab, under **Associations**, select the **Enable SQL Server store mirroring** check box. Also do this for Archiving and Monitoring, if necessary. Then, in the **Mirroring SQL Server store** field, type the FQDN of the new server (n this example, BE1.contoso.com). Then click **OK**.
    - Right-click the Lync Server 2013 node, click **Topology**, and then click **Install Database**.
    - Follow the **Install Database** wizard. On the **Create databases** page, select the databases that you want to recreate.
    - Follow the wizard until you come to the prompt, **Create Mirror Database**. Select the database that you want to install, and complete this process.

1.7.19.3.4.2 Restoring a Mirrored Enterprise Edition Back End Server - Mirror

Restoring a Mirrored Enterprise Edition Back End Server - Mirror

Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings > Restoring an Enterprise Edition Back End Server >

***Topic Last Modified:** 2013-02-19*

If you have an Enterprise Edition Back End Server in a mirrored configuration and only the mirror fails, follow the procedures in this section. If both the primary database and mirror fail, see Restoring an Enterprise Edition Back End Server. If only the primary fails, see Restoring a Mirrored Enterprise Edition Back End Server - Primary. If the database hosting the Central Management store fails, see Restoring the Server Hosting the Central Management Store. If an Enterprise Edition member server that is not the Back End Server fails, see Restoring an Enterprise Edition Member Server.

We recommend that you take an image copy of the system before you start restoration. You can use this image as a rollback point, in case something goes wrong during restoration. You might want to take the image copy after you install the operating system and SQL Server, and restore or reenroll the certificates.

⊟To restore an Enterprise Edition Back End Server Mirror Database

1. From a user account that is a member of the RTCUniversalServerAdmins group, log on to a Front End Server.
2. Start the Lync Server Management Shell: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Management Shell**.
3. Uninstall mirroring. First, type the following cmdlet:

   ```
   Uninstall -CsMirrorDatabase -DatabaseType User -SqlServerFqdn <Primary
   ```

   For example:

   ```
   Uninstall -CsMirrorDatabase -DatabaseType User -SqlServerFqdn server4.
   ```

   Do this for all database types on this server.
4. Create a clean or new server that has the same fully qualified domain name (FQDN) (DB1.contoso.com) as the failed computer, install the operating system, and then restore or reenroll the certificates. This server will function as the new mirror.
5. From a user account that is a member of the RTCUniversalServerAdmins group, log on to the new server.

6. Install SQL Server 2012 or SQL Server 2008 R2, keeping the instance names the same as before the failure.
7. From a user account that is a member of the RTCUniversalServerAdmins group, log on to a Front End Server.
8. Use Topology Builder to install the mirror database. Perform the following:
   - Start Topology Builder: Click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Topology Builder**.
   - Right-click the Lync Server 2013 node, click **Topology**, and then click **Install Database**.
   - Follow the **Install Database** wizard. On the **Create databases** page, select the databases that you want to recreate.
   - Follow the wizard until a prompt of **Create Mirror Database** appears. Select the database that you want to install and complete this process.

Tip:

Instead of running Topology Builder, you can use the **Install-CsMirrorDatabase** cmdlet to configure mirroring. For details, see the Lync Server Management Shell documentation.

1.7.19.3.5 Restoring Response Group Settings

Restoring Response Group Settings

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-18*

If you deployed the Response Group application and you need to restore a Back End Server or a Standard Edition server, you also need to restore the Response Group configuration settings.

To restore Response Group configuration settings

1. At the command line, type:

```
Import-CsRgsConfiguration -Destination "service:ApplicationServer:<pod
```

For example:

```
Import-CsRgsConfiguration -Destination "service: ApplicationServer:poo
```

1.7.19.3.6 Restoring an Enterprise Edition Member Server

Restoring an Enterprise Edition Member Server

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-18*

If a server running one of the following server roles fails, follow the procedure in this topic to restore the server. If multiple servers fail independently, follow the procedure for each server.

- Front End Server
- Mediation Server
- Director
- Persistent Chat Server
- Edge Server

Tip:

We recommend that you take an image copy of the system before you start restoration. You can use this image as a rollback point, in case something goes wrong during restoration. You might want to take the image copy after you install the operating system and SQL Server, and restore or reenroll the certificates.

⊟To restore a member server

1. Start with a clean or new server that has the same fully qualified domain name (FQDN) as the failed server, install the operating system, and then restore or reenroll the certificates.

   Note:
   Follow your organization's server deployment procedures to perform this step.

2. From a user account that is a member of the RTCUniversalServerAdmins group, log on to the server that you are restoring.
3. Browse to the Lync Server installation folder or media, and start the Lync Server Deployment Wizard located at \setup\amd64\Setup.exe.
4. Follow the Deployment Wizard to do the following:
   4.a. Run **Step 1: Install Local Configuration Store** to install the local configuration files.
   4.b. Run **Step 2: Setup or Remove Lync Server Components** to install the Lync Server server role.
   4.c. Run **Step 3: Request, Install or Assign Certificates** to assign the certificates.
   4.d. Run **Step 4: Start Services** to start services on the server.

   For details about running the Deployment Wizard, see the Deployment documentation for the server role that you are restoring.

1.7.19.3.7 Restoring a Lync Server Pool

Restoring a Lync Server Pool

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-18*

Your Lync Server deployment may include any of the following types of pools:

- Front End Server
- Mediation Server
- Persistent Chat Server
- Edge Server

If an entire pool experiences an outage, follow these procedures for each member server in the pool.

- For a Front End pool, restore the Back End Server first, and then restore each Front End Server. For details, see Restoring an Enterprise Edition Back End Server and Restoring an Enterprise Edition Member Server.
- For all other types of pools, restore each member server. For details, see Restoring an Enterprise Edition Member Server.

1.7.19.3.8 Performing an ABC Front End Pool Failover

Performing an ABC Front End Pool Failover

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-21*

The two topics in this section describe the procedure for performing an ABC pool failover in Lync Server 2013, where there are paired Lync Server Front End pools A and B, and pool A becomes unrecoverable. Using this procedure, you create a new Front End pool C with a new fully qualified domain name (FQDN). Pool C is constructed from the information from failed pool A. The procedure also includes pairing together pools B and C.

- Backup Prerequisites for ABC Pool Failover
- Front End Pool ABC Failover Procedure

1.7.19.3.8.1 Backup Prerequisites for ABC Pool Failover

Backup Prerequisites for ABC Pool Failover

Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings > Performing an ABC Front End Pool Failover >

Topic Last Modified: *2013-02-18*

To get the maximum benefit from using the ABC pool failover procedure, you must perform certain backups before the disaster and failover happen:

- You must regularly back up the Location Information Service (LIS) configuration data from pool A by using the **Export-CsLISConfiguration** cmdlet.

  ```
  Export-csLisConfiguration -FileName <C:\LISExportPrimary.zip>
  ```

- You must regularly back up the Response Group configuration data in pool A by using the **Export-CsRgsConfiguration** cmdlet.

  ```
  Export-CsRgsConfiguration -Source "service:ApplicationServer:<Pool A FQ
  ```

  In general, we recommend that you perform daily backups, but if you have a high volume of changes, you might want to schedule more frequent backups. The amount of information that you can lose in the event of a disaster depends on the frequency of your backups, as well as on the frequency and volume of changes.

  The Response Group application can store only one set of application-level settings per pool. These settings can be accessed through the **Get-CsRgsConfiguration** cmdlets. The settings include the default music-on-hold configuration, the default music-on-hold audio file, the agent ring-back grace period, and the call context configuration. These settings can be transferred from one pool to another through the **Import-CsRgsConfiguration** cmdlet by using the **ReplaceExistingSettings** parameter, but this operation will override any application-level settings in the destination pool.

  Tip:

  In a separate location, keep a backup copy of all the original audio files that have been used to configure the Response Group application (that is, any recordings or music-on-hold files).

  If you have any customized music-on-hold files that have been uploaded for Call Park in a pool, you should keep a copy of these in another location. These files are not backed up as part of the Lync Server 2013 disaster recovery process, and they will be lost if the files uploaded to the pool are damaged, corrupted, or erased.

  ```
  Xcopy  <Source: Pool A CPS File Store Path>  <Destination>
  Example: Xcopy  "<Pool A File Store Path>\LyncFileStore\coX-Application
  ```

  Note:

  The Call Park application can store only one set of settings and one customized music-on-hold audio file per pool. These settings can be accessed through the **Get-CsCpsConfiguration** cmdlet. Because the disaster recovery mechanism for Call Park relies on the Call Park application of the backup pool, the settings of the primary pool are not backed up or preserved if a disaster occurs. If the primary pool is lost, these settings cannot be recovered, and when a new pool is deployed to replace the primary pool, the Call Park settings and any customized music-on-hold audio file would need to be reconfigured.

- If you configure any announcements as part of the Unassigned Number Voice Feature, we recommend that you keep in another location a copy of any original audio file used during the initial configuration. If you did not do that, you can get a copy of the configured audio files in the file store of the server or pool to which the audio files were imported. These files are not backed up as part of the Lync Server 2013 disaster recovery process, and they will be lost if the files uploaded to the pool are damaged, corrupted, or erased. To copy all the audio files used to configure the Unassigned Number Voice Feature from the file store of a server or a pool, use:

```
Use: Xcopy  <Source: Pool A Announcement Service File Store Path>  <Des
Example Usage:  Xcopy  "<Pool A File Store Path>\X-ApplicationServer-X\
```

- If you have Monitoring and Archiving databases in a pool, you should use SQL Server management tools to back them up. In the ABC failover procedure, Monitoring and Archiving databases are not preserved if they are collocated in pool A, because these databases are not backed up through Lync Server Backup Service.
  Note that Lync Server supports only the Simple Recovery model for Monitoring and Archiving databases. With the Simple Recovery model, databases are recovered to the point of the last full backup. This means that you cannot restore a database to the point of failure or to a specific point in time.

1.7.19.3.8.2 Front End Pool ABC Failover Procedure

Front End Pool ABC Failover Procedure

Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings > Performing an ABC Front End Pool Failover >

Topic Last Modified: *2013-02-21*

Use the following steps to perform the ABC failover procedure. This procedure contains a high-level description of each step, followed by commands and cmdlets to be run for each step.

To run the cmdlets, open a Lync Server Management Shell using Run as Administrator.

To Perform an ABC Failover

1. Check whether the pool A is the host for the Central Management Server (CMS).
   - Run the following cmdlet:

     ```
     Get-CsService -CentralManagement
     ```

     If the Identity field of the active CMS points to the fully qualified domain name (FQDN) of Pool A, then you use steps 2 and 3 of this procedure to fail over the Central Management Server first. Otherwise, skip to step 4.
2. Fail over the CMS to Pool B in disaster recovery mode by running the following cmdlet:

   ```
   Invoke-CsManagementServerFailover -BackupSqlServerFqdn <Pool B BE FQDN
   ```

   After you do this, we recommend that you move the CMS from pool B to another existing paired pool for extra resiliency. For details, see Move-

CsManagementServer..

3. If Pool A contains CMS, import the LIS configuration from pool A into pool B’s LIS database (Lis.mdf). This will work only if you have been backing up LIS data on a regular basis. To import the LIS configuration, run the following cmdlets:

```
Import-CsLisConfiguration -FileName <String>
Publish-CsLisConfiguration
```

4. Import backed-up Lync Server Response Group service workflows from pool A into pool B.

Note:

Currently, the **Import-CsRgsConfiguration** cmdlet requires that the queue and workflow names on pool A are distinct from the queue and workflow names on pool B. If the names are not distinct, you will get an error when running the **Import-CsRgsConfiguration** cmdlet, and the queues and workflows will need to be renamed in pool B before proceeding with **Import-CsRgsConfiguration** cmdlet.

You have two options for importing the Response Group configuration from pool A to pool B. Which option you use depends on whether you want to overwrite the application-level settings of pool B with the application-level settings in pool A.

- If you want to overwrite the Pool B settings, run the **Import-CsRgsConfiguration** cmdlet with the **ReplaceExistingSettings** option:

```
Import-CsRgsConfiguration -Destination "service:ApplicationS
```

- If you do not want to overwrite the Pool B settings, use the **Import-CsRgsConfiguration** cmdlet without the **ReplaceExistingSettings** option.

```
Import-CsRgsConfiguration -Destination "service:ApplicationS
```

Warning:

Keep in mind that if you do not want to overwrite the application-level settings of the backup pool (pool B) with the settings of the primary pool (pool A), pool A’s application-level settings will be lost if pool A is lost, because the Response Group application can store only one set of application-level settings per pool. When pool C is deployed to replace pool A, the application-level settings must be reconfigured, including the default music-on-hold audio file.

5. Verify that the Response Group configuration import was successful by running the following cmdlets to display the imported response groups. Note that the imported response groups are still owned by pool A.

```
Get-CsRgsWorkflow -Identity "service:ApplicationServer:<Pool B FQDN>"
Get-CsRgsQueue -Identity "service:ApplicationServer:<Pool B FQDN>" -Ow
Get-CsRgsAgentGroup -Identity "service:ApplicationServer:<Pool B FQDN>
```

6. For Unassigned Numbers, move the Unassigned Number ranges that are using "Announcement" as the selected announcement service from pool A to pool B. To do so:

- Re-create all announcements that were deployed in pool A on pool B. If any audio files were used when deploying the announcements in pool A, these files will be needed to re-create the announcements in pool B. To re-create the announcements in pool B, use the **New-CsAnnouncement** cmdlets, with pool B as the Parent service.
- Retarget all the Unassigned Number ranges that are targeting an announcement in pool A to the newly deployed announcements in pool B. Run the following cmdlet for every Unassigned Number range targeting an announcement of pool A:

```
Set-CsUnassignedNumber -Identity "<Range Name>" -Announcemer
```

Note:

This step is not required for unassigned number ranges that use "Exchange UM" as the selected announcement service.

7. Fail over Pool A to Pool B in Disaster Recovery (DR) mode, by running the following cmdlet:

```
Invoke-CsPoolFailover -PoolFqdn <Pool A FQDN> -DisasterMode
```

8. Build pool C, but do not start any services on pool C.
   If pool C is an Enterprise Edition pool, see Deploying Lync Server 15 Enterprise Edition Cookbook for details. If pool C is a Standard Edition pool, see Deploying Lync Server 15 Standard Edition Cookbook for details.
   Note that this step can be carried out concurrently with steps 5 and 6.
9. Force users homed on pool A to move to pool C by running the following cmdlet:

```
Get-csuser -Filter {RegistrarPool -eq "<Pool A FQDN>"} | Move-CsUser -
```

   At this point, users homed on pool A will begin to experience a service outage. This outage will continue until step 16, at which point services are started on pool C.
10. Force the conference directory of pool A to move to pool C by running the following cmdlet:

```
Move-CsConferenceDirectory -Identity <Conference Directory ID of Pool
```

11. Force the Conference Auto Attendant (CAA) Contact Object to move from pool A to pool C by running the following cmdlet:

```
Move-csApplicationEndpoint -Identity "<Pool A CAA Uri>" -targetApplica
```

12. Copy conference content from pool B to pool C. For details, see HADR Scenario – Bulk meeting content hydration/dehydration.
13. Export user data from pool B and import the user data into pool C by running the following cmdlets:

```
Export-CsUserData -PoolFqdn <Pool B Fqdn> -FileName <String>
Import-CsUserData -PoolFqdn <Pool C Fqdn> -FileName <String>
```

14. Restore backed-up Call Park application data from pool A into pool C and assign the Call Park orbit ranges of pool A to pool C.
    - You can reassign a Call Park orbit range of pool A to pool C either through the Lync Server Control Panel or the Lync Server Management Shell. For the Lync Server Management Shell, run the following cmdlet for every Call Park orbit range assigned to pool A (note that the Identity parameter refers to the Call Park Orbit Ranges that belong to pool A):

```
Set-CsCallParkOrbit -Identity "<Call Park Orbit Identity>" -
```

    - If a customized music-on-hold has been configured for Call Park in pool A, restore the Call Park customized music-on-hold file in pool C.

```
Xcopy <Source> <Destination: Pool C CPS File Store Path>
```

      For example:

```
Xcopy "Source Path" "<Pool C File Store Path>\OcsFileStore\c
```

    - Finally, reconfigure the Call Park settings on pool C by using the **Set-CsCpsConfiguration** cmdlet. The Call Park application can store only one set of settings and one customized music-on-hold audio file per pool, and these settings are not backed up or preserved in the event of a disaster.
15. If the next hop pool for Persistent Chat is pointing to pool A, make and publish topology changes so that the next hop server points to pool C.
    - In Topology Builder, change the Persistent Chat pool to point to Pool C as its next hop. To do so, right-click on the Persistent Chat pool, then click the **General** tab, and then type the name of Pool C in **Next Hop Pool**.
    - Start services on pool C by running the following cmdlet:

```
Start-csWindowsService
```

   At this point, the service outage ends for users originally homed on pool A.

16. Export Lync Server Response Group service workflows from pool B owned by pool A for import into pool C by running the following cmdlet:

```
Export-CsRgsConfiguration -Source "service:ApplicationServer:<Pool B F
```

17. Import Lync Server Response Group service workflows into pool C from pool B.
    You have two options are for importing the Response Group configuration from pool B to pool C. Which option you use depends on whether you want to overwrite the application-level settings of pool C with the application-level settings in pool B.
    - If you want to overwrite the Pool C settings, run the **Import-CsRgsConfiguration** cmdlet with the **ReplaceExistingSettings** option:

      ```
      Import-CsRgsConfiguration -Destination "service:ApplicationS
      ```

    - If you do not want to overwrite the Pool C settings, use the **Import-CsRgsConfiguration** cmdlet without the **ReplaceExistingSettings** option.

      ```
      Import-CsRgsConfiguration -Destination "service:ApplicationS
      ```

Warning:

Keep in mind that if you do not want to overwrite the application-level settings of Pool C with the settings of the backup pool (pool B), pool B's application-level settings will be lost because the Response Group application can store only one set of application-level settings per pool.

18. Verify that the Response Group configuration import was successful by running the following cmdlets to display the response groups that have been imported to Pool C.

```
Get-CsRgsWorkflow -Identity "service:ApplicationServer:<Pool C FQDN>"
 Get-CsRgsQueue -Identity "service:ApplicationServer:<Pool C FQDN>" -S
Get-CsRgsAgentGroup -Identity "service:ApplicationServer:<Pool C FQDN>
```

19. When the imported configuration has been verified in pool C, remove the response groups owned by the primary pool from pool B. This will minimize the downtime of the response groups.
    This step creates a new file with the exported configuration, and then removes the file from pool B.

```
Export-CsRgsConfiguration -Source "service:ApplicationServer:<Pool B F
```

20. Move to pool C the Unassigned Number ranges that were moved from pool A to pool B.
    - Re-create in pool C all announcements that were re-created from pool A in pool B. If any audio files were used when deploying the announcements to be moved, you will need to use these files to re-create the announcements in pool C. To re-create the announcements in pool C, use the **New-CsAnnouncement** cmdlets, with pool C as the Parent service.
    - Retarget to pool C all the unassigned number ranges that were retargeted from pool A to pool B. Run the following cmdlet for every Unassigned Number range that needs to be retargeted:

      ```
      Set-CsUnassignedNumber -Identity "<Range Name>" -Announcemen
      ```

    - (Optional) Remove from pool B the announcements that were re-created in pool C if they are no longer in use in pool B. To remove announcements, use the **Remove-CsAnnouncement** cmdlet.

      Note:

      This step is not required for unassigned number ranges that use "Exchange UM" as the announcement service.

21. Clean up user data of pool A in pool B by running the following cmdlet:

```
Remove-CsUserStoreBackupData -PoolFqdn <Pool B FQDN> -Verbose
```

22. Do the following in Topology Builder:
    - Unpair pool A and pool B. Pair pool B and pool C. Then remove Pool A from

the topology and publish it. To do so:

- In Topology Builder, right-click on Pool B, and then click **Edit Properties**.
- Click **Resiliency** in the left pane.
- In the box below **Associated Backup Pool**, select Pool C. Note that the Associated Backup Pool selection box will initially display pool A, because pool B was previously associated with this pool.
- Select **Automatic failover and failback for Voice**, and then click **OK**.

  When you view the details about this pool, the associated pool now appears in the right pane under **Resiliency**.
- In the console tree, right-click pool A, and then click Delete.
- Publish the topology.

23.Run the bootstrapping application on pool C to install the backup service application, and then start the backup service application by running the following from the deployment folder on a local machine in pool C:

```
Run "%SYSTEMROOT%\Program Files\Microsoft Lync Server 2013\Deployment\
Start-CsWindowsService -name LyncBackup
```

24.Restart the backup service application on pool B by running the following cmdlets:

```
Stop-CsWindowsService -name LyncBackup
Start-CsWindowsService -name LyncBackup
```

25.If pool C is a Standard Edition (SE) Pool and pool B has CMS, install the CMS database manually on pool C by running the following cmdlet:

```
Install-CsDatabase -CentralManagementDatabase -SqlServerFqdn <Pool C F
```

26.Invoke the backup service to sync old conferencing content from pool B to pool C that was generated before pairing B and C together, and to sync new conferencing content from pool C to pool B that was generated after starting pool C and before B and C were paired together. To do so, run the following cmdlets:

```
Invoke-CsBackupServiceSync -PoolFqdn <Pool C FQDN>
Invoke-CsBackupServiceSync -PoolFqdn <Pool B FQDN>
```

27.For each Survivable Branch Appliance X associated with pool A:

- Shut down SBA X by running the following cmdlet:

  ```
  Stop-CsWindowsService
  ```

- Create a file that contains a list of users homed on SBA X. The list will be needed when the users are moved back to SBA X in step 30. To do so, run the following cmdlet:

  ```
  Get-CsUser -Filter {RegistrarPool -eq "<SBA X FQDN>"} | Expo
  ```

- Force users homed on SBA X to move to pool C by running the following cmdlet:

  ```
  Get-CsUser -Filter {RegistrarPool -eq "<SBA X FQDN>"} | Move
  ```

- Update the data of these users by first running the following cmdlets:

  ```
  Convert-csUserData -InputFile <Data file exported from PoolB
  $a=get-csuser -Filter {RegistrarPool -eq "FQDN of SBA X"} |
  foreach($x in $a) {$x.SipAddress.Substring(4) >> users.txt}
  ```

  And then run this script:

  ```
  $users=gc c:\logs\users.txt
  foreach ($user in $users)
  {
  Update-CsUserData -FileName c:\logs\exportedUserDAta.xml -Us
  }
  ```

  Note:

  A service outage will occur for users who are homed on SBAs that are associated with pool A until these users are moved to pool C.

28. In Topology Builder, for each SBA X previously associated with Pool A, do the following:
    - Change the association to Pool C. To do so, click the branch site, expand the Survivable Branch Appliances or Servers node, and click **Survivable Branch Appliance**. Then select the **Front End pool, User Services Pool** that this Survivable Branch Appliance will connect to as Pool C, and then click **Next**.
    - Publish the topology. To do so, in the console tree, right-click the new **Survivable Branch Appliance**, click **Topology**, and then click **Publish**.
29. For each SBA X now associated with pool C:
    - Start SBA X by running the following cmdlet on the survivable branch appliance:

      ```
      Start-CsWindowsService
      ```

    - Move users who were originally homed on SBA X from pool C to SBA X by running the following cmdlet.

      ```
      Import-Csv d:\sbaxusers.txt | Move-CsUser -Target <SBA X FQD
      ```

1.7.19.3.9 Restoring a File Store

Restoring a File Store

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-18*

File Stores for Standard Edition are typically located on the Standard Edition server. File Stores for Enterprise Edition are typically located on a file server or cluster. The following procedure describes how to restore a File Store.

To restore a File Store

1. If a File Store fails, copy the appropriate File Store from $Backup\ to the File Store location on the file server or Standard Edition server, and then share the folder.

   > **Important:**
   > The path and file name for the restored File Store should be exactly the same as the backed up File Store, so that components that use the files can access them.

2. If necessary, set the access control lists (ACLs) for the File Store. At the command line, type:

   ```
   Enable-CsTopology
   ```

   > **Note:**
   > You need to perform this step only if you have not otherwise run Topology Builder during your restoration process.

1.7.19.3.10 Restoring Monitoring or Archiving Data

Restoring Monitoring or Archiving Data

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-18*

Restoring monitoring and archiving data is not required to get Lync Server up and running after a failure. However, if monitoring and archiving data is critical to your organization, you will want to restore the data after you re-create the databases.

The following procedure describes how to use SQL Server Management Studio to restore archiving or monitoring data.

⊟To restore monitoring or archiving data from a backup file

1. Log on to the server that you are restoring as a member of the Administrators group on the local computer or a group with equivalent user rights.
2. Open SQL Server Management Studio: click **Start**, click **All Programs**, click **Microsoft SQL Server 2012** or **Microsoft SQL Server 2008 R2**, and then click **SQL Server Management Studio**.
3. In **Connect to Server**, connect to the SQL Server instance by providing at least the name of the server and the authentication information.
4. In **Object Explorer**, right-click **Databases**, and then click **Restore Database**.
5. Under **Select a page**, click **General**, and then in **To database** select the database name as follows:
   - For an Archiving database, select **LcsLog**.
   - For a call detail recording (CDR) database, select **LcsCDR**.
   - For a Quality of Experience (QoE) database, select **QoEMetrics**.
6. Click **From device**.
7. Under **Select the backup sets to restore**, click the backup file, and then click **Restore**.
8. Under **Select a page**, click **Options**, verify that the data file path and log path are in the correct folder, and then click **OK**.

⊟To make sure that access control lists (ACLs) are correct

1. Expand **Databases**, expand the archiving or monitoring database, expand **Security**, and then expand **Users**.
2. Verify that the domain group RTCComponentUniversalServices exists as a user.
3. If RTCComponentUniversalServices does not exist under **Users**, do the following:
   3.a. Right-click **Users**, and then click **New User**.
   3.b. In **Login name**, type the missing group name, RTCComponentUniversalServices.
   3.c. Under **Database role membership**, select the **ServerRole** permission, and then click **OK**.

Note:
You do not need to restart the archiving or monitoring service.

1.7.19.3.11 Restoring Persistent Chat Data

Restoring Persistent Chat Data

Operations > Backing Up and Restoring Lync Server 2013 > Restoring Data and Settings >

Topic Last Modified: *2013-02-18*

Persistent Chat room content is stored in the Persistent Chat database (mgc.mdf). This is business-critical data that should be backed up regularly. In addition to the chat room content, principals (such as users and groups) and the roles and access that they have to chat rooms and chat room content, is also stored in the Persistent Chat database.

How you restore your Persistent Chat data depends on the method that you used to back it up.

- If you used SQL Server backup procedures, you must use SQL Server restore procedures.

- If you used the **Export-CsPersistentChatData** cmdlet to back up Persistent Chat data, then you must use the **Import-CsPersistentChatData** cmdlet to restore the data.

1.7.19.4 Backup and Restoration Worksheets

Backup and Restoration Worksheets

Microsoft Lync Server 2013 > Operations > Backing Up and Restoring Lync Server 2013 >

Topic Last Modified: *2013-02-18*

The backup and restoration plan for your organization should contain details about how and when you back up data and settings. You can use the worksheets presented here to help you document this information for your specific deployment and for your organization's backup and restoration requirements.

Use the following worksheets to record the information that you need to back up and restore database, File Store, and settings information for a Lync Server pool or Standard Edition server. Keep one or more copies of these worksheets in a secure location so that they are readily accessible if you need to restore Lync Server.

Note:

The worksheets in this section cover only the information that is required to restore the data and settings of Lync Server databases and servers. If you need to document other restoration information, such as the information for reinstalling operating systems and other software, use your organization's deployment plans and backup and restoration plans to address those requirements.

Database Backup and Restoration Worksheet

Use the following table to record the information that you need to back up and restore Lync Server databases.

Database Information for Backup and Restoration

Database	Server name (FQDN)	Backup schedule	Database backup tool	Backup set	Backup destination	Notes
Rtc database on Back End Server for user data			**Export-CsUserData** cmdlet	Name: Expiration:		
LcsLog (default name) database on Archiving database server			SQL Server management tool	Name: Expiration:		
LcsCdr database			SQL Server managemen	Name:		

on Monitoring database server for call detail records (CDRs)			t tool	Expiration:		
QoEMetrics database on Monitoring database server for Quality of Experience (QoE) data			SQL Server management tool	Name: Expiration:		
Persistent Chat Database			SQL Server management tool or **Export-CsPersistentChatData** cmdlet	Name: Expiration:		

No backup or restoration is required of the following databases:

- Rtcdyn. The transient user data in this database is not necessary for restoration of service.
- Rtcab. The Address Book database is automatically recreated from the Global Address List (GAL) in Active Directory Domain Services (AD DS).
- Rgsdyn. The transient Response Group service data in this database is not necessary for restoration of service.
- Cpsdyn. The dynamic information for the Call Park application is not necessary for restoration of service.
- MgcComp. The compliance database for Persistent Chat is not necessary for restoration of service.

File Store Backup and Restoration Worksheet

Use the following table to record the information that you need to back up and restore the File Stores. File Stores contain data such as meeting content metadata, meeting compliance logs, update logs for device updates, and audio files for the Response Group, Call Park, and Announcement applications.

File Store Information for Backup and Restoration

Content	Server name (FQDN)	Backup schedule	File system backup tool	File share to be backed up *	Backup destination	Notes
Lync Server File Store			Standard backup tool, such as Robocopy	On file server for Enterprise Edition. On Standard		Files named **Meeting.Active** should not be backed up.

				Edition by default, for Standard Edition deployment. Typically, one per site.		These files are in use and are locked while a meeting takes place.

Settings Backup and Restoration Worksheet

Use the following table to record the information that you need to back up and restore settings.

Settings Information for Backup and Restoration

Database	Server name (FQDN)	Backup schedule	Backup tool	Configuration file (.xml) name	Backup location	Notes
Xds database in Central Management store for topology configuration (global)			**Export-CsConfiguration** cmdlet			
Lis database in Central Management store for E9-1-1 location information (global)			**Export-CsLisConfiguration** cmdlet			
RgsConfig database on Back End Server for Response Group configuration (pool)			**Export-CsRgsConfiguration** cmdlet			

1.7.20 Monitoring and Health Configuration

Monitoring and Health Configuration

See Also

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2013-02-22*

Topics in this section provide step-by-step procedures for monitoring and health configuration tasks you can perform in Lync Server 2013 Control Panel and Lync Server 2013 Management Shell.

- Call Detail Recording (CDR)
- Quality of Experience (QoE)
- Monitoring Mobility for Performance
- Using Monitoring Reports

⊟See Also

Concepts

Operations

1.7.20.1 Call Detail Recording (CDR)

Call Detail Recording (CDR)

See Also

Microsoft Lync Server 2013 > Operations > Monitoring and Health Configuration >

Topic Last Modified: *2012-10-22*

Call detail recording (CDR) records usage and diagnostic information about peer-to-peer activities, including instance messaging, Voice over Internet Protocol (VoIP) calls, application sharing, file transfer, and meetings. The usage data can be used to calculate return on investment (ROI) and the diagnostic data can be used to troubleshoot peer-to-peer activities and meetings. When you install Lync Server 2013, you will also install a predefined collection of global configuration settings for CDR. Use the topics in this section to configure CDR.

- View CDR Configuration Information
- Enable Call Detail Recording
- Create or Modify a Collection of CDR Configuration Settings
- Delete an Existing Collection of CDR Configuration Settings
- Manually Purging the Call Detail Recording and Quality of Experience Databases

⊟See Also

Concepts

Configuring Call Detail Recording and Quality of Experience Settings

1.7.20.1.1 View CDR Configuration Information

View CDR Configuration Information

Operations > Monitoring and Health Configuration > Call Detail Recording (CDR) >

Topic Last Modified: *2013-02-23*

Call Detail Recording (CDR) enables you to track usage of such things as peer-to-peer instant messaging sessions, Voice over Internet Protocol (VoIP) phone calls, and conferencing calls. This usage data includes information about who called whom, when they called, and how long they talked.

When you install Microsoft Lync Server 2013, a single, global collection of CDR configuration settings is created for you. Administrators also have the option of creating custom setting collections that can be applied to individual sites. You can view the CDR configuration settings in use in your organization by using Lync Server Control Panel or the Get-CsCdrConfiguration cmdlet.

To view CDR configuration information by using Lync Server Control Panel

1. In Lync Server Control Panel click **Monitoring and Archiving**.
2. A list of all your CDR configuration settings will be displayed in the **Call Detail Recording** tab; for each collection of settings you will see the collection **Name**; whether or not CDR has been enabled (the **CDR** property); and whether or not purging has been enabled (the **CDR purging** property). To see detailed information about a collection, double-click the collection, or select the appropriate collection, click **Edit**, and then click **Show Details**. Note that you can only view detailed information for a single collection of CDR configuration settings at a time.

Viewing CDR Configuration Information by Using Windows PowerShell Cmdlets

You can view CDR configuration settings by using Windows PowerShell and the Get-CsCdrConfiguration cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To view CDR configuration information

- To view information about all your CDR configuration settings, type the following command in the Lync Server Management Shell and then press ENTER:

  ```
  Get-CsCdrConfiguration
  ```

  That will return information similar to this:

  ```
  Identity                 : Global
  EnableCDR                : True
  EnablePurging            : True
  KeepCallDetailForDays    : 90
  KeepErrorReportForDays   : 60
  PurgeHourOfDay           : 2
  ```

For more information, see the help topic for the Get-CsCdrConfiguration cmdlet.

1.7.20.1.2 Enable Call Detail Recording

Enable Call Detail Recording

See Also

Operations > Monitoring and Health Configuration > Call Detail Recording (CDR) >

Topic Last Modified: *2013-02-23*

Call detail recording (CDR) records usage and diagnostic information about peer-to-peer activities including instance messaging, Voice over Internet Protocol (VoIP) calls, application sharing, file transfer, and meetings. The usage data can be used to calculate return on investment (ROI) and the diagnostic data can be used to troubleshoot peer-to-peer activities and meetings.

Use the following procedure to enable CDR for your whole organization or each site in your organization.

Note:
In order to enable CDR you must configure monitoring and a monitoring database. For details, see Deploying Monitoring.

To enable CDR with Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Call Detail Recording**.
4. On the **Call Detail Recording** page, click the appropriate site from the table, click **Action**, and then click **Enable CDR**.

   Note:
   CDR is enabled by default.

Enabling CDR by Using Windows PowerShell Cmdlets

You can enable CDR by using Windows PowerShell and the **Set-CsCdrConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable CDR for a single location

- To disable CDR, set the EnableCDR parameter to True ($True).

```
Set-CsCdrConfiguration -Identity "site:Redmond" -EnableCDR $True
```

To disable CDR for a single location

- To disable CDR, set the EnableCDR parameter to False ($False). Disabling CDR does not uninstall monitoring. It pauses the collection and storage of CDR data.

```
Set-CsCdrConfiguration -Identity "site:Redmond" -EnableCDR $False
```

To use a single command to enable CDR in multiple locations

- This command enables CDR for all the CDR configuration settings currently in use in your organization.

```
Get-CsCdrConfiguration | Set-CsCdrConfiguration "site:Redmond" -EnableC
```

For more information, see the help topic for the Set-CsCdrConfiguration cmdlet.

See Also

Other Resources

Planning for Monitoring
Deploying Monitoring

1.7.20.1.3 Specifying Retention of CDR Data

Specifying Retention of CDR Data

See Also

Operations > Monitoring and Health Configuration > Call Detail Recording (CDR) >

Topic Last Modified: *2013-02-23*

By default, call detail recording (CDR) data is purged after 60 days. You can use the settings on the **Call Detail Recording** page to retain the data for a longer or shorter period of time. If you disable CDR, data that was captured before CDR was enabled will also be subject to purging.

Note:
You should configure CDR and Quality of Experience (QoE) to retain data for the same number of days. Each call in the call detail reports (CDRs), available from the Monitoring Server Reports webpage, includes CDR and QoE information. If the purging duration for CDR and QoE is different, some calls might only include CDR data, while other may only include QoE data.

Use the following procedures to configure purge settings for CDR data.

⊟To specify retention of CDR data

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Call Detail Recording**.
4. On the **Call Detail Recording** page, click the appropriate site in the table, click **Edit**, and then click **Show Details**.
5. To turn on purging, select **Enable purging of CDRs**.
6. In **Keep CDRs for maximum duration (days):** select the maximum number of days that call detail recordings should be retained.
7. In **Keep error report data for maximum duration (days):** select the maximum number of days that error reports should be retained.
8. Click **Commit**.

Specifying CDR Retention by Using Windows PowerShell Cmdlets

You can create CDR retention settings by using Windows PowerShell and the Set-CsCdrConfiguration cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To specify CDR retention for a specific location

- This command enables purging of CDR data for the Redmond site, and configures the site to maintain both CDR data and error reports data for 20 days.

```
Set-CsCdrConfiguration -Identity "site:Redmond" -EnablePurging -KeepCal
```

To specify CDR retention for multiple locations

- This command configures CDR retention for all the CDR configuration settings in use in an organization.

```
Get-CsCdrConfiguration | Set-CsCdrConfiguration-EnablePurging -KeepCall
```

For more information, see the help topic for the Set-CsCdrConfiguration cmdlet.

See Also

Other Resources

Call Detail Recording (CDR)

1.7.20.1.4 Create or Modify a Collection of CDR Configuration Settings

Create or Modify a Collection of CDR Configuration Settings

Operations > Monitoring and Health Configuration > Call Detail Recording (CDR) >

Topic Last Modified: *2013-02-23*

Call detail recording (CDR) enables you to track usage of such things as peer-to-peer instant messaging sessions, Voice over Internet Protocol (VoIP) phone calls, and conferencing calls. This usage data includes information about who called whom, when they called, and how long they talked.

When you install Microsoft Lync Server 2013 a single, global collection of CDR configuration settings is created for you. Administrators also have the option of creating custom settings at the site scope. Whenever these site-scoped settings are used, they take precedence over the global settings. For example, if you create site-scoped settings for the Redmond site then those settings (rather than the global settings) will be used to manage CDR in Redmond.

You can create CDR configuration settings by using either Lync Server Control Panel or the New-CsCdrConfiguration cmdlet. You can use Lync Server Control Panel or the Set-CsCdrConfiguration cmdlet to modify existing settings. If you are using Lync Server Control Panel to create or modify settings, the following options will be available to you:

UI Setting	PowerShell Parameter	Description
Name	Identity	Unique identifier for the CDR configuration settings being created. These settings can only be created at the site scope.
Enable monitoring of CDRs	EnableCDR	Indicates whether or not CDR is enabled.
Enable purging of CDRs	EnablePurging	Indicates whether or not CDR records will periodically be

		deleted from the CDR database.
Keep CDRs for maximum duration (days)	KeepCallDetailForDays	Indicates the number of days that CDR records will be kept in the CDR database. Any records older than the specified number of days will automatically be deleted. (Note that purging will take only place if purging has been enabled.)
Keep error report data for maximum duration (days)	KeepErrorReportForDays	Indicates the number of days that CDR error reports are kept. Any reports older than the specified number of days will automatically be deleted. CDR error reports are diagnostic reports uploaded by client applications.

Note:

The New-CsCdrConfiguration and Set-CsCdrConfiguration cmdlets include additional options not available in Lync Server Control Panel. See the New-CsCdrConfiguration and the Set-CsCdrConfiguration help topics for more information.

To create CDR configuration settings by using Lync Server Control Panel

1. In Lync Server Control Panel click **Monitoring and Archiving**.
2. On the **Call Detail Recording** tab, click **New**.
3. In the **Select a Site** dialog box, select the site where the new configuration settings are to be created. If the dialog box is empty, that means all of your sites have already been assigned a collection of CDR configuration settings. Each site is limited to a single such collection. In that case you can either delete and then re-create the settings, or simply modify the existing settings.
4. In the **New Call Detail Recording (CDR) Setting** dialog, make the desired selections and then click **Commit**.

To modify existing CDR configuration settings by using Lync Server Control Panel

1. In Lync Server Control Panel click **Monitoring and Archiving**.
2. Double-click the collection of settings to be modified, or select the collection, click **Edit**, and then click **Show Details**. Note that you can only modify a single collection at a time. To make the same changes to multiple collections, use the Lync Server Management Shell instead.
3. In the **Edit Call Detail Recording (CDR) Setting** dialog, make the desired selections and then click **Commit**.

Creating CDR Configuration Settings by Using Windows PowerShell Cmdlets

You can create CDR configuration settings can also be created by using Windows PowerShell and the **New-CsCdrConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/

p/?linkId=255876.

⊟To create a new collection of CDR configuration settings

- This command creates a new collection of CDR configuration settings applied to the Redmond site:

```
New-CsCdrConfiguration -Identity "site:Redmond"
```

⊟To create a collection of CDR configuration settings that disable call detail recording

- Because no parameters (other than the mandatory Identity parameter) were specified in the preceding command, the new collection of configuration settings will use the default values for all its properties. To create settings that use different property values, simply include the appropriate parameter and parameter value. For example, to create a collection of Call Detail configuration settings that, by default, allow disable Call Detail recording use a command like this:

```
New-CsCdrConfiguration -Identity "site:Redmond" -EnableCDR $False
```

⊟To specify multiple property values when creating a new collection of CDR configuration settings

- You can modify multiple property values by including multiple parameters. For example, this command configures the new settings to keep Call Detail records for 30 days and error reports for 90 days:

```
New-CsCdrConfiguration -Identity "site:Redmond" -KeepCallDetailForDays
```

For more information, see the help topic for the New-CsCdrConfiguration cmdlet.

1.7.20.1.5 Delete an Existing Collection of CDR Configuration Settings

Delete an Existing Collection of CDR Configuration Settings

Operations > Monitoring and Health Configuration > Call Detail Recording (CDR) >

Topic Last Modified: *2013-02-23*

Call Detail Recording (CDR) enables you to track usage of such things as peer-to-peer instant messaging sessions, Voice over Internet Protocol (VoIP) phone calls, and conferencing calls. This usage data includes information about who called whom, when they called, and how long they talked.

When you install Microsoft Lync Server 2013, a single, global collection of CDR configuration settings is created for you. Administrators also have the option of creating custom setting collections that can be applied to individual sites. By design, settings configured at the site scope take precedence over settings configured at the global scope. If you delete site-scoped settings, then CDR will be managed in that site by using the global settings.

Note that you can also “delete” the global settings. However, the global settings will not actually be removed. Instead, all the properties in that collection will be reset to their default values. For example, by default purging is enabled in a collection of CDR configuration settings. Suppose you modify the global collection so that purging is disabled. If you later delete the global settings, all the properties will be reset to their default values. In this case, that means that purging will once again be enabled.

You can remove CDR configuration settings by using the Lync Server Control Panel or the Remove-CsCdrConfiguration cmdlet.

To remove CDR configuration settings with Lync Server Control Panel

1. In Lync Server Control Panel, click **Monitoring and Archiving**.
2. On the **Call Detail Recording** tab, select the collection (or collections) of CDR settings to be removed. To select multiple collections, click the first collection, hold down the Ctrl key, and click additional collections.
3. Click **Edit**, and then click **Delete**.
4. In the Lync Server Control Panel dialog box, click **OK**.

Removing CDR Configuration Settings by Using Windows PowerShell Cmdlets

You can delete call detail recording configuration settings by using Windows PowerShell and the **Remove-CsCdrConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specified collection of CDR configuration settings

- This command removes the CDR configuration settings applied to the Redmond site:

```
Remove-CsCdrConfiguration -Identity "site:Redmond"
```

To remove all the CDR configuration settings applied to the site scope

- This command removes all the CDR configuration settings applied to the site scope:

```
Get-CsCdrConfiguration -Filter "site:*" | Remove-CsCdrConfiguration
```

To remove all the CDR configuration settings that disable call detail recording

- This command removes all the CDR configuration settings where Call Detail recording has been disabled:

```
Get-CsCdrConfiguration | Where-Object {$_.EnableCDR -eq $False} | Remov
```

For more information, see the help topic for the Remove-CsCdrConfiguration cmdlet.

1.7.20.1.6 Manually Purging the Call Detail Recording and Quality of Experience Databases

Manually Purging the Call Detail Recording and Quality of Experience Databases

Microsoft Lync Server 2013 > Deployment > Deploying Monitoring >

Topic Last Modified: *2012-11-01*

Administrators can configure the Call Detail Recording (CDR) and/or the Quality of Experience (QoE) databases to automatically purge old records from the database; this occurs if purging has been enabled for the specified database (CDR or QoE) and if there are any records that have been in the database longer than the specified amount of time.

For example, every day at 1:00 AM administrators might configure the system so that QoE records more than 60 days old will be deleted from the QoE database.

In addition to that automatic purging, two new cmdlets -- Invoke-CsCdrDatabasePurge and Invoke-CsQoEDatbasePurge -- have been added to Microsoft Lync Server 2013; these cmdlets allow administrators to manually purge records from the CDR and the QoE databases at any time. For example, to manually purge all the records more than 10 days old from the CDR database you can use a command similar to this:

```
Invoke-CsCdrDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

In the preceding command both call detail records and diagnostic data records older than 10 days are deleted from the monitoring database on atl-sql-001.litwareinc.com. (Call detail records are user/session reports. Diagnostic data records are diagnostic logs uploaded by client applications such as Lync 2013.)

As shown above, when you run the Invoke-CsCdrDatabasePurge cmdlet you must include both the PurgeCallDetaiDataOlderThanDays and the PurgeDiagnosticDataOlderThanDays parameters. However, these parameters do not have to be set to the same value. For example, it's possible to purge call detail records more than 10 days old and yet, at the same time, leave all the diagnostic data records in the database. To do that, set PurgeCallDetailDataOlderThanDays to 10 and PurgeDiagnosticDataOlderThanDays to 0. For example:

```
Invoke-CsCdrDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

By default, any time you run Invoke-CsCdrDatabasePurge you will see a prompt similar to this one for each database table that must be purged:

```
Confirm
Are you sure you want to perform this action?
Performing operation "Stored procedure: RtcCleanupDiag" on Target "Target SQL Ser
[Y] Yes  [A] Yes to All  [N] No  [L] No to All [S] Suspend  [?] Help (default is
```

You must type either Y (for Yes) or A (for Yes to All) before the database purging will actually take place. If you would prefer to suppress these confirmation prompts, add the following parameter to the end of your call to Invoke-CsCdrDatabasePurge:

```
-Confirm:$False
```

For example:

```
Invoke-CsCdrDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

If you do that, confirmation prompts will not be displayed, and database purging will immediately be performed.

To purge the QoE database, use the Invoke-CsQoEDatabasePurge cmdlet and specify the age (in days) of the records to be deleted:

```
Invoke-CsQoEDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

1.7.20.2 Quality of Experience (QoE)

Quality of Experience (QoE)

See Also

Microsoft Lync Server 2013 > Operations > Monitoring and Health Configuration >

Topic Last Modified: *2012-11-01*

Quality of Experience (QoE) records numeric data that indicates the media quality and information about participants, device names, drivers, IP addresses, and endpoint types involved in calls and sessions. When you install Lync Server 2013, you will also install a predefined collection of global configuration settings for QoE. Use the topics in this section to configure QoE settings.

- Create Quality of Experience Configuration Settings
- Enable Quality of Experience
- Modify Quality of Experience Settings
- Delete Quality of Experience Configuration Settings
- Manually Purging the Call Detail Recording and Quality of Experience Databases

⊟See Also

Concepts

Configuring Call Detail Recording and Quality of Experience Settings

1.7.20.2.1 Create Quality of Experience Configuration Settings

Create Quality of Experience Configuration Settings

Operations > Monitoring and Health Configuration > Quality of Experience (QoE) >

Topic Last Modified: *2013-02-23*

Quality of Experience (QoE) metrics track the quality of audio and video calls made in your organization, including such things as the number of network packets lost, background noise, and the amount of "jitter" (differences in packet delay). These metrics are stored in a database apart from other data (such as call detail records), which allows you to enable and disable QoE independent of other data recording.

When you install Microsoft Lync Server 2013, a single, global collection of QoE configuration settings is created for you. Administrators also have the option of creating custom settings at the site scope. Whenever these site-scoped settings are used, they take precedence over the global settings. For example, if you create site-scoped settings for the Redmond site then those settings (rather than the global settings) will be used to manage QoE in Redmond.

QoE configuration settings can be created by using either Lync Server Control Panel or the New-CsQoEConfiguration cmdlet. If you are using Lync Server Control Panel to create new settings the following options will be available to you:

UI Setting	PowerShell Parameter	Description
Name	Identity	Unique identifier for the settings to be created. QoE configuration settings can only be created at the site scope.
Enable monitoring of QoE data	EnableQoE	Specifies whether QoE records will be collected and saved to the monitoring database.
Enable purging of QoE data	EnablePurging	Specifies whether records will be purged after the duration defined in the **Keep QoE data for a maximum**

		duration (days) property has elapsed.
Keep QoE data for maximum duration (days)	KeepQoEDataForDays	Number of days QoE data will be stored before being purged from the database. This value is ignored if purging is disabled.

Note:

The New-CsQoEConfiguration cmdlet includes additional options not available in Lync Server Control Panel. For more information, see the New-CsQoEConfiguration help topic.

To create QoE configuration settings by using Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Quality of Experience Data**.
4. On the **Quality of Experience Data** page, click **New**.
5. In **Select a Site**, click the site to which the policy is to be applied, and click **OK**.
6. In **New Quality of Experience Setting**, do the following:
   - Select **Enable monitoring of QoE data** to turn on monitoring.
   - Select **Enable purging of QoE data** to turn on purging.
   - In **Keep QoE for maximum duration (days)**, select the maximum number of days that QoE records should be retained.
7. Click **Commit**.

Creating QoE Configuration Settings by Using Windows PowerShell Cmdlets

You can create QoE configuration settings by using Windows PowerShell and the New-CsQoEConfiguration cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To create a new collection of QoE configuration settings

- This command creates a new collection of QoE configuration settings applied to the Redmond site:

```
New-CsQoEConfiguration -Identity "site:Redmond"
```

To create a new collection of QoE configuration settings where QoE monitoring is disabled

- Because no parameters (other than the mandatory Identity parameter) were specified in the preceding command, the new collection of configuration settings will use the default values for all its properties. To create settings that use different property values, simply include the appropriate parameter and parameter value. For example, to create a collection of Quality of Experience configuration settings that, by default, allow disable QoE recording use a command like this:

```
New-CsQoEConfiguration -Identity "site:Redmond" -EnableQoE $False
```

To specify multiple property values when creating a new collection of QoE configuration settings

- You can multiple property values by including multiple parameters. For example, this command configures the new settings to keep QoE data for 30 days and to purge old data at 3:00 AM:

```
New-CsQoEConfiguration -Identity "site:Redmond" -KeepQoEDataForDays 30
```

For more information, see the help topic for the New-CsQoEConfiguration cmdlet.

1.7.20.2.2 Enable Quality of Experience

Enable Quality of Experience

See Also

Operations > Monitoring and Health Configuration > Quality of Experience (QoE) >

Topic Last Modified: *2013-02-23*

Quality of Experience (QoE) records numeric data that indicates the media quality and information about participants, device names, drivers, IP addresses, and endpoint types involved in calls and sessions. For details, see Planning for Monitoring in the Planning documentation.

Use the following procedure to enable QoE for your whole organization or each site in your organization.

> **Note:**
>
> To enable QoE, you must first configure monitoring and a monitoring back-end database. For details, see Deploying Monitoring.

To enable QoE by using Lync Server Control Panel

1. From a user account that is a member of the RTCUniversalServerAdmins group (or has equivalent user rights), or assigned to the CsServerAdministrator or CsAdministrator role, log on to any computer that is in the network in which you deployed Lync Server 2013.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Quality of Experience Data**.
4. On the **Quality of Experience Data** page, click the appropriate collection from the table, click **Action**, and then click **Enable QoE**.

Enabling QoE by Using Windows PowerShell Cmdlets

You can enable QoE by using Windows PowerShell and the **Set-CsQoEConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To enable QoE for a single location

- To enable QoE, set the EnableQoE parameter to True ($True).

```
Set-CsQoEConfiguration -Identity "site:Redmond" -EnableQoE $True
```

To disable QoE for a single location

- To disable QoE, set the EnableQoE parameter to False ($False). This does not uninstall monitoring. It pauses the collection and storage of QoE data.

```
Set-CsQoEConfiguration -Identity "site:Redmond" -EnableQoE $False
```

To use a single command to enable QoE in multiple locations

- This command enables QoE for all the QoE configuration settings currently in use in your organization.

```
Get-CsQoEConfiguration | Set-CsQoEConfiguration "site:Redmond" -EnableQ
```

For details, see Set-CsQoEConfiguration.

See Also

Other Resources

Planning for Monitoring
Deploying Monitoring

1.7.20.2.3 Modify Quality of Experience Settings

Modify Quality of Experience Settings

See Also

Operations > Monitoring and Health Configuration > Quality of Experience (QoE) >

Topic Last Modified: *2013-02-23*

By default, Quality of Experience (QoE) data is purged after 60 days. You can use the settings on the **Quality of Experience Data** page to retain the data for a longer or shorter period of time. If you disable QoE, data that was captured before QoE was enabled will also be subject to purging.

Note:

You should configure call detail recording (CDR) and QoE to retain data for the same number of days. Each call in the call detail reports (CDRs), available from the Monitoring Reports homepage, includes CDR and QoE information. If the purging duration for CDR and QoE is different, some calls may only include CDR data, while other may only include QoE data.

The following procedure describes how to configure purge settings for QoE data.

To specify retention of QoE data by using Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click

Quality of Experience Data.

4. On the **Quality of Experience Data** page, click the appropriate site from the table, click **Edit**, and then click **Show Details**.
5. To turn on purging, select **Enable Purging of QoE**.
6. In **Keep QoE for maximum duration (days)** select the maximum number of days that QoE data should be retained.
7. Click **Commit**.

Specifying QoE Retention by Using Windows PowerShell Cmdlets

You can create QoE retention settings by using Windows PowerShell and the **Set-CsQoEConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To specify QoE retention for a specific location

- This command enables purging of QoE data for the Redmond site, and configures the site to maintain QoE data for 20 days.

```
Set-CsQoeConfiguration -Identity "site:Redmond" -EnablePurging -KeepQoE
```

To specify QoE retention for multiple locations

- This command configures QoE retention for all the QoE configuration settings in use in an organization.

```
Get-CsQoEConfiguration | Set-CsQoEConfiguration-EnablePurging -KeepQoED
```

For more information, see the help topic for the Set-CsQoEConfiguration cmdlet.

See Also

Other Resources

Deploying Monitoring

1.7.20.2.4 Delete Quality of Experience Configuration Settings

Delete Quality of Experience Configuration Settings

Operations > Monitoring and Health Configuration > Quality of Experience (QoE) >

Topic Last Modified: *2013-02-23*

Quality of Experience (QoE) metrics track the quality of audio and video calls made in your organization, including such things as the number of network packets lost, background noise, and the amount of "jitter" (differences in packet delay). These metrics are stored in a database apart from other data (such as call detail records), which allows you to enable and disable QoE independent of other data recording.

When you install Microsoft Lync Server 2013, a single, global collection of QoE configuration settings is created for you. Administrators also have the option of creating custom setting collections that can be applied to individual sites. By design, settings configured at the site scope take precedence over settings configured at the global scope. If you delete site-scoped settings, then QoE will be managed in that site by using the global settings.

Note that you can also “delete” the global settings. However, the global settings will not actually be removed. Instead, all the properties in that collection will be reset to their default values. For example, by default purging is enabled in a collection of QoE configuration settings. Suppose you modify the global collection so that purging is disabled. If you later delete the global settings, all the properties will be reset to their default values. In this case, that means that purging will once again be enabled.

You can remove QoE configuration settings by using the Lync Server Control Panel or by using the Remove-CsQoEConfiguration cmdlet.

To delete QoE configuration settings by using Lync Server Control Panel

1. Log on to the computer as a member of the RTCUniversalServerAdmins group, or as a member of the CsVoiceAdministrator, CsServerAdministrator, or CsAdministrator role. For details, see Delegate Setup Permissions.
2. Open a browser window, and then enter the Admin URL to open the Lync Server Control Panel. For details about the different methods you can use to start Lync Server Control Panel, see Open Lync Server Administrative Tools.
3. In the left navigation bar, click **Monitoring and Archiving**, and then click **Quality of Experience Data**.
4. On the **Quality of Experience Data** page, click the policy that you want, click **Edit**, and then click **Delete**.
5. Click **OK**.

Removing QoE Configuration Settings by Using Windows PowerShell Cmdlets

You can delete QoE configuration settings by using Windows PowerShell and the **Remove-CsQoEConfiguration** cmdlet. You can run this cmdlet either from the Lync Server 2013 Management Shell or from a remote session of Windows PowerShell. For details about using remote Windows PowerShell to connect to Lync Server, see the Lync Server Windows PowerShell blog article "Quick Start: Managing Microsoft Lync Server 2010 Using Remote PowerShell" at http://go.microsoft.com/fwlink/p/?linkId=255876.

To remove a specified collection of QoE configuration settings

- This command removes the QoE configuration settings applied to the Redmond site:

```
Remove-CsQoEConfiguration -Identity "site:Redmond"
```

To remove all of the QoE configuration settings applied to the site scope

- This command removes all the QoE configuration settings applied to the site scope:

```
Get-CsQoEConfiguration -Filter "site:*" | Remove-CsQoEConfiguration
```

To remove all of the QoE configuration settings where QoE monitoring is disabled

- This command removes all the QoE configuration settings where QoE monitoring has been disabled:

```
Get-CsQoEConfiguration | Where-Object {$_.EnableQoE -eq $False} | Remov
```

For details, see Remove-CsQoEConfiguration.

1.7.20.2.5 Manually Purging the Call Detail Recording and Quality of Experience Databases

Manually Purging the Call Detail Recording and Quality of Experience Databases

Microsoft Lync Server 2013 > Deployment > Deploying Monitoring >

Topic Last Modified: *2012-11-01*

Administrators can configure the Call Detail Recording (CDR) and/or the Quality of Experience (QoE) databases to automatically purge old records from the database; this occurs if purging has been enabled for the specified database (CDR or QoE) and if there are any records that have been in the database longer than the specified amount of time. For example, every day at 1:00 AM administrators might configure the system so that QoE records more than 60 days old will be deleted from the QoE database.

In addition to that automatic purging, two new cmdlets -- Invoke-CsCdrDatabasePurge and Invoke-CsQoEDatbasePurge -- have been added to Microsoft Lync Server 2013; these cmdlets allow administrators to manually purge records from the CDR and the QoE databases at any time. For example, to manually purge all the records more than 10 days old from the CDR database you can use a command similar to this:

```
Invoke-CsCdrDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

In the preceding command both call detail records and diagnostic data records older than 10 days are deleted from the monitoring database on atl-sql-001.litwareinc.com. (Call detail records are user/session reports. Diagnostic data records are diagnostic logs uploaded by client applications such as Lync 2013.)

As shown above, when you run the Invoke-CsCdrDatabasePurge cmdlet you must include both the PurgeCallDetaiDataOlderThanDays and the PurgeDiagnosticDataOlderThanDays parameters. However, these parameters do not have to be set to the same value. For example, it's possible to purge call detail records more than 10 days old and yet, at the same time, leave all the diagnostic data records in the database. To do that, set PurgeCallDetailDataOlderThanDays to 10 and PurgeDiagnosticDataOlderThanDays to 0. For example:

```
Invoke-CsCdrDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

By default, any time you run Invoke-CsCdrDatabasePurge you will see a prompt similar to this one for each database table that must be purged:

```
Confirm
Are you sure you want to perform this action?
Performing operation "Stored procedure: RtcCleanupDiag" on Target "Target SQL Ser
[Y] Yes  [A] Yes to All  [N] No  [L] No to All [S] Suspend  [?] Help (default is
```

You must type either Y (for Yes) or A (for Yes to All) before the database purging will actually take place. If you would prefer to suppress these confirmation prompts, add the following parameter to the end of your call to Invoke-CsCdrDatabasePurge:

```
-Confirm:$False
```

For example:

```
Invoke-CsCdrDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

If you do that, confirmation prompts will not be displayed, and database purging will immediately be performed.

To purge the QoE database, use the Invoke-CsQoEDatabasePurge cmdlet and specify the age (in days) of the records to be deleted:

```
Invoke-CsQoEDatabasePurge -Identity MonitoringDatabase:atl-sql-001.litwareinc.com
```

1.7.20.3 Monitoring Mobility for Performance

Monitoring Mobility for Performance

Microsoft Lync Server 2013 > Operations > Monitoring and Health Configuration >

Topic Last Modified: *2013-02-14*

The Lync Server Mobility Service (Mcx) and the Unified Communications Web API (UCWA) increase the load on Front End Servers and Front End pools. Mobile devices that maintain a connection to the server even when the mobile application is minimized, such as Android and Nokia devices running Lync 2010 Mobile, as well as Android and Apple devices running Lync 2013 Mobile, impose a greater load than devices that terminate their connection to the server when the mobile application is minimized. As your mobility usage increases, you must monitor mobility performance to determine when you need to increase your capacity.

Several limits influence mobility performance:

- Available memory
- Request queue limit
- Concurrent connections
- IIS queue length

Other limits on servers that can influence mobility performance are a maximum of twelve concurrent sign-ins, authentications, session renewals, and terminations. These maximums do not need to be modified for most deployments.

- Monitoring for Server Memory Capacity Limits
- Monitoring Mobility Service and UCWA Usage
- Configuring Mobility Service for High Performance
- Monitoring IIS Request Tracing Log Files
- Mobility Performance Counters

1.7.20.3.1 Monitoring for Server Memory Capacity Limits

Monitoring for Server Memory Capacity Limits

See Also

Operations > Monitoring and Health Configuration > Monitoring Mobility for Performance >

Topic Last Modified: *2013-02-16*

```
Some information in this topic pertains to Cumulative Updates for Lync Server 201
```

> ⚠**Warning:**
> The information in this topic that refers to Capacity Planning pertains only to Lync 2010 Mobile clients and the Mobility Service (Mcx). Capacity Planning for the Unified Communications Web API (UCWA), used by the Lync 2013 Mobile clients, is provided by the Lync Server 2013, Planning Tool.

Two mobility performance counters can help you to determine your current usage and help you plan capacity for the Lync Server 2013 Mobility Service (Mcx), as well as to monitor memory usage for UCWA. For UCWA, the counter category is **LS:WEB – UCWA**.

For the Mobility Service (Mcx), the counters are under the category **LS:WEB - Mobile Communication Service**. The counters to monitor are:

- **Currently Active Session Count with Active Presence Subscriptions**, which is the current number of endpoints registered through UCWA or the Mobility Service (Mcx) that have active presence subscriptions (number of always-connected mobile users)
- **Currently Active Session Count**, which is the current number of endpoints registered through UCWA or the Mobility Service

If the difference between **Currently Active Session Count with Active Presence Subscriptions** and **Currently Active Session Count** is small over time, this means that most mobile device users have an always-connected device, such as an Android or Nokia mobile device (for Mcx only). UCWA always-connected devices include Apple and Android devices running Lync 2013 Mobile clients). If **Currently Active Session Count** is much higher than **Currently Active Session Count with Active Presence Subscriptions**, this indicates that more users are using a background endpoint device, such as an Apple iOS device or Windows Phone under Mcx. (Windows Phone is the only Lync 2013 Mobile client that will register as this).

You should set a limit on the **Currently Active Session Count with Active Presence Subscriptions** and **Currently Active Session Count** performance counters based on your expected usage, capacity planning results, and ongoing monitoring of Mobility Service and other Front End Server counters. The limits you set should enable you to evaluate server capacity and raise alerts when capacity is exceeded.

To determine the appropriate limits, you need to first determine how much memory is available on the Front End Server for the Mobility Service. Monitor the counters to determine when you need to plan for extra capacity, according to the following formula:

Total memory used by the Mcx Mobility Service (MB) = 164 + (400 + 134) / 1024 * **Currently Active Session Count with Active Presence Subscriptions** + 400 / 1024 * (**Currently Active Session Count** – **Currently Active Session Count with Active Presence Subscriptions**)

Important:

The Microsoft Lync Server 2010 Capacity Calculator is a spreadsheet that is prepopulated with all of the formulas that enable a planner to determine what the requirements will be for the servers, including CPU, memory, and hard drive. You can download the spreadsheet and an associated document at: http://go.microsoft.com/fwlink/p/?LinkID=212657

The Front End Server needs enough available memory to support the Mobility Service in failover situations. You can monitor the current available memory on the Front End Server by using the **Memory\Available Mbytes** counter, or by using the equation mentioned earlier, to plan for the amount of memory that you expect the Mobility Service to use.

If the amount of memory available on the Front End Server is lower than 1,500 MB when you plan for the expected number of mobility users, you need to add more hardware to support the Mobility Service. For more details, see Monitoring Mobility for Performance in the Operations documentation.

Other Resources

Monitoring Mobility for Performance

1.7.20.3.2 Monitoring Mobility Service and UCWA Usage

Monitoring Mobility Service and UCWA Usage

See Also

Operations > Monitoring and Health Configuration > Monitoring Mobility for Performance >

Topic Last Modified: *2013-02-14*

On an ongoing basis, you should monitor the CPU and memory that is used by the Lync Server Mobility Service (Mcx) and the Unified Communications Web API (UCWA). To monitor usage, you can use the following:

For Unified Communications Web API (UCWA):

- The **LyncUcwa** worker process in Internet Information Services (IIS) Manager. In the **Worker Processes** pane, look at the **CPU %** and **Private Bytes (KB)** (memory) columns.
- The **CPU** and **Processor** performance counters.

For most deployments, UCWA CPU usage should be below 15 percent on average. Memory usage should fall within the limits described in Monitoring for Server Memory Capacity Limits.

In addition to CPU and memory usage counters, you can use the following performance counters to help determine when a server is overloaded with requests:

- **LS:WEB – Throttling and Authentication\WEB – Total Requests in Processing**, which indicates the number of pending web requests on the server. When this counter reaches 10,000, subsequent requests will fail, with the error message, "503 - Service Unavailable."
- **ASP.NET\Requests Queued** (should always be zero).

Note:

If you meet or exceed these values, you should revisit and re-compute your capacity planning for the correct sizing of CPU, number of cores and memory for the computers hosting the Web services.

For the Mobility Service (Mcx):

- The **CSIntMcxAppPool** and **CSExtMcxAppPool** worker processes in Internet Information Services (IIS) Manager. In the **Worker Processes** pane, look at the **CPU %** and **Private Bytes (KB)** (memory) columns.
- The **CPU** and **Processor** performance counters.

For most deployments, Mobility Service CPU usage should be below 15 percent, on average. Memory usage should fall within the limits described in Monitoring for Server Memory Capacity Limits.

In addition to CPU and memory usage counters, you can use the following ASP.NET performance counters to help determine when a server is overloaded with requests:

- **ASP.NET v2.0.50727\Requests Current**, which indicates the number of pending web requests on the server. When this counter reaches 5,000, subsequent requests will fail with the error message, "503 - Service Unavailable."
- **ASP.NET\Requests Queued** (should always be zero).

Note:

If you meet or exceed these values, you should revisit and recompute your capacity planning for the correct sizing of CPU, number of cores, and memory for the computers hosting the Web services.

Concepts

Monitoring for Server Memory Capacity Limits

1.7.20.3.3 Monitoring IIS Request Tracing Log Files

Monitoring IIS Request Tracing Log Files

Operations > Monitoring and Health Configuration > Monitoring Mobility for Performance >

Topic Last Modified: *2013-02-14*

```
This topic applies to deployments supporting Lync 2010 Lync Mobile clients only,
```

When you enable Internet Information Services (IIS) request tracing for the Lync Server Mobility Service (Mcx), the log files that are generated can consume up to three gigabytes of disk space per day. IIS trace logging is enabled by default. You should monitor the Front End Servers to make sure that they do not run out of disk space.

By default, IIS stores the log files at %SystemDrive%\inetpub\logs\LogFiles.

To turn off IIS request tracing for an entire server, at the command line, type the following:

```
%SystemDrive%\Windows\System32\inetsrv\appcmd set config /section:httpLogging /do
```

For details about the **httpLogging** command, see http://go.microsoft.com/fwlink/p/?linkId=234927.

1.7.20.3.4 Configuring Mobility Service for High Performance

Configuring Mobility Service for High Performance

Operations > Monitoring and Health Configuration > Monitoring Mobility for Performance >

Topic Last Modified: *2013-02-17*

Important:

This topic applies only to the Lync Server 2013 Mobility Service (Mcx), and does not apply to Unified Communications Web API (UCWA), as delivered in the Cumulative Updates for Lync Server 2013: February 2013.

When you install the Mobility Service (Mcx) on Internet Information Services (IIS) 7.5, the Mobility Service installer configures some performance settings on the Front End Server. We recommend that you use IIS 7.5 for mobility. The settings affect the maximum number of concurrent user requests and the maximum number of threads that are allowed for the Mobility Service.

Here are the performance settings:

Settings for Mcx on IIS 7.5

1. **maxConcurrentThreadsPerCPU** is set to zero (0).
2. **maxConcurrentRequestsPerCPU** is set to zero (0).
3. ASP.NET process model is set to AutoConfig (for IIS 7.5 only).
4. HTTP.sys queue limit is set to 1,000 (by default).

Mobility Performance Counters

Operations > Monitoring and Health Configuration > Monitoring Mobility for Performance >

***Topic Last Modified:** 2013-02-22*

The following tables list the names and descriptions of performance counters that you can use to monitor servers running the Unified Communications Web API (UCWA) and the Lync Server 2013 Mcx Mobility Service.

The category name for the counters in the UCWA table is **LS:WEB – UCWA**.

The category name for the counters in the Mcx Mobility Service table is **LS:WEB - Mobile Communication Service**.

Performance Counters for UCWA

Counter	Description
Active Application Count	The current number of applications
Active Application Sharing Modality Count	The current number of Application Sharing modality
Active Audio Modality Count	The current number of Audio modality
Active Data Collaboration Modality Count	The current number of Data Collaboration modality
Active Directory Photo Get Latency (ms)	This counter shows the average time (in milliseconds) to retrieve a photo from active directory
Active Messaging Modality Count	The current number of Messaging modality
Active Panoramic Video Modality Count	The current number of Panoramic Video modality
Active Pending Get Count	The number of currently active pending gets; long-held connections to the server
Active Session Count	The current number of endpoints registered in UCWA per application and total
Active User Instance Count	The current number of user instances
Active User Instances without Application	The current number of user instances without application
Active Video Modality Count	The current number of Video modality
Application Creation Requests Received/ Second	The per second rate of received application creation requests
AS MCU Join Failures	The number of AS MCU Join Failures
AV MCU Join Failures	The number of AV MCU Join Failures
Average Application Startup Time (ms)	The average application startup time in Milliseconds

Average Lifetime for Session (ms)	The average lifetime for a session in milliseconds
Data MCU Join Failures	The number of Data MCU Join Failures
Exchange Contact Search Latency (ms)	This counter shows the average time (in milliseconds) to search contact in Exchange
Exchange HD Photo Get Latency (ms)	This counter shows the average time (in milliseconds) to retrieve a photo from Exchange
HTTP 4xx Responses/Second	The per second rate of responses with HTTP 4xx code
HTTP 5xx Responses/Second	The per second rate of responses with HTTP 5xx code
IM MCU Join Failures	The number of IM MCU Join Failures
Number of Active Directory Photo Get Failures	The total number of failures to retrieve photos from Active Directory
Number of Contact Search failures	The total number of failures to search contacts in Exchange
Number of Deserialization Failures	The total number of deserialization failures
Number of HD Photo Get Failures	The total number of failures to retrieve HD photos from Exchange
Over The Maximum Subscriptions Per Application	The number of Subscription requests over the maximum allowed per application
Over The Maximum Subscriptions Per Batch	The number of Subscription requests over the maximum allowed per batch
Presence Subscription Failures	The number of failures to subscribe presence
Registering Endpoint Failures	The number of failures to register endpoints
Requests Received/Second	The per second rate of received requests
Requests Succeeded/Second	The per second rate of successful requests (HTTP 2xx/3xx response codes)
Succeeded Create Application Requests/ Second	The per second rate of successful application creation requests
Timed Out Pending Get Count	The number of pending gets that timed out
Total Application Creation Requests Received	The total number of application creation requests received since the service was started
Total HTTP 4xx Responses	The total number of HTTP 4xx responses
Total HTTP 5xx Responses	The total number of HTTP 5xx responses
Total Requests Received on the Command Channel	The total number of requests received on the command channel
Total Requests Succeeded	The total number of requests that

	succeeded
Total Sessions Initiated	The total number of sessions that were initiated since the service was started
Total Sessions Terminated Because of Idle Timeout	The total number of sessions that were terminated because of user idle timeout
Total Throttled Applications	The number of throttled applications

Performance Counters for Mcx Mobility Service

Counter	Description
Average Lifetime for a Session in Milliseconds	The average lifetime for a session in milliseconds
Current Push Notification Subscriptions	The current number of push notification subscriptions. This number, in conjunction with Currently Active Session Count, represents the subset of currently active sessions that are registered for Windows Mobile or iPhone devices.
Currently Active Network Timeout Poll Count	The number of network polls that timed out
Currently Active Poll Count	The number of currently active polls (long-held connections to the server)
Currently Active Session Count	Current number of endpoints registered in the Mobility Service
Currently Active Session Count with Active Presence Subscriptions	The number of currently active sessions with active presence subscriptions
Push Notification Requests Failed/Second	The per second rate of failed push notifications
Push Notification Requests Succeeded/Second	The per second rate of successful push notifications
Push Notification Requests Throttled/Second	The per second rate of throttled push notifications
Push Notification Requests/Second	The per second rate of sent push notifications
Requests Failed/Second	The per second rate of failed requests
Requests Received/Second	The per second rate of received requests
Requests Rejected/Second	The per second rate of rejected requests
Requests Succeeded/Second	The per second rate of successful requests
Succeeded Initiate Session Requests/Second	The per second rate of successful Get Location requests. Requests to initiate a session consume the most CPU on the server. Peak supported load is 12/second. Sustainability depends on other loads on the server. Initiate a session typically means a sign-in for a user that has been signed out for an extended period of time.

Total Declined Inbound Voice Calls	The total number of inbound voice calls that were declined
Total Failed Inbound Voice Calls	The total number of inbound voice calls that failed
Total Failed Outbound Voice Calls	The total number of outbound voice calls that failed
Total number of sessions terminated by user	The total number of sessions terminated by users
Total Push Notification Requests	The total number of push notification requests
Total Push Notification Requests Failed	The total number of push notification requests that failed
Total Push Notification Requests Succeeded	The total number of push notification requests that were successful
Total Push Notification Requests Throttled	The total number of push notification requests that were throttled
Total Requests Failed	The total number of requests that failed
Total Requests received on the Command Channel	The total number of requests received on the command channel
Total Requests Rejected	The total number of requests that were rejected
Total Requests Succeeded	The total number of requests made to the Mobility Service that succeeded
Total Session Initiated Count	The total number of sessions that were initiated since the Mobility Service was started
Total Sessions Terminated Because of User Idle Timeout	The total number of sessions that were terminated because of user idle timeout
Total Successful Inbound Voice Calls	The total number of inbound voice calls that were successful
Total Successful Outbound Voice Calls	The total number of outbound voice calls that were successful

1.7.20.3.6 UCWA Events

UCWA Events

Operations > Monitoring and Health Configuration > Monitoring Mobility for Performance >

Topic Last Modified: *2013-02-15*

`The information in this topic pertains to Cumulative Updates for Lync Server 2013`

Lync Server 2013 uses the Unified Communications Web API (UCWA) for a number of purposes, from accessing Microsoft Exchange for contact searches to updating presence for mobile clients.

UCWA will write records of operational behavior as event types Informational, Warning, and Error. The following table describes the events that can be written by the UCWA components.

Event ID	Event Type	Summary	Cause and Resolution
20001	Informational	UCWA initialized	N/A N/A
20002	Error	UCWA encountered an unexpected exception during initialization	An unexpected error has occurred during initialization Examine the exception details in the associated event log entry to determine the possible cause
20003	Error	UCWA encountered an unhandled exception	An unhandled exception happened Restart the server. If the problem persists contact product support
20004	Error	Cannot access Exchange for HD photo	Connection to Exchange is not available Make sure the connection to Exchange is available
20005	Informational	Recovered from failing to access Exchange for HD photo	N/A
20006	Error	Cannot access Exchange for contact search	Connection to Exchange is not available Make sure the connection to Exchange is available
20007	Informational	Recovered from failing to search contact in Exchange	N/A
20008	Warning	Attempt to subscribe more than the allowed presence subscriptions per application	Attempt to subscribe more than the allowed presence subscriptions per application Check the clients for

			unnecessary subscriptions
20009	Warning	Attempt to subscribe more than the allowed presence subscriptions per batch	Attempt to subscribe more than the allowed presence subscriptions per batch Check the clients for unnecessary subscriptions
20010	Error	Cannot retrieve inband data	Cannot retrieve inband data If the problem persists contact product support
20011	Error	Cannot subscribe presence	Cannot subscribe presence If the problem persists contact product support
20012	Error	Failed to register endpoint	Failed to register endpoint If the problem persists contact product support
20013	Error	IM MCU is unavailable	IM MCU is unavailable See whether IM MCU is running
20014	Informational	Recovered from failing to connect to IM MCU	N/A
20015	Error	AV MCU is unavailable	AV MCU is unavailable See whether AV MCU is running
20016	Informational	Recovered from failing to connect to AV MCU	N/A
20017	Error	AS MCU is unavailable	AS MCU is unavailable See whether AS MCU is running
20018	Informational	Recovered from failing to connect to AS MCU	N/A
20019	Error	Data MCU is unavailable	Data MCU is unavailable

			See whether Data MCU is running
20020	Informational	Recovered from failing to connect to Data MCU	N/A
20021	Error	Cannot join IM MCU	Cannot join IM MCU See whether IM MCU is running
20022	Error	Cannot join AV MCU	Cannot join AV MCU See whether AV MCU is running
20023	Error	Cannot join AS MCU	Cannot join AS MCU See whether AS MCU is running
20024	Error	Cannot join Data MCU	Cannot join Data MCU See whether Data MCU is running
20025	Error	Cannot access active directory for photo	Connection to active directory is not available Make sure the connection to active directory is available
20026	Informational	Recovered from failing to access active directory for photo	N/A
20027	Warning	Cannot deserialize	Cannot deserialize If the problem persists contact product support

1.7.20.4 Using Monitoring Reports

Using Monitoring Reports

Microsoft Lync Server 2013 > Operations > Monitoring and Health Configuration >

Topic Last Modified: *2012-10-21*

Lync Server 2013 includes a set of standard reports that are published by Microsoft SQL Server Reporting Service. These reports, which are accessible by using a web browser, provide usage, call diagnostic information, and media quality information, all based on call detail recording (CDR) and Quality of Experience (QoE) records stored in the CDR and QoE databases.

In order to use these reports, you must install Monitoring Reports on a computer that is running an instance of the SQL Server.

In This Section

- Using the Monitoring Dashboard Provides administrators with a quick overview of their system health and system usage.
- System Usage Reports Provides system usage information based on CDR data collected by Lync Server.
- Call Diagnostic Reports (per user) Provides per-user information about failed peer-to-peer and conferencing sessions.
- Call Diagnostic Reports Provides summary information and diagnostic data for failed peer-to-peer and conferencing sessions.
- Media Quality Diagnostic Reports Provides information about call quality as well as diagnostic and troubleshooting information for failed calls.

Locating Records

Monitoring Reports only show a limited number of records on the screen at any one time. The actual number of records displayed on a screen varies depending on the report. To view the records that are not currently shown on the screen you can use the standard forward and backward control (found on each report’s toolbar) that enable you to page through the data. You can also quickly jump to the first page or the last page of the dataset.

In addition to using the forward and backward controls, you can also jump to any page in the dataset simply by typing the page number in the **Current Page** box, and then press ENTER.

In addition to providing the ability to page through the data, each report also includes the limited ability to find records. To find records based on a given value, type that value into the **Find** box, and then click **Find**. The report begins searching through the data and stops on the first instance of the value that you entered in the **Find** box. To find the next record that meets the search criteria, click **Next**.

As noted, the Monitoring Reports provide only the most basic search functions. For example, you cannot specify which field the value should be found in. The search mechanism automatically searches for matching values in every field in every record. You cannot use wildcards in your searches, and all searches look for partial values. That means that if you search for 111 the search returns the value 111 along with the values 11100, 811, 3112, 611A5B, and any other fields that include the value 111 anywhere within that field.

Each report is configured to show a default set of records. For example, by default the User Registration Report shows user registration activities for the past week. In some cases, this might result in a report that returns no records. In this case, it means that no user registrations have taken place in the past week. If you see the message “No results match the report filters,” try changing the filter values (for example, change the time period to the past month rather than the past week) and rerun the query. For details, see the "Filtering Data" section later in this topic.

Filtering Data

There will likely be times when you want to look at only a subset of records. For example, only peer-to-peer sessions as opposed to both peer-to-peer sessions and conference sessions. Likewise, there will be times when you need to reduce the number of records that are returned. By default, a report can only display the first 1,000 records in a data set. To address these issues, most reports include a number of filtering options. For example, if you want to view only records for the time period January 1, 2011 through January 15, 2011, you can enter January 1, 2011 in the **From** box and January 15, 2011 in the **To** box. If you then click **View Report**, the returned data will be limited to activities that took place between January 1, 2011 and January 15, 2011.

The filters available to you vary depending on the report that you are viewing. For details about a specific report, see the help topic for that report.

Exporting Data

The Monitoring Reports provide at least two different ways to export the data included in a report. You can use the **Export** option in the toolbar that appears at the top of each report. To use this option, select the desired export format from the **Select a format** drop-down list. The following formats are available to you:

- XML file with report data
- CSV (comma delimited)
- Acrobat (PDF) file
- MHTML (web archive)
- Excel
- TIFF file
- Word

After selecting a format, click **Export**. When the **File Download** dialog box appears, click **Save**. In the **Save As** dialog box, select a destination folder, enter a file name, and then click **Save**.

If you have Microsoft OneNote installed, you can also copy the report data to OneNote. To do this, right-click the **View Report** button on the toolbar. In the **Select Location in OneNote** dialog box select the section in OneNote where you want to copy the data, and then click **OK**.

1.7.20.4.1 Using the Monitoring Dashboard

Using the Monitoring Dashboard

Operations > Monitoring and Health Configuration > Using Monitoring Reports >

Topic Last Modified: *2012-10-21*

The Monitoring Dashboard provides administrators with a quick overview of their Microsoft Lync Server 2013 system health and system usage. The Dashboard is designed to show an aggregate view of key system metrics and to do so by displaying either:

- Totals for the current day. Note that values shown for the current day represent data that has been recorded from midnight until the current time (based on the local time of the reporting server). That means that you will typically be viewing data for a partial day and not for a 24-hour period. For example, if the local time of the server is 8:00 AM, you see eight hours’ worth of data because there are eight hours between midnight and the current time of 8:00 AM.
- Totals for the week, and trend totals for the past six weeks.
- Totals for the month, and trend totals for the past six months (for system usage only).

By default, the Monitoring Dashboard shows data for the following metrics for the current week (and trend totals for the previous six weeks):

System Usage Metrics

Registration

- Unique user logons

Peer-to-peer

- Total sessions
- IM sessions
- Audio sessions
- Video sessions
- Application sharing
- Total audio session minutes
- Avg. audio session minutes

Conference

- Total conferences
- IM conferences
- A/V conferences
- Application sharing conferences
- Web conferences
- Total organizers
- Total A/V conference minutes
- Avg. A/V conference minutes
- Total PSTN conferences
- Total PSTN participants
- Total PSTN participant minutes

In addition to the System Usage metrics, the following metrics displays total for the current day and the previous six days (if you select **Weekly View**) or for the current week and the past six weeks if you select **Monthly View**.

Per-User Call Diagnostics

Users with call failures

- Total users with call failures
- Conference organizers with call failures

Users with poor quality calls

- Total users with poor quality calls

Call Diagnostics

Peer-to-peer

- Total failures
- Overall failure rate
- IM failure rate
- Audio failure rate
- Application sharing failure rate

Conference

- Total failures
- Overall failure rate
- IM failure rate
- A/V failure rate
- Application sharing failure rate

Top five servers by failed sessions

Media Quality Diagnostics

Peer-to-peer

- Total poor quality calls
- Poor quality call percentage
- PSTN calls with poor quality

Conference

- Total poor quality calls
- Poor quality call percentage
- PSTN calls with poor quality

Top worst servers by poor quality call percentage

Working with the Monitoring Dashboard

As noted, by default totals are shown for the current week and trend values are shown for the past six weeks. If you would prefer to see totals for the current month (as well as trend values for the past six months), click the **Monthly View** link in the upper right corner of the dashboard. If you decide to view monthly totals, the link text will change to **Weekly View**. You can switch back to the weekly view by clicking that link.

Tip:

The Monitoring Dashboard restricts you to looking at totals for the current week (or month) and trend values for the past six weeks (or months). You cannot change these dates and times. For example, you cannot use the Dashboard to view report totals for the time period beginning nine months ago.

The values shown in the **This week**, **This month**, or **Today** columns link you to more detailed information about the item. Keep in mind that the column name and the values displayed in that column will often differ depending on the metric chosen and depending on whether you have selected weekly view or monthly view. For example, if you click the totals shown for the **Unique user logons** metric you will see the **User Registration Report** for the specified time period. You can return to the Monitoring Dashboard at any time by clicking **Dashboard**.

Tip:

You can also access the Monitoring Server Reports home page by clicking the **Reports** link in the upper right corner of the Dashboard.

The **Trend** column displays a simple line graph that shows totals for the past six weeks (or, depending on the metric and the time interval, the past six days or the past six months). These simple line graphs display one unlabeled data point for each time period (for example, one unlabeled data point for each of the past six weeks). However, you can retrieve actual values for these graphs by holding your mouse pointer over the graph. In that case, a tooltip shows you the maximum and minimum values in the graph.

Exporting Data from the Monitoring Dashboard

The Monitoring Dashboard provides a number of ways to export the current dashboard view. On the Dashboard toolbar, you'll see an icon that looks like a floppy disk with a green arrow attached to it. If you click this icon, a dropdown list will appear giving you the following data export formats:

- XML file with report data
- CSV (comma delimited)
- PDF
- MHTML (web archive)
- Excel
- TIFF file
- Word

To export the current dashboard view (and its values), click the desired export option. Lync Server 2013 generates a report in the specified format and then give you the option of opening that report or saving it. Note that, by default, Lync Server titles the report **Monitoring Dashboard** and saves it to your Downloads folder. To give the report a different name or to store it in a different folder, click the arrow next to the **Save** button and then click **Save As**. If you are fine with name **Monitoring Dashboard** and with having the report saved in the Downloads folder you can just click the **Save** button.

It's possible that, when you try to export dashboard data, a **Security Alert** dialog box will appear along with the message "Your current settings do not allow this file to be downloaded." If that occurs, do the following:

- In Internet Explorer, select **Internet Options**.
- In the **Internet Options** dialog box, on the **Security** tab, click **Trusted sites** and then click **Sites**.
- In the **Trusted sites** dialog box, click **Add** to add the Lync Server 2013 that is running Lync Server 2013 Reports to the collections of trusted websites.
- Click **Close** and then click **OK**.

You will then need to refresh the Monitoring Dashboard before the changes take effect. To do that, either press F5 or click the **Refresh** icon in the Dashboard toolbar. (The **Refresh** icon is a circle with a pair of green arrows in it.)

You can also create an Excel spreadsheet that includes live data feeds, which includes links to the latest Monitoring Dashboard data. To create a live data feed file, click the orange **Export to Data Feed** icon in the toolbar.

If you would prefer to print the current Dashboard then click the printer icon in the toolbar.

1.7.20.4.2 System Usage Reports

System Usage Reports

Operations > Monitoring and Health Configuration > Using Monitoring Reports >

Topic Last Modified: *2012-10-21*

The System Usage Reports provide system usage information based on call detail recording (CDR) data collected by the Lync Server.

- User Registration Report
  Provides a summary of user connectivity to the Lync Server 2013 deployment based on registration events such as user logons. The report provides a way to view both internal and external logons, and to compare the number of users who logged on to Lync Server 2013 with the number of users who actually used the service while they were logged on.
- Peer-to-Peer Activity Summary Report
  Provides a summary of peer-to-peer instant messaging (IM), audio, video, file transfer, and application sharing sessions. Peer-to-peer sessions are sessions involving just two users.
- Conference Summary Report

Provides a summary of all conference activities. Conferences are sessions involving three or more people.

- PSTN Conference Summary Report
  Provides a summary of all PSTN conferences. These are conferences where at least one user dials in using the public switched telephone network (PSTN), which is also referred to as *dial-in conferencing*.
- Response Group Usage Report
  Provides a summary of Response Group usage. The Response Group application provides a way for you to automatically route phone calls to entities such as a help desk or customer support line.
- IP Phone Inventory Report
  Provides information about the IP phones currently in use in the organization. The report is based on phone registrations and logons. It should not be considered a complete inventory. For example, you might have removed phones that are still listed in the report because they logged on at least once. Likewise, you might also have new phones that do not show up in the report simply because users have not logged on to Lync Server with their new phones yet.
- Call Admission Control Report
  Provides a list of peer-to-peer and conference activities that use call admission control. Call admission control (CAC) is a way of determining whether you should allow real-time communications sessions, such as voice or video calls, based on bandwidth constraints.

1.7.20.4.2.1 User Registration Report

User Registration Report

Monitoring and Health Configuration > Using Monitoring Reports > System Usage Reports >

***Topic Last Modified:** 2012-10-21*

The User Registration Report provides an overview of user logon activity, most notably information about the number of users who logged on to Microsoft Lync Server 2013 during a specified time period (hourly, daily, weekly, monthly). Keep in mind that the report only tells you how many people logged on. It does not tell you *which* people logged on. Monitoring Reports do not provide information about which specific users are using Lync Server 2013 (and which ones are not). However, you can get a rough estimate of user information by using the User Activity Report.

When providing information about user logons, the User Registration Report draws two important distinctions. First, it breaks logons down into two primary categories: internal logons and external logons. Internal logons represent users who logged on from inside your organization's firewall (that is, while connected to the corporate network). External logons represent users who logged on from outside the firewall through an Edge Server (for example, a user who logged on from an Internet café counts as an external logon). If you need to know how many of your users are logging on from outside the firewall, the User Registration Report can provide you with this information.

In addition, the User Registration Report notes how many *active* users were present during a given time period. An active user is a user who took part in an instant messaging (IM) session, participated in a Lync Meeting, made or received a phone call, or otherwise used Lync Server during that period of time. This is different from a user who logged on, but never actually used the system.

Accessing the User Registration Report

You access the User Registration Report only from the Monitoring Reports home page. The User Registration Report does not link to any other reports.

Making the Best Use of the User Registration Report

After you've deployed Lync Server one commonly-asked question is this: How do I know if my users are actually using this new technology? Although it has a few limitations in this regard, the User Registration Report can help you answer this question. To determine whether or not users are using Lync Server, you need to do two things. First, get the value of the Unique logon users metric from the User Registration Report. This value tells you how many distinct individuals logged on to Lync Server.

By comparison, the Total logons metric shows how many total times anyone logged on to Lync Server. For example, suppose Ken Myer logged on to Lync Server five different times in a single day. In that case, Ken Myer would count as five separate logon sessions for the Total logons metric, but just one logon user for the Unique logon users metric. Likewise, it's not uncommon for a user to log on from multiple devices or multiple locations. For example, a user can log on using her desktop computer, her laptop computer, and she can have an IP phone that automatically logs on to Lync Server. In this example, there is one unique user with three logons.

To further explain the difference between total logons and unique logons, consider the logons for a given time period in the following table.

User	Logon time
Ken Myer	7/7/2012 8:45 AM
Ken Myer	7/7/2012 8:46 AM
Pilar Ackerman	7/7/2012 9:17 AM
Ken Myer	7/7/2012 9:22 AM
Pilar Ackerman	7/7/2012 9:31 AM

Notice that there is a total of five logons; however, there are only two unique logon users: Ken Myer (who logged on three times) and Pilar Ackerman (who logged on twice). That's the difference between logons and unique logon users.

In addition to knowing the number of unique logons, you need to know the total number of users who have been enabled for Lync Server. That value can be retrieved by opening the Lync Server 2013 Management Shell and running the following Windows PowerShell command:

```
(Get-CsUser).Count
```

If the preceding command returns a value of 1,236 and Unique logon users metric returns an average value of 667, that suggests that a little over half of your users enable for Lync are actually logging on to the system each day (that is, 667 divided by 1,236, which is approximately 54%).

⚠Warning:

Keep in mind that the logon metrics record users who actually logged on during the specified time period. They don't keep track of users who were already logged on to the system. For example, if your Unique logon users metric shows 667 logons and you have 1,236 users, that suggests that about half your users are logging on to the system. However, suppose 300 users were already logged on to the system at the time you began checking the logon data. That would mean that you actually had nearly 1,000 users logged on to Lync Server, which would mean that closer to 80% of your users were logged on.

You should also compare the Unique logon users value with the value of the Unique active users metric. The Unique active users metric tells you how many unique users actually used Lync Server: they made a phone call, they joined a Lync Meeting, or they participated in an IM session. This is useful information, because Microsoft Lync 2013 can be configured to automatically start each time a user starts Windows. Because of that, you might have a large number of users who automatically log on to Lync when they log on to Windows each day, but then never actually use Lync Server during that time period.

The Unique active users metric also provides more meaningful data in an organization where users typically do not log off Windows at the end of the day. Instead, they simply lock their computers and leave Windows and Lync running. In a situation like that, you might end up with very few logons per day because your users logged on several days ago and never logged off. However, Unique active users tells you whether users are actively using Lync or another Lync Server client.

Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. For example, the User Registration Report enables you to view data for all your Registrar pool and Edge Servers or to view data for an individual pool. You can also choose how data should be grouped. In this case, registrations grouped by hour, day, week, or month.

The following table lists the filters that you can use with the User Registration Report.

User Registration Report Filters

Name	Description
From	Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date and time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date:

	7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) are displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or choose **[All]** to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.

Metrics

The following table lists the information provided in the User Registration Report.

User Registration Report Metrics

Name	Can you sort on this item?	Description
Hourly **Daily** **Weekly** **Monthly**	No	Indicates the time interval that you selected on the filter toolbar. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/7/2012, you see an hourly breakdown of user registration activity for that date.

Total logons	No	Total number of successful logon sessions.
Internal logons	No	Total number of logons within the internal network.
External logons	No	Total number of logons from outside the internal network, using the Edge Server.
Unique logon users	No	Total number of users who had at least one logon session. A user who had multiple logon sessions counts as one user, the same as a person who had just a single logon session.
Unique active users	No	Total number of users who were involved in a peer-to-peer or conferencing session. A user who had multiple sessions counts as one user, the same as a person who had just a single session.

1.7.20.4.2.2 Peer-to-Peer Activity Summary Report

Peer-to-Peer Activity Summary Report

Monitoring and Health Configuration > Using Monitoring Reports > System Usage Reports >

***Topic Last Modified:** 2012-10-21*

The Peer-to-Peer Activity Summary Report provides an overall view of your peer-to-peer communication sessions. A peer-to-peer session typically involves just two users, and does not require the use of the Lync Server conferencing services. By comparison, a conference typically involves more than two users and requires the use of Microsoft Lync Server 2013 conferencing services. Conference activity is reported on the Conference Summary Report.

The Peer-to-Peer Activity Summary Report helps you answer questions like the following:

- How many peer-to-peer instant messages do my users send on a typical day?
- Are any of my users actually taking advantage of the Lync Server application sharing and file transfer capabilities?
- Users have been complaining that the network seems slow at certain times of the day. How many minutes are devoted to peer-to-peer audio and video sessions during those time periods?

Accessing the Peer-to-Peer Activity Summary Report

You access the Peer-to-Peer Activity Summary Report from the Monitoring Reports home page. You open the Peer-to-Peer IM Report by clicking either of the following metrics:

- Total peer-to-peer IM sessions
- Total peer-to-peer IM messages

Likewise, you can open the Peer-to-Peer Voice and Video Report by clicking any of these metrics:

- Total peer-to-peer audio sessions
- Total peer-to-peer audio session minutes
- Total peer-to-peer audio sessions
- Total peer-to-peer audio session minutes

Making the Best Use of the Peer-to-Peer Activity Summary Report

At the bottom of the Peer-to-Peer Activity Summary Report you'll find totals for metrics such as Total peer-to-peer IM sessions and Total peer-to-peer IM messages. This provides a quick summary of the detailed information found in the body of the report.

Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. For example, the Peer-to-Peer Activity Summary Report enables you to choose how data should be grouped. In this case, activity grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Peer-to-Peer Activity Summary Report.

Peer-to-Peer Activity Summary Report Filters

Name	Description
From	Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/17/12012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/12012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2012 Weeks always run from Sunday through Saturday.
To	End date and time for the time range. To view data by hours, enter both the end date and time as follows: 7/17/12012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date:

	7/17/12012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/17/12012 and an end date of 2/28/2012, data is displayed for the days 8/7/12012 12:00 AM to 9/7/12012 12:00 AM (that is, a total of 31 days' worth of data).

Metrics

The following table lists the information provided in the Peer-to-Peer Activity Summary Report.

Peer-to-Peer Activity Summary Report Metrics

Name	Can you sort on this item?	Description
Hourly **Daily** **Weekly** **Monthly**	No	Indicates the time interval that you selected on the filter toolbar. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/17/12012, you see an hourly breakdown of user registration activity for that date.
Total peer-to-peer sessions	No	Total number of peer-to-peer sessions conducted, regardless of session type.
Total peer-to-peer IM	No	Total number of peer-to-peer

sessions		instant messaging (IM) sessions. When you click this item, the report shows you the Peer-to-Peer IM Report for the selected time period.
Total peer-to-peer IM messages	No	Total number of instant messages sent in peer-to-peer sessions. When you click this item, the report shows you the Peer-to-Peer IM Report for the selected time period.
Total peer-to-peer audio sessions	No	Total number of peer-to-peer audio calls. When you click this field, the report shows you the Peer-to-Peer Voice and Video Report for the selected time period.
Total peer-to-peer audio session minutes	No	Total amount of time spent in peer-to-peer audio sessions. When you click this item, the report shows you the Peer-to-Peer Voice and Video Report for the selected time period.
Average peer-to-peer audio session minutes	No	Average amount of time spent in peer-to-peer audio sessions. Calculated by dividing the total audio session time by the total number of audio sessions.
Total peer-to-peer video sessions	No	Total number of peer-to-peer video calls. Note that video sessions are also counted as audio sessions: each video session is counted as one video session and one audio session. When you click this item, the report shows you the Peer-to-Peer Voice and Video Report for the selected time period.
Total peer-to-peer video session minutes	No	Total amount of time spent in peer-to-peer video sessions. When you click this item, the report shows you the Peer-to-Peer Voice and Video Report for the selected time period.
Average peer-to-peer video session minutes	No	Average amount of time spent in peer-to-peer video sessions. Calculated by dividing the total video

		session time by the total number of video sessions.
Total peer-to-peer file transfer sessions	No	Total number of peer-to-peer sessions that included file transfers.
Total peer-to-peer application sharing sessions	No	Total number of peer-to-peer sessions that included application sharing.

Peer-to-Peer IM Report

Using Monitoring Reports > System Usage Reports > Peer-to-Peer Activity Summary Report >

Topic Last Modified: *2012-11-01*

The Peer-to-Peer IM Report provides trend information about peer-to-peer instant messaging (IM) sessions, broken down by pool and by authentication type. The report can show either the total number of sessions held during the specified time period (for example, day-by-day or hour-by-hour), or it can show the total number of instant messages sent during that time period.

Accessing the Peer-to-Peer IM Report

You can access the Peer-to-Peer IM Report only by opening the Peer-to-Peer Activity Summary Report and then clicking either of the following metrics:

- Total peer-to-peer IM sessions
- Total peer-to-peer IM messages

Making the Best Use of the Peer-to-Peer IM Report

By default, the Peer-to-Peer IM Report shows you the message count per-hour (or day, depending on your settings). However, you can also choose to view the day by sessions per hour. To do that, click **Hide/Show Parameters** in the upper-right corner of the Reports window, and then click **Session Count** from the **Report by** list.

Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Peer-to-Peer IM Report.

Peer-to-Peer IM Report Filters

Name	Description
From	Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified

	day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date and time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval then only the maximum number of values (starting from the start date) are displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Report by	Indicates the values to be used in the report. Select one of the following: • Session count • Message count

Metrics for Peer-to-Peer IM Session by Pool

The following table lists the information provided in the Peer-to-Peer IM Report.

Metrics for Peer-to-Peer IM Session by Pool

Name	Can you sort on this item?	Description
Pool	No	Name of the Registrar pool or Edge Server.
Date/Time	No	Date and time that the sessions took place.
Total	No	Total number of sessions or total message count.

Metrics for Peer-to-Peer IM Session by Authentication Type

The following table lists the information provided in the Peer-to-Peer IM Report for each type of authentication used by the participants in a peer-to-peer session.

Metrics for Peer-to-Peer IM Session by Authentication Type

Name	Can you sort on this item?	Description
Authentication type	No	Type of authentication used by the session participants. Values are typically one of the following: • Enterprise • Federated • PIC
Date/Time	No	Date and time that the sessions took place.
Total	No	Total number of sessions or total message count.

Peer-to-Peer Voice and Video Report

Using Monitoring Reports > System Usage Reports > Peer-to-Peer Activity Summary Report >

Topic Last Modified: *2012-10-21*

The Peer-to-Peer Voice and Video Report provides a detailed look at the distribution of voice and video calls over a specified period of time (for example, calls per hour or calls per day). The report also gives you the option of viewing all the voice and video calls that were made, or of viewing only the successful or failed calls. The reports shows call information broken down into the following groupings:

- Calls per pool
- Calls per call type (for example, a Lync to Lync call vs. a Lync call to a person on the PSTN network)

- Calls per access type (users logged on to the internal network vs. users logged on to the external network)
- Calls per Mediation Server

To access the peer-to-peer voice and video report

You can access the Peer-to-Peer Voice and Video Report only by opening the Peer-to-Peer Activity Summary Report and then clicking any of the following metrics:

- Total peer-to-peer audio sessions
- Total peer-to-peer audio minutes
- Total peer-to-peer video sessions
- Total peer-to-peer video minutes

To make the best use of the peer-to-peer voice and video report

There are a number of ways you can filter the Peer-to-Peer Voice and Video Report. However, those filtering options are hidden from view by default. To view the filtering options available to you, click **Show/Hide Parameters** button in the upper-right corner of the Report window.

Filters

Filters provide a way for you to return a more finely targeted set of data or to view the data in different ways. The following table lists the filters that you can use with the Peer-to-Peer Voice and Video Report.

Peer-to-peer voice and video report filters

Name	Description
From	Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows:

	7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Media type	Indicates the type of media used in the session. Select one of the following: • Both • Audio • Video
Call disposition	Indicates the success or failure of the session. Select one of the following: • [All] • Success Calls • Failed Calls
Report by	Indicates the values to be used in the report. Select one of the following: • Session count • Call minutes

Metrics for peer-to-peer voice and video activity by Pool

The following table lists the information provided in the Peer-to-Peer Voice and Video

Report for each pool.

Metrics for peer-to-peer voice and video activity by pool

Name	Can you sort on this item?	Description
Pool	No	Name of the Registrar pool or Edge Server used for the call.
Date/Time	No	Date and time period in which the call took place.
Total	No	Total number of sessions or total message count.

Metrics for peer-to-peer voice and video activity by call type

The following table lists the information provided in the Peer-to-Peer Voice and Video Report for each type of call that was made.

Metrics for peer-to-peer voice and video activity by call type

Name	Can you sort on this item?	Description
Call type	No	Indicates the type of call that was made. Values are one of the following: • UC-to-UC • UC-to-PSTN • PSTN-to-UC • PSTN-to-PSTN
Date/Time	No	Date and time period in which the call took place.
Total	No	Total number of sessions or total message count.

Metrics for peer-to-peer voice and video activity by access type

The following table lists the information provided in the Peer-to-Peer Voice and Video Report for each network access type.

Metrics for peer-to-peer voice and video activity by access type

Name	Can you sort on this item?	Description
Activity type	No	Indicates whether the clients were logged on to the internal network or the external network when the call was placed. Values are typically one of the following: • Internal • External • Mixed
Date/Time	No	Date and time period in which the call

		took place.
Total	No	Total number of sessions or total message count.

Metrics for peer-to-peer voice and video activity by mediation server

The following table lists the information provided in the Peer-to-Peer Voice and Video Report for each Mediation Server.

Metrics for peer-to-peer voice and video activity by mediation server

Name	Can you sort on this item?	Description
Mediation Server	No	Name of the Mediation Server.
Date/Time	No	Date and time period in which the call took place.
Total	No	Total number of sessions or total message count.

1.7.20.4.2.3 Conference Summary Report

Conference Summary Report

Monitoring and Health Configuration > Using Monitoring Reports > System Usage Reports >

Topic Last Modified: *2012-06-06*

The Conference Summary Report provides an overall view of your online conferencing sessions. A conference typically involves more than 2 users and requires the use of Microsoft Lync Server 2013 conferencing services. By comparison, a peer-to-peer session typically involves just 2 users and does not require the use of Lync Server's conferencing services. Peer-to-peer activities are reported on the Peer-to-Peer Activity Summary Report.

The Conference Summary Report not only tells you how many conferences were held during a given time period (hourly, daily, weekly, monthly) but also tells you the total number of people who took part in those conferences, and the total number of unique conference organizers.

A "unique” organizer is anyone who schedules at least one conference. For example, if Pilar Ackerman schedules one conference she counts as one unique organizer. If Ken Myer schedules 148 conferences he, too counts as one unique organizer. For example, the table below shows 8 conferences scheduled, but just three unique organizers (Ken Myer, Pilar Ackerman, and David Ahs).

Conference Organizer	Conference Date
Ken Myer	7/7/2012 10:00 AM
David Ahs	7/7/2012 10:00 AM
Ken Myer	7/7/2012 11:00 AM
Pilar Ackerman	7/7/2012 11:00 AM

Ken Myer	7/7/2012 1:00 PM
Pilar Ackerman	7/7/2012 2:00 PM
Ken Myer	7/2/2012 10:00 AM
Pilar Ackerman	7/2/2012 10:00 AM

The Conference Summary Report also indicates how many conferences included audio and/or video.

Accessing the Conference Summary Report

The Conference Summary Report is accessed from the Monitoring Reports home page. You can drill down to the Conference Activity report by clicking either of the following metrics:

- Total conferences
- Total participants

Making the Best Use of the Conference Summary Report

Total values for most of the metrics used on the Conference Summary Report can be found at the bottom of the report; scroll down to see values such as the total number of conferences held during the specified time period, and the total number of people who participated in those conferences. One metric that is not totaled at the bottom of the report is Total unique conference organizers. Why not? Here’s one reason. Suppose you are looking at a month's worth of data. On day 1 you had 34 unique conference organizers; on day 2 you had 27 unique conference organizers. Does that mean you had 61 unique conference organizers for those two days? Not necessarily. After all, all 27 people who organized conferences on day 2 might be among the 34 people who organized conferences on day 1. For example, in this simple report, note that Ken Myer and Pilar Ackerman scheduled conferences both on 7/7/2012 and on 7/2/2012:

Conference Organizer	Conference Date
Ken Myer	7/7/2012 10:00 AM
David Ahs	7/7/2012 10:00 AM
Ken Myer	7/7/2012 11:00 AM
Pilar Ackerman	7/7/2012 11:00 AM
Ken Myer	7/7/2012 1:00 PM
Pilar Ackerman	7/7/2012 2:00 PM
Ken Myer	7/2/2012 10:00 AM
Pilar Ackerman	7/2/2012 10:00 AM

To get a better idea of the total number of unique users who organized conferences, change your time interval; for example, look at the data by month instead of by day.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Conference Summary Report enables you to choose how data should be grouped. In this case, conferences grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Conference Summary Report.

Conference Summary Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed)

	If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) are displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).

Metrics

The following table the information provided by the Conferences Summary Report.

Conference Summary Report Metrics

Name	Can you sort on this item?	Description
Hourly **Daily** **Weekly** **Monthly**	No	Indicates the time interval that you selected on the filter toolbar. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/7/2012, you see an hourly breakdown of user registration activity for that date.
Total conferences	No	Total number of conferences (regardless of conference type) that were held. When you click this item, the report shows you the Conference Activity Report for the selected time period.
Total participants	No	Total number of people who took part in the conferences. When you click this item, the report shows you the Conference Activity Report for the selected time period.
Average participants per conference	No	Average number of people who took part in a given conference. Determined by dividing the total conferences by the total participants.
Total A/V conferences	No	Total number of conferences that included audio or video.
Total A/V conference minutes	No	Total number of minutes devoted to audio/video conferencing.

Total A/V conference participant minutes	No	Total number of participant minutes devoted to audio/ video conferencing. For example, suppose one user spends 5 minutes in an audio/video conference and a second user spends 3 minutes in that same conference. That makes a total of 8 participant minutes: 5 minutes plus 3 minutes.
Average A/V conference minutes	No	Average number of minutes per audio/video conference.
Total number of unique organizers of conferences	No	Total number of users who organized at least one conference. Users who organized more than one conference are counted as one unique organizer, just like users who only organized a single conference.
Total conference messages	No	Total number of instant messages sent during the conferences.

Conference Activity Report

Using Monitoring Reports > System Usage Reports > Conference Summary Report >

Topic Last Modified: *2012-10-22*

The Conference Activity Report makes it easy for you to answer questions like these: how many conferences are being held each day, and when are those conferences being held? Information like this is useful not only in its own right, but also as a troubleshooting tool. For example, suppose users are complaining that the network seems particularly slow in the middle of the day. A quick glance at the Conference Activity reports might suggest one possible reason: far more conferences are being scheduled between the hours of 10:00 AM and 2:00 PM then at any other time.

If the slow network is causing problems, you can encourage users to reschedule some of their conferences during the less-heavily trafficked times of the day.

Accessing the Conference Activity Report

The Conference Activity Report is accessed from the Conference Summary Report by clicking either one of the following metrics:

- Total conferences
- Total participants

Making the Best Use of the Conference Activity Report

By default the Conference Activity Report shows you the total number of conferences for the specified time period (for example, the total number of conferences per day, or the total number of conferences per hour of the day). However, you can also choose to display the total number of participants for that time period or the total number of participant minutes. To do that, click the Show/Hide Parameters button to display the filtering options, and then select one of the following from the Report by dropdown list:

- Participant count
- Participant minutes
- Conference count

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Conference Activity Report.

Conference Activity Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.

Interval	Time interval. Select any of the following: - Hourly (a maximum of 25 hours can be displayed) - Daily (a maximum of 31 days can be displayed) - Weekly (a maximum of 12 weeks can be displayed) - Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Report by	Indicates the values to be used in the report. You can select one of the following: - Participant Count - Participant Minutes - Conference Count

Metrics for Conferences by Pool

The following table lists the information in the Conference Activity Report for each pool.

Metrics for Conferences by Pool

Name	Can you sort on this item?	Description
Pool	No	Name of the Registrar pool or Edge Server used in the conference.
Date/Time	No	Date and time when the conference was held.
Total	No	Total participant count, total participant minutes, or total conference count.

Metrics for Conferences by Server Type

The following table lists the information in the Conference Activity Report for each type of server.

Metrics for Conferences by Server Type

Name	Can you sort on this item?	Description
Conferencing server type	No	Type of server used in the conference, typically one of the following: - Web Conferencing Server - IM Conferencing Server - Telephony Conferencing

		Server - AV Conferencing Server - Application Sharing
Date/Time	No	Date and time when the conference was held.
Total	No	Total participant count, total participant minutes, or total conference count.

Conference Detail Report

Using Monitoring Reports > System Usage Reports > Conference Summary Report >

Topic Last Modified: *2012-10-22*

The Conference Detail Report provides detailed information about all the users who participated in a conference. For example, you can see such information as the date and time that a user joined the conference, the date and time that the user left the conference, and the user agent of the endpoint that was used to connect that user to the conference. You can also see information the user's role in each conference (for example, Presenter or Attendee). Perhaps most important, you get quickly see which users successfully join and complete the conference, and which users were not able to successfully join and complete the conference.

Accessing the Conference Detail Report

The Conference Detail Report can be accessed from the following reports:

- The Call Admission Control Report (by clicking the Detail metric for a conference)
- The Failure List Report (by clicking the Conference metric)
- The User Activity Report (by clicking the Conference URI metric)

From the Conference Detail Report you can access the Diagnostic Report by clicking the Diagnostic Report (Detail) metric.

Filters

None. You cannot filter on the Conference Detail Report.

Metrics

The following table lists the information provided in the Conference Information section of the Conference Detail Report.

Conference Information Metrics

Name	Can you sort on this item?	Description
Conference URI		URI assigned to the conference. For example: sip:kmyer@litwareinc.com;gruu;opaque=app:conf:focus:id:drg2y8v4

Pool FQDN		Fully-qualified domain name of the Registrar pool or Edge Server involved in a session.
Start time		Date and time that the conference started.
Organizer		SIP address of the user who organized the conference.
End time		Date and time that the conference ended.

The following table lists the information provided in the Conference Participation Section of the Conference Detail Report.

Conference Participation Metrics

Name	**Can you sort on this item?**	**Description**
User		SIP address of the user who participated in the conference.
Role		Role (for example, Presenter) played by the conference participant.
Connectivity		Network connectivity (typically From Internal or From External) for the participant.
Join time		Date and time that the participant joined the conference.
Leave time		Date and time that the participant left the conference.
User agent		Identifier for the software used by the participant’s endpoint.
Diagnostic reports		Provides diagnostic and troubleshooting information. Including SIP response codes, diagnostic headers, conference join times, and diagnostic IDs for failed sessions.

The following table lists the information provided in the Conference Modalities section of the Conference Detail Report.

Conference Modalities Metrics

Name	**Can you sort on this item?**	**Description**
User		SIP address of the user who

		participated in the conference.
Join time		Date and time that the participant joined the conference.
Leave time		Date and time that a participant left the conference.
Conferencing server URI		URI for the Conferencing server used in the conference.
Diagnostic reports		Provides diagnostic and troubleshooting information. Including SIP response codes, diagnostic headers, conference join times, and diagnostic IDs for failed sessions.

Conference Join Time Report

Using Monitoring Reports > System Usage Reports > Conference Summary Report >

Topic Last Modified: *2012-10-01*

The Conference Join Time Summary enables you to determine how long it takes your users to join a conference. The report shows the average join time (in milliseconds), and also provides a breakdown that lets you know how many users were able to join a conference in 2 seconds or less, how many users required between 2 and 5 seconds to join the conference, and so on.

Accessing the Conference Join Time Report

The Conference Join Time Report is accessed from the Monitoring Reports home page.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Conference Join Time Report.

Conference Join Time Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report

	automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click **[All]** to view data

	for all the pools. This drop-down list is automatically populated for you based on the records in the database.
Conference sessions	Type of session. Allowed values are: - [All] - Focus sessions - Application sharing - A/V conferencing If you select [All], the total conference join time will be displayed at the top of the report. Note that these totals are only for conferences which were scheduled by using Microsoft Exchange or Microsoft Outlook.

Metrics

The following table lists the information provided in the Conference Join Time Report.

Conference Join Time Report Metrics

Name	Can you sort on this item?	Description
Date The actual title for this metric will vary depending on the Interval that was selected.	No	Date and time that the conference took place.
Total sessions	No	Total number of sessions, including successful sessions, failed sessions (both expected failures and unexpected failures), and uncategorized sessions.
Average (ms)	No	Average amount of time (in milliseconds) that it took participants to join the conference.
Sessions < 2 seconds, Volume	No	Number of participants who were able to join the conference in less than 2 seconds.
Sessions < 2 seconds, Percentage	No	
Sessions 2-5 seconds, Volume	No	Number of participants who took between 2 seconds and 5 seconds to join the conference.
Sessions 2-5 seconds, Percentage	No	Percentage of the total call participants who took between 2 seconds and 5 seconds to join the conference.

Sessions 5-10 seconds, Volume	No	Number of participants who took between 5 seconds and 10 seconds to join the conference.
Sessions 5-10 seconds, Percentage	No	Percentage of the total call participants who took between 5 seconds and 10 seconds to join the conference.
Sessions > 10 seconds, Volume	No	Number of participants who required more than 10 seconds to join the conference.
Sessions > 10 seconds, Percentage	No	Percentage of the total call participants who required more than 10 seconds to join the conference.

1.7.20.4.2.4 PSTN Conference Summary Report

PSTN Conference Summary Report

Monitoring and Health Configuration > Using Monitoring Reports > System Usage Reports >

Topic Last Modified: *2012-10-22*

In Microsoft Lync Server 2013, a PSTN conference is any conference in which at least one participant dials in to the audio portion by a using a PSTN (public switched telephone network) phone. (A PSTN phone is a "landline," a cell phone, or any other phone which does not make use of Voice over IP.) Although referred to as PSTN conferences in the Monitoring Reports, these conferences are perhaps more-commonly known as dial-in conferences.

The PSTN Conference Summary Report provides information about all the PSTN conferences held in your organization (that is, all the conferences that had at least one dial-in user). The report includes information about the total number of PSTN conferences, the total number of people who participated in those conferences, and, perhaps, most important, the total number of dial-in users (the Total PSTN participants metric).

Accessing the PSTN Conference Summary Report

The PSTN Conference Summary Report can only be accessed from the Monitoring Reports home page. This report is not linked to any other reports. Note that you cannot retrieve detailed call information for a PSTN conference, in part because individual endpoints are responsible for submitting this information. PSTN phones are not capable of tracking or submitting call detail information.

Making the Best Use of the PSTN Conference Summary Report

To determine the percentage of all your conferences that include dial-in users, compare the value of the Total PSTN conferences metric with the Total conferences metric found on the Conference Summary Report.

If you don't see as many PSTN conferences as you might have expected to see, keep in mind that the ability to organize a conference that allows dial-in users depends on the conferencing policy that has been assigned to a user: if very few of your users are allowed to hold PSTN conferences you would obviously see very few PSTN conferences. You can quickly verify which of your conferencing policies (if any) allow users to schedule PSTN conferences by running the following command from within the Lync Server Management Shell:

```
Get-CsConferencingPolicy | Select-Object Identity, EnableDialInConferencing
```

That will return data similar to this:

```
Identity                                EnableDialInConferencing
--------                                ------------------------
Global                                                      True
site:Redmond                                               False
site:Dublin                                                False
Tag:RedmondDialInUsers                                      True
Tag:DublinDialInUsers                                       True
```

That will return data similar to this:

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the PSTN Conference Summary Report enables you to choose how data should be grouped. In this case, conferences are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the PSTN Conference Summary Report.

PSTN Conference Summary Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.

To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).

Metrics

The following table lists the information in the PSTN Conference Summary Report.

PSTN Conference Summary Report Metrics

Name	Can you sort on this item?	Description
Hourly **Daily** **Weekly** **Monthly**	No	Indicates the selected time interval. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/7/2012, you see an hourly breakdown of user registration activity for that

		date.
Total PSTN conferences	No	Total number conferences that allowed dial-in access.
Total participants	No	Total number of people who participated in conferences that allowed dial-in access.
Total A/V conference minutes	No	Total amount of audio/visual conference time.
Total A/V conference participant minutes	No	Total amount of audio/visual participant time. For example, if one participant spent five minutes in an A/V conference and another participant spent three minutes in the same conference, the total A/V conference participant time would be eight minutes.
Total PSTN participants	No	Total number of users who dialed in to conferences that allowed dial-in access.
Total PSTN participant minutes	No	Total amount of conference time spent by dial-in users. For example, if one dial-in participant spent five minutes in a conference and another participant spent three minutes in the same conference, the total PSTN participant time would be eight minutes.
Unique conference organizers	No	Total number of users who organized at least one conference that allowed dial-in access. Users who organized more than one conference are counted as one unique organizer, just like users who only organized a single conference.

1.7.20.4.2.5 Response Group Usage Report

Response Group Usage Report

Monitoring and Health Configuration > Using Monitoring Reports > System Usage Reports >

Topic Last Modified: *2013-02-22*

The Response Group application provides a way for Microsoft Lync Server 2013 to answer and route phone calls based on the number that was dialed and, optionally, on the caller's responses to a series of questions. Typically, Response Group calls are not routed to an individual person but, instead, are routed to a team of people referred to as an agent group. For example, if someone calls the phone number for your help desk, Lync Server 2013 can automatically route that call to the first available help desk agent. Alternatively, Lync Server could ask a series of questions ("Press 1 if you are having hardware problems. Press 2 if you are having software problems. Press 3 if you are having network problems.") and then route the call to the most appropriate help desk agent based on the answer to those questions.

The Response Group Usage Report provides a detailed look at the number of phone calls received by all your Response Group workflows, then breaks those calls down into more finite categories such as Offered calls, Answered calls, and Abandoned calls.

The key to working with the Response Group Usage Report is to understand the difference between the reported call types:

- **Received calls**. Total number of calls received by all instances of the Response Group application.
- **Successful calls**. Total number of calls that were picked up by the Response Group application.
- **Offered calls**. Total number of calls that were transferred to a Response Group agent.
- **Answered calls**. Total number of calls that were actually answered by a Response Group agent.
- **Percentage of abandoned calls**. Percentage of calls that were received by the Response Group application but were never answered by an agent. This value is calculated by subtracting the Answered calls from the Received calls, and then dividing that value by the number of Received calls. For example, if you received 10 calls and 7 were answered, you would subtract 7 from 10, leaving 3 unanswered calls. That value would then be divided by 10, giving you an abandoned call percentage of 30%.
- **Transferred calls**. Total number of Response Group calls that were transferred because of a queue timeout or queue overflow.

If you are looking at the Response Group Usage Report and can't remember the definition for any of these call types, simply hold your mouse over the appropriate call type label. A tooltip will appear that offers a brief description of the call type.

The Response Group Usage Report allows you to filter on a workflow URI (the SIP address associated with that workflow). However, workflow URIs do not actually appear on the report itself. If you would like to know things such as which workflows are answering the most calls or which workflows are experiencing the most transferred calls, click the appropriate metric to open the Response Group Call List Report for that given time period. That reports does list the workflow URIs.

Accessing the Response Group Usage Report

The Response Group Usage Report is accessed from the Monitoring Reports home page. You can drill down to the Response Group Call List Report by clicking any of the following metrics:

- Received calls
- Successful calls
- Offered calls
- Answered calls
- Transferred calls

Making the Best Use of the Response

Group Usage Report

One of the more interesting uses of the Response Group Usage Report might not be readily apparent: the ability to retrieve usage information for a single Response Group workflow.

> ⚠**Warning:**
>
> A Response Group workflow is basically a set of instructions that determines what Lync Server does when a user dials a particular phone number. To that end, each workflow is uniquely associated with a phone number. When someone calls that number, the workflow determines how the call will be handled. For example, the workflow might cause the call to be routed to a series of interactive voice response (IVR) questions that prompt the caller to enter additional information ("Press 1 for hardware support. Press 2 for software support."). Alternatively, the workflow might cause the call to be placed in a queue , with the caller put on hold until an agent is available to answer the call. The availability of agents to answer calls is also dictated by the workflow: workflows are used to configure both business hours (the days of the week and the times of day when agents are available to answer calls) and holidays (days when no agents are available to answer calls). Any time you dial a phone number that belongs to the Response Group application you are essentially calling a Response Group workflow.

Although workflow URIs do not appear in the Response Group Usage Report, it's still possible to view the usage statistics for a single workflow, something that is often extremely useful. For example, suppose you recently unveiled a new ad campaign and are curious to know whether people are calling in to ask about that product. If you have associated a Response Group workflow with the phone number given in the ad campaign, you can easily check to see how many people (if any) are calling that number.

You might also use a similar approach to gauge the number of calls being handled by your internal help desk or your customer service department.

To review usage statistics for a particular workflow, enter the workflow URI in the Workflow URI box. Of course, as noted, workflow URIs (the SIP address associated with a workflow) do not appear on the report. That means you need to find some other way to determine the URI of a workflow. One way to do this is to use Windows PowerShell and the Lync Server Management Shell. For example, this command returns the URIs for all your Response Group workflows:

```
Get-CsRgsWorkflow | Select-Object Name, PrimaryUri
```

That will return data similar to this:

```
Name                            PrimaryUri
----                            ----------
Customer Support                sip:support@litwareinc.com
Help Desk                       sip:helpdesk@litwareinc.com
New Ad Campaign                 sip:newads@litwareinc.com
```

This command returns information for a single workflow, the one with the name New Ad Campaign:

```
Get-CsRgsWorkflow -Name "New Ad Campaign" | Select-Object Name, PrimaryUri
```

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Response Group Usage Report enables you to view data for all your Response Group workflows or to view data for an individual workflow. You can also choose how data should be grouped. In this case, usages are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Response Group Usage Report.

Response Group Usage Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum

	number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Workflow URI	Enables you to limit the returned data to the specified Response Group workflow. To use this filter, enter the Workflow SIP address. For example: sip:helpdesk@litwareinc.com

Metrics

The following table lists the information provided in the Response Group Usage Report.

Response Group Usage Report Metrics

Name	Can you sort on this item?	Description
Hourly **Daily** **Weekly** **Monthly**	No	Indicates the selected time interval. Where applicable, you can click a given time interval to view detailed information for that interval. For example, if you are using the Daily interval and you click 7/7/2012, you see an hourly breakdown of user registration activity for that date.
Received calls	No	Total number of calls received by all instances of the Response Group application. When you click this item, the report shows you the Response Group Call List report for the selected time period.
Successful calls	No	Total number of calls that were picked up the Response Group application. When you click this item, the report shows you the Response Group Call List report for the selected time period.
Offered calls	No	Total number of calls that were transferred to a Response Group agent. When you click this item, the report shows you the

		Response Group Call List report for the selected time period.
Answered calls	No	Total number of calls that were actually answered by a Response Group agent. When you click this item, the report shows you the Response Group Call List report for the selected time period.
Percentage of abandoned calls	No	Total number of calls that were received by the Response Group application but were never answered by an agent. This is calculated by subtracting the Answered calls from the Received calls, and then dividing that value by the number of received calls. For example, if you have 10 received calls and seven were answered, you would subtract seven from 10, leaving three unanswered calls. That value would then be divided by 10, giving you an abandoned call percentage of 30%.
Average call minutes by agent	No	Average amount of time a Response Group agent spent on a call.
Transferred calls	No	Total number of Response Group calls that were transferred because of a queue timeout or queue overflow. When you click this item, the report shows you the Response Group Call List report for the selected time period.

Response Group Call List Report

Using Monitoring Reports > System Usage Reports > Response Group Usage Report >

Topic Last Modified: *2013-02-22*

The Response Group application provides a way for Microsoft Lync Server 2013 to answer and route phone calls based on the number that was dialed and, optionally, on the caller's responses to a series of questions. Typically, Response Group calls are not routed to an individual person but, instead, are routed to a team of people referred to as an agent group. For example, if someone calls the phone number for your help desk, Lync Server 2013 can automatically route that call to the first available help desk agent. Alternatively, Lync Server could ask a series of questions ("Press 1 if you are having hardware problems. Press 2 if you are having software problems. Press 3 if you are having network problems.") and then route the call to the most appropriate help desk agent based on the answer to those questions.

The Response Group Call List Report represents a collection of calls made for a specified period of time and for a specified type of call. The Response Group Usage Report (which must be opened first before you can open the Response Group Call List Report) recognizes the following call types:

- **Received calls**. Total number of calls received by all instances of the Response Group application.
- **Successful calls**. Total number of calls that were picked up by the Response Group application.
- **Offered calls**. Total number of calls that were transferred to a Response Group agent.
- **Answered calls**. Total number of calls that were actually answered by a Response Group agent.
- Percentage of abandoned calls. Percentage of calls that were received by the Response Group application but were never answered by an agent. This value is calculated by subtracting the Answered calls from the Received calls, and then dividing that value by the number of Received calls. For example, if you received 10 calls and 7 were answered, you would subtract 7 from 10, leaving 3 unanswered calls. That value would then be divided by 10, giving you an abandoned call percentage of 30%.
- **Transferred calls**. Total number of Response Group calls that were transferred because of a queue timeout or queue overflow.

Accessing the Response Group Call List Report

The Response Group Call List Report can only be accessed by clicking one of the following metrics found on the Response Group Usage Report:

- Received calls
- Successful calls
- Offered calls
- Answered calls
- Transferred calls

Making the Best Use of the Response Group Call List Report

The Response Group Call List Report allows you to limit the displayed data to calls involving a particular Response Group workflow. To do that, you need to enter the workflow URI (the workflow's SIP address) in the Workflow URI box. Before you can do that, however, you must actually be able to see the Workflow URI box. To display the filtering options for the Response Group Call List Report, click the Show/Hide Parameters button in the upper left-hand portion of the report window.

Note that the Response Group Call List does not display information about either the Response code or the Diagnostic ID if you hold the mouse over either of those metrics. If you need more information, you might note the Response code and/or Diagnostic ID, and then search for those values in the Top Failures Report.

a question like this one: "Which individual workflow received the most calls?", you can do the following:

1. On the Response Group Usage Report, set the desired time period and then click the Received Calls metric. That will open the Response Group Call List

Report.

2. Export the data shown on the Response Group Call List Report. For example, you might export the data in Microsoft Excel format, and then use Excel to convert that data to a comma-separated values file.
3. Run your analyses using Windows PowerShell.

For example, if you have saved the data to a file named C:\Data \Response_Group_Call_List_Report.csv, you can then use the following command to return the total number of received calls for each workflow listed in the report:

```
$calls = Import-Csv -Path "C:\ Data\Response_Group_Call_List_Report.csv"
$calls | Group-Object Workflow | Select-Object Count, Name | Sort-Object Count -D
```

That will information similar to this:

```
Count    Name
-----    ----
  160    Redmond Help Desk
   47    Dublin Help Desk
   31    North America Customer Support
   16    EMEA Customer Support
   14    Employment Opportunities
```

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Response Group Call List Report.

Response Group Call List Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date:

	7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Workflow URI	Enables you to limit the returned data to the specified Response Group workflow. To use this filter, enter the Workflow SIP address. For example: sip:helpdesk@litwareinc.com
Calls	You can select one of the following call types: • Received Calls • Successful Calls • Offered Calls • Answered Calls • Transferred Calls

Metrics

The following table lists the information provided in the Response Group Call List Report for each call received by the Response Group application.

Response Group Call List Report Metrics

Name	**Can you sort on this item?**	**Description**
Caller	No	SIP address of the caller.
Workflow	No	SIP address of the Response Group workflow.
Start time	No	Date and time that the call started.
End time	No	Date and time that the call ended.
Response code	No	SIP response code sent when the session failed.
Diagnostic ID	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.

1.7.20.4.2.6 IP Phone Inventory Report

IP Phone Inventory Report

Monitoring and Health Configuration > Using Monitoring Reports > System Usage Reports >

Topic Last Modified: *2012-11-12*

The IP Phone Inventory Report reports information about the IP phones currently in use in your organization. The IP Inventory Report provides a detailed list of the IP phones that were actually used during the specified reporting period. Among other things, this report lets administrators know if there are any old, outdated phones still in use that should be replaced; it can also alert administrators to the fact that there are expensive phones in the organization that are rarely being used. That type of information can be invaluable when it comes time to purchase new phones or to redistribute existing phones. (For example, a user who rarely uses his or her expensive phone might be asked to swap phones with a user who uses his or her phone much more frequently.)

It should be noted that this report does have a few limitations when it comes to being used as a true inventory report. For one thing, the IP Phone Report simply lists all the phones that logged on to Lync Server during the specified time period, sorted by their last logon time. If a phone did not log on during the specified time period then it will not be listed in the inventory report. That includes phones that logged on before the time period started and were still logged on during the specified time interval. For example, suppose you wanted to look at all the phone inventory for July, 2012. Suppose, as well, that several phones logged on to Lync Server on June 30, 2012 and were still logged on as of July 1st. Those phones will not show up on the inventory report for July 1st.

It's also important to note that the inventory report could include phones that your organization no longer uses. For example, suppose a number of Fabrikam phones logged on to the system on July 1, 2012; 5 days later your organization got rid of all those Fabrikam phones and replaced them with a newer Contoso model. The Fabrikam phones will still appear on the "inventory" report simply because they logged on to the system during the month of July.

In addition, the IP Phone Inventory Report does not report summary totals for the different types of phones. For example, suppose you have 105 Polycom CX600 phones. The report will not tell you that you have 105 of these phones; instead, you will simply see 105 separate entries for the Polycom Cx600. The only way to know that there are 105 entries for the Polycom Cx600 would be to count each of those entries manually.

⚠**Warning:**
Or, export the data and use Microsoft Excel or Windows PowerShell to do that counting for you.

Accessing the IP Phone Inventory Report

The IP Phone Inventory Report is accessed from the Monitoring Reports home page. If you click the User URI metric you can access the User Activity Report for that user. Clicking the Last activity metric for a peer-to-peer call will take you to the Peer-to-Peer Session Detail Report; clicking that same metric for a conference will take you to the Conference Detail Report.

Making the Best Use of the IP Phone Inventory Report

If you're only interested in usage information for one particular kind of phone (for example, "How often are users using a Polycom CX600 phone?") you can get that information directly from the IP Phone Inventory Report by filtering for that particular kind of phone. However, if you want summary information for all your phones (how many people are using a Polycom CX600, how many are using an LG-Nortel IP8540, etc.) then you will need to export the data and use another application (such as Windows PowerShell) to do that type of analysis. For example, suppose you export the data to a comma-separated values file (C:\Data\IP_Phone_Inventory_Report.csv). In that case, you could use these two commands to provide summary data for all your phones:

```
$phones = Import-Csv "C:\Data\IP_Phone_Inventory_Report.csv"
$phones |Group-Object Manufacturer, "Hardware version" | Select-Object Count, Nam
```

That will return data similar to this:

```
Count    Name
-----    ----
  267    POLYCOM, CX700
  267    POLYCOM, CX600
  166    POLYCOM, C
   68    Microsoft, CPE
   64    LG-Nortel, IP8540
   59    Aastra, 6725ip
   37    LG-Nortel, IP
   22    POLYCOM, CX3000
   11    Microsoft, CPE_A
    9    POLYCOM, CX500
    7    Aastra, 6721ip
```

Similarly, these two commands tell you which phones logged on to the system but were never actually used to make a call (the value of the Last activity metric is blank, indicating that there hasn't been any last activity):

```
$phones = Import-Csv "C:\Data\IP_Phone_Inventory_Report.csv"
$phones | Where-Object {$_."Last activity" -eq ""}
```

That returns data similar to this for each phone that has not been used:

```
Manufacturer     : POLYCOM
Hardware version : CX600
MAC address      : 00-04-F2-00-01-76
User URI         : 422
User agent       : CPE/4.0.7423.1 OCPhone/4.0.7423.1 (Microsoft Lync 2010 (Beta)
Last logon time  : 8/30/2010 4:44:48 PM
Last logoff time : 8/30/2010 5:59:07 PM
Last activity    :
```

Another interesting way to use the IP Phone Inventory Report is this: if you have the MAC address of an IP Phone you can find out the user who last used that phone simply by entering that address in the MAC address text box. The IP Phone Inventory report will then report back (among other things) the SIP address of the user who last logged on with that phone. Alternatively, you can enter a user SIP address (in the User URI prefix box) to find out all the phones that have been used by that user.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the IP Phone Inventory enables you to view only the phones manufactured by a specific company, or even a specific version of those phones. You can also choose how data should be grouped. In this case, registrations are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the IP Phone Inventory Report.

IP Phone Inventory Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Manufacturer	Name of the company that manufactured the IP phone. The values for this filter are automatically populated for you based on the IP phones that are currently in the database.
Hardware version	Version number of the IP phone; by using the Manufacturer and the Hardware version filters you can uniquely identity a particular type of phone. The values for this filter are automatically populated for you based on the IP phones that are currently in the database.
User agent	Identifier for the software used by the IP phone. The values for this filter are automatically populated for you based on the IP phones currently in the database.

MAC address	Unique identifier for the network interface on the IP phone. The Media Access Control (MAC) address is typically assigned at the time the phone is manufactured and is hard-wired into the device hardware. To search for records pertaining to a specific MAC address simply enter that address. For example: 00-08-5D-16-16-48 You must enter the complete address. A partial address (for example 00-08-5D) does not return any data.
Last activity before days	Select one of the following values: • [All] • 10 • 20 • 30
Last logoff time before days	Select one of the following values: • [All] • 10 • 20 • 30
User URI prefix	SIP address of the user who used the IP phone.

Metrics

The following table lists the information provided in the IP Phone Inventory Report.

IP Phone Inventory Report Metrics

Name	Can you sort on this item?	Description
Manufacturer	Yes	Name of the company that manufactured the IP phone.
Hardware version	Yes	Version number of the IP phone.
MAC address	Yes	Unique identifier for the network interface on the IP phone. The MAC address is typically assigned at the time the phone is manufactured and is hard-wired into the device hardware.
User URI	Yes	SIP address of the user who used the IP phone.
User agent	Yes	Identifier for the software used by the IP phone.
Last logon time	Yes	Date and time that the IP phone last logged on to Lync Server.

Last logoff time	Yes	Date and time that the IP phone last logged off from Lync Server.
Last activity	Yes	Date and time that the IP phone was last used.

1.7.20.4.2.7 Call Admission Control Report

Call Admission Control Report

Monitoring and Health Configuration > Using Monitoring Reports > System Usage Reports >

Topic Last Modified: *2012-06-29*

The Call Admission Control Report provides information about peer-to-peer and conferencing sessions that were conducted under restrictions set in place by Call Admission Control. Call Admission Control, introduced in Microsoft Lync Server 2010, provides a way for administrators to allow (or not allow) communication sessions based on bandwidth constraints. For example, administrators can create policies that impose a limit on the amount of bandwidth available for voice and video calls. If that bandwidth limit has been reached, then no new voice or video calls can be placed until one of the current calls has ended and freed up the required network resources.

Accessing the Call Admission Control Report

The Call Admission Control Report is accessed from the Monitoring Reports home page. From the Call Admission Control Report you can drill down to either of the following reports:

- Conference Detail Report – To access this report, click the Details metric from a conference session.
- Peer-to-Peer Session Detail Report – To access this report, click the Details metric for a peer-to-peer session.

Making the Best Use of the Call Admission Control Report

To get a list of calls that failed because of insufficient bandwidth, select Calls rejected because of call admission control from the Call category dropdown list. Most of the returned calls will likely have a diagnostic ID of 5:

Insufficient bandwidth to establish session. Attempt PSTN re-route.

That indicates that Call Admission Control limitations were preventing the call from being made on the VoIP network.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Call Admission Control Report enables you to filter calls by the user who initiated the call or by the user who was being called. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Call Admission Control Report.

Call Admission Control Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/17/12012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/12012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/17/12012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/12012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2012 Weeks always run from Sunday through Saturday.
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click **[All]** to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.
Activity type	Type of activity. Select one of the following activities: • [All] • Peer-to-Peer • Conference

Call category	Indicates the reason that CAC was used for the call. Select one of the following: • [All] • Call rejected because of call admission control • Calls rerouted through PSTN because of call admission control

Metrics for Peer-to-Peer Sessions

The following table lists the information provided in the Call Admission Control Report for peer-to-peer sessions (that is, sessions involving just two participants).

Metrics for Peer-to-Peer Sessions

Name	Can you sort on this item?	Description
Detail	No	When you click this item, the report shows you a Peer-to-Peer Session Detail Report for the specified session.
From user	Yes	SIP address of the user who initiated the session.
To user	Yes	SIP address of the user who was invited to join the session.
Modalities	Yes	Communication modalities (such as audio and video) that were used during the session.
Invite time	Yes	Date and time the initial session invitation was sent to the From user.
Response time	Yes	Date and time that the invitation acceptance was received.
End time	Yes	Date and time that the session ended.
Diagnostic ID	Yes	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

Metrics for Conferencing Sessions

The following table lists the information provided in the Call Admission Control Report for conferencing sessions (that is, sessions involving three or more participants).

Metrics for Conferencing Sessions

Name	Can you sort on this item?	Description
Conference URI	Yes	Unique identifier for the conference. When you click this item, the report shows the individual conference participants.
Organizer	Yes	SIP address of the user who organized the conference.
Pool	Yes	Edge Server used in the conference.
Start time	Yes	Date and time that the conference started.
End time	Yes	Date and time that the conference ended.

Metrics for Individual Conference Participants

The following table lists the information provided in the Call Admission Control Report for individual conference participants.

Metrics for Individual Conference Participants

Name	Can you sort on this item?	Description
Role	No	Role (for example, Presenter) played by the conference participant.
Participant	No	SIP address of the conference participant.
Connectivity	No	Network connectivity (typically From Internal or From External) for the participant.
Modality	No	Conference type (for example, A/V conferencing).
Join time	No	Date and time that the participant joined the conference.
Leave time	No	Date and time that the participant left the conference.

Diagnostic ID	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

Peer-to-Peer Session Detail Report

Using Monitoring Reports > System Usage Reports > Call Admission Control Report >

Topic Last Modified: *2012-06-06*

The Peer-to-Peer Session Detail Report returns detailed information about a peer-to-peer session. For example, if you select an instant messaging session, the report will tell you the number of messages sent by each of the two users in the session.

Accessing the Peer-to-Peer Session Detail Report

The Peer-to-Peer Session Detail Report can be accessed from any of the following reports (all of which can be accessed from the Monitoring Reports home page):

- IP Phone Inventory Report
- User Activity Report
- Call Admission Control Report
- Failure List Report

From within the Peer-to-Peer Session Detail Report you can access the Diagnostic Report by clicking the Diagnostic Report (Details) metric. You can also access the Top Failures Report by clicking either of these two metrics:

- Response
- Diagnostic ID

Making the Best Use of the Peer-to-Peer session Detail Report

The Peer-to-Peer Session Detail Report includes a large number of metrics, many of which might not be familiar to system administrators. Often-times, however, you can view a tooltip that offers a brief description of that metric simply by holding your mouse over the metric label.

Note that the actual metrics shown on a given report will depend on the type of peer-to-peer session you selected. An audio/video session will report a different set of metrics than an instant messaging session.

You can also hold your mouse over the Response code and Diagnostic ID metrics in order to obtain a description of those values:

Filters

None. You cannot filter the Peer-to-Peer Session Detail Report.

Session Information Metrics

The following table lists the information provided in the Peer-to-Peer Session Detail Report for each session.

Session Information Metrics

Name	Description
Pool FQDN	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server involved in the session.
Invite time	Date and time the session invitation was originally sent.
Response time	Date and time that the invitation acceptance was received.
From user	SIP address of the user who initiated the session.
From user agent	Software used by the endpoint of the user who initiated the session.
Is From user internal	Indicates whether the user who initiated the session was logged on to the internal network.
Is From user integrated with desk phone	Indicates whether the endpoint used by the user who initiated the session is integrated with his or her desktop phone.
Session Priority	Priority assigned to the session. Valid priorities are: Unknown; Non-Urgent; Normal; Urgent; and Emergency.
Response code	SIP response code sent when the session failed.
Front end	Name of the Front End Server used in the conference.
Capture time	Date and time that the session information was recorded.
End time	Date and time the session ended.
To user	SIP address of the user who was invited to the session.
To user agent	Software used by the endpoint of the user who was invited to the session.

Is To user internal	Indicates whether the user who was invited to the session was logged on to the internal network.
Is To user integrated with desk phone	Indicates whether the endpoint used by the user who was invited to the session is integrated with his or her desktop phone.
Is retried session	Indicates whether the session is an attempt to retry a session that previously failed.
Diagnostic ID	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Hold the mouse over the ID number to view additional information about that ID.

Metrics for Modalities

The following table lists the information provided in the Peer-to-Peer Session Detail Report for each session modality.

Metrics for Modalities

Name	Can you sort on this item?	Description
Modalities	No	Modalities used in the session. For example, instant messaging (IM) or file transfer.
From user messages	No	Number of messages sent by the user who initiated the session.
To user messages	No	Number of messages sent by the user who was invited to join the session.

Metrics for Diagnostic Reports

The following table lists the information provided in the Peer-to-Peer Session Detail Report for each diagnostic report.

Metrics for Diagnostic Reports

Name	Can you sort on this item?	Description
Detail	No	When you click this item, the report shows the Diagnostic Report for the session.
Report time	No	Date and time the report was recorded.
Request	No	SIP request type. For example, INVITE or BYE.
Diagnostic ID	No	Unique identifier (in the form

		of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.
Content type	No	Type of media content used in the conference. For example, a common content type is Application/sdp. Session Description Protocol (SDP) is a standard Internet protocol used for session announcements, session invitations, and other forms of multimedia session initiation.
Reported by	No	Computer (that is, client or server) that reported the problem.

1.7.20.4.3 Call Diagnostic Reports (per user)

Call Diagnostic Reports (per user)

Operations > Monitoring and Health Configuration > Using Monitoring Reports >

Topic Last Modified: *2012-10-21*

The Call Diagnostic Reports provide per-user information about failed peer-to-peer and conferencing sessions.

- User Activity Report   Provides information about peer-to-peer and conference activities for each of your users.

1.7.20.4.3.1 User Activity Report

User Activity Report

Monitoring and Health Configuration > Using Monitoring Reports > Call Diagnostic Reports (per user) >

Topic Last Modified: *2012-10-22*

The User Activity Report provides a detailed list of the peer-to-peer and conferencing sessions carried out by your users in a given time period. Unlike many of the Monitoring Reports, the User Activity Report ties each call to individual users. For example, peer-to-peer sessions specify the SIP URIs of the person who initiated the call (the From user) and the person who was being called (the To user). If you expand the information for a conference, you'll see a list of all the conference participants and the role they held for that conference.

The User Activity Report is sometimes referred to as the "help desk" report. That's because the report is often used by help desk personnel to retrieve session information for a specific user. You can filter for calls made to or made by an individual user simply by typing the user's SIP URI in the User URI prefix box.

If you do this, keep in mind that the User Activity Report will search anywhere in the Uri field for the value entered in this box. For example, suppose you are searching for this user:

Ken.Myer@litwareinc.com

If you type **ken** in the URI box, the User Activity Report will locate **Ken**.Myer@litwareinc.com. It will also locate these users:

- Ronen.Ash**ken**azi@litwareinc.com
- Markus.Ran**ken**burg@litwareinc.com
- **Ken**.Sanchez@litwareinc.com
- Will. **Ken**nedy@litwareinc.com

In other words, the more specific the information you enter, the more likely it will be that you will get back just the information of interest to you.

To access the user activity report

The User Activity Report is accessed from the Monitoring Reports home page. You can also reach the User Activity Report by clicking the User URI metric on the IP Phone Inventory Report. From within the User Activity Report, clicking the Conference URI (for a conference) takes you to the Conference Detail Report. Similarly, clicking the Detail metric for a peer-to-peer call takes you to the Peer-to-Peer Session Detail Report.

Making the best user of the user activity report

Although there is a lot of good information in the User Activity Report, that information can sometimes be difficult to locate. For example, all the user activity that takes place in your organization during a specified period is included in the User Activity Report; that means that, buried, within the report is information about which users actually used Microsoft Lync Server 2013 in some way.

⚠**Warning:**

Technically, it’s possible that some s user activity might go unrecorded: while Lync Server strives to keep information about all phone calls it's possible that a call could have been made without the information about that call being written to the database. Lync Server is designed to give an extremely accurate but not necessarily perfect look at how Lync Server 2013 is being used. (The fact that there is no guarantee that 100% of all calls are recorded explains why Lync Server monitoring should not be used as a billing system.) Second, a Monitoring Report report can only display, at most, 1,000 records. Depending on the amount of user activity you have, and depending on the time period you are working with, that means your query might not return all the data actually stored in the database.

In addition to that, the User Activity Report indicates the type of session (modality) that a user participated in (for example, instant messaging, file transfer, audio, etc.). However, you can't filter by modality. The Modality filter only offers one choice: All. The only way to filter by modality is to export the data and then do your filtering in another application (such as Microsoft Excel or Windows PowerShell).

This means is that you can easily retrieve detailed information about any one user in your organization. What you can't do, at least not directly, is answer questions like this:

- Which users actually used the system during this time period?
- Which of my users were the most active during this time period?
- Are the users who make the most phone calls also the users who participate

in the most instant messaging sessions?

If you need to answer questions like this, you can export the data retrieved by the Monitoring Reports to an Excel spreadsheet. You then use that spreadsheet and/or a comma-separated values file to analyze the data in ways that the User Activity Report. For example, suppose you have exported the report data to Excel and then to a comma-separated values file. At that point, you can import the data from the .CSV file to Windows PowerShell by using a command similar to this:

```
$x = Import-Csv -Path "C:\Data\User_Activity_Report.csv"
```

After the data has been imported you can then use simple Windows PowerShell commands to help answer your questions. For example, this command returns a list of unique users who served as the "From user" in at least one session:

```
$x | Group-Object "From user" | Select Name | Sort-Object Name
```

In other words:

```
Name
----
David.Ahs@litwareinc.com
Gilead.Amosnino@litwareinc.com
Henrik.Jensen@litwareinc.com
Ken.Myer@litwareinc.com
Pilar.Ackerman@litwareinc.com
```

This command lists the unique users (based on the total number of sessions that they participated in:

```
$x | Group-Object "From user" | Select Count, Name | Sort-Object Count -Descendin
```

That returns data similar to this:

```
Count    Name
-----    ----
  523    Ken.Myer@litwareinc.com
   63    David.Ahs@litwareinc.com
   29    Pilar.Ackerman@litwareinc.com
   17    Gilead.Amosnino@litwareinc.com
   10    Henrik.Jensen@litwareinc.com
```

This command limits the reported sessions to those that included audio as a modality:

```
$x | Where-Object {$_.Modalities -match "audio"} | Group-Object "From user" | Sel
```

If you hold your mouse over any Diagnostic ID shown on the report, a tooltip will appear describing that ID.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the User Activity Report enables you to filter the returned data based on such things as activity type (that is, peer-to-peer sessions or conferencing sessions) or by the user's SIP address (allowing you to view the activities for one user). You can also choose how data should be grouped. In this case, usages are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the User Activity Report.

User activity report filters

Name	Description

From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/17/12012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/12012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/17/12012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/17/12012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/13/2012 Weeks always run from Sunday through Saturday.
Activity type	Type of activity. Select one of the following: • [All] • Peer-to-peer • Conference
Modality	You can only select **[All]**, which shows information for all modalities, including audio, video, instant messaging (IM), and file transfer.
Session category	Indicates whether the activity in question succeeded or failed. Select one of the following: • [All] • Success • Expected failure • Unexpected failure An "expected failure" is a failure that is expected to happen; for example, if a user has set his or her

	status to Do Not Disturb you would expect any call to that user to fail. An "unexpected failure" is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.
User URI prefix	SIP address for the user. To view records only for the user Ken Myer you need to enter Ken Myer's SIP address. For example: sip:kenmyer@litwareinc.com

Metrics for peer-to-peer sessions

The following table lists the information provided in the User Activity Report for peer-to-peer sessions (that is, sessions involving just two participants).

Metrics for peer-to-peer sessions

Name	Can you sort on this item?	Description
Detail	No	When you click this item, the report shows you the Peer-to-Peer Session Detail Report for the selected session.
From user	Yes	SIP address of the user who initiated the peer-to-peer session.
To user	Yes	SIP address of the user who joined the peer-to-peer session.
Modalities	Yes	Type of communication used in the session. For example, IM, audio, or file transfer.
Invite time	Yes	Date and time the initial invitation to join the peer-to-peer session was sent.
Response time	Yes	Date and time that the "To" user accepted the session invitation.
End time	Yes	Date and time the peer-to-peer session ended.
Diagnostic ID	Yes	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to

		have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

Metrics for conferencing sessions

The following table lists the information provided in the User Activity Report for conferencing sessions (that is, sessions involving three or more participants).

Metrics for conferencing sessions

Name	Can you sort on this item?	Description
Conference URI	Yes	Unique conference identifier. When you click this item, the report shows you the Conference Detail Report for the selected session. When you expand this item, the report shows you information about the conference participants. For details, see the "Metrics for Conference Participants" section later in this topic.
Organizer	Yes	SIP address of the user who organized the conference.
Pool	Yes	Name of the Edge Server (if any) used in the conference.
Start time	Yes	Date and time that the conference began.
End time	Yes	Date and time that the conference ended.

Metrics for conference participants

The following table lists the information provided in the User Activity Report provides for each participant in a conference.

Metrics for conference participants

Name	Can you sort on this item?	Description
Role	No	Conference role (for example, Presenter) for the user.
Participant	No	SIP address of the user.
Connectivity	No	Network connection type. For example "From Internal" for internal connection or "From PSTN" for dial-in users.

Join time	No	Date and time that the user joined the conference.
Leave time	No	Date and time that the user left the conference.
Diagnostic ID	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

1.7.20.4.4 Call Diagnostic Reports

Call Diagnostic Reports

Operations > Monitoring and Health Configuration > Using Monitoring Reports >

Topic Last Modified: *2012-10-21*

The Call Diagnostic Reports provide summary information and diagnostic data for failed peer-to-peer and conferencing sessions.

- Call Diagnostic Summary Report Provides an overall summary of failed peer-to-peer sessions and conference sessions. Peer-to-peer sessions are sessions that involve just two participants. Conferencing sessions involve three or more participants.
- Peer-to-Peer Activity Diagnostic Report Provides an overall trend view of failed peer-to-peer sessions. A peer-to-peer session involves just two participants.
- Conference Diagnostic Report Provides an overall trend view of failed conferencing sessions and trend views for each conference modality. Conferencing sessions involve at least three participants.
- Top Failures Report Provides a list of the most frequent failures and their trends over time.
- Failure Distribution Report Provides an analysis of failed sessions.
- Failure List Report Provides detailed information about the individual participants involved in a failed conference.
- Diagnostic Report Provides diagnostic and troubleshooting information (including SIP response codes and diagnostic headers and IDs) for failed sessions.

1.7.20.4.4.1 Call Diagnostic Summary Report

Call Diagnostic Summary Report

Monitoring and Health Configuration > Using Monitoring Reports > Call Diagnostic Reports >

Topic Last Modified: *2012-06-06*

The Call Diagnostic Summary Report provides an overall look at failed peer-to-peer and conferencing sessions. The report shows the overall failure rate for both types of sessions, and further breaks the failure information down by session modality type:

- Instant messaging
- Application sharing
- File transfer
- Audio
- Video

Accessing the Call Diagnostic Summary Report

The Call Diagnostic Summary Report is accessed from the Monitoring Reports Home page. From the Call Diagnostic Summary Report you can access the Peer-to-Peer Activity Diagnostic Report by clicking the Failure rate metric under the Peer-to-Peer Session Summary section of the report. You can also access the Conference Diagnostic Report by clicking any of the following conference metrics:

- Overall session failure rate
- Focus failure rate
- MCU failure rate

Making the Best Use of the Call Diagnostic Summary Report

The Call Diagnostic Summary Report includes graphs that compare failure rates for the various modalities used in Microsoft Lync Server 2013. The columns in these graphs are actually hotlinks; for example, if you click the Instant messaging column for peer-to-peer sessions, you'll drill down to an instance of the Peer-to-Peer Activity Diagnostic Report, a report that provides additional details about all the instant messaging sessions included in the Call Diagnostic Summary Report.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Call Diagnostic Summary Report enables you to filter on such things as the Registrar pool or Edge Server used in the session. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Call Diagnostic Summary Report.

Call Diagnostic Summary Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date:

	7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click **[All]** to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.

Metrics for Peer-to-Peer Sessions

The following table lists the information provided in the Call Diagnostic Summary Report for peer-to-peer sessions (that is, sessions involving just two participants).

Metrics for Peer-to-Peer Sessions

Name	Can you sort on this item?	Description
Total sessions	No	Total number of peer-to-peer sessions conducted.
Failure rate	No	Percentage of peer-to-peer sessions that failed. When you click this item, the report shows the Peer-to-Peer Activity Diagnostic report, which displays more detailed information about the failed peer-to-peer sessions.

Metrics for Conferencing Sessions

The following table lists the information provided in the Call Diagnostic Report for conferencing sessions (that is, sessions involving three or more participants).

Metrics for Conferencing Sessions

Name	Can you sort on this item?	Description
Total conferences	No	Total number of conferences conducted.
Total conference sessions	No	Total number of conferencing sessions conducted.
Overall session failure rate	No	Percentage of the total conferencing sessions that failed.
Focus sessions	No	Total number of Focus-based conferencing sessions that failed.
Focus failure rate	No	Percentage of the Focus-based conferencing sessions that failed.
MCU sessions	No	Total number of conferencing server-based (formerly known as Multipoint Control Unit or MCU) conferences that failed.
MCU failure rate	No	Percentage of the conferencing server-based (formerly known as Multipoint Control Unit or MCU) conferences that failed.

Conference Summary Subreport

Using Monitoring Reports > Call Diagnostic Reports > Call Diagnostic Summary Report >

Topic Last Modified: *2012-06-06*

The Conference Summary Subreport provides an overall view of failed conference sessions. These failed sessions are further broken down by session type: Focus sessions and MCU sessions.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Conference Summary Subreport.

Conference Summary Subreport Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not

	have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click **[All]** to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.

Metrics

The following table lists the information provided in the Conference Summary Subreport.

Conference Summary Subreport Metrics

Name	Can you sort on this item?	Description
Total conferences	No	Total number of conferences held.
Total conference sessions	No	Total number of conference sessions. A single conference can have multiple sessions; for example, a conference might include both a Focus session and an MCU session.
Overall session failure rate	No	Percentage of all conferences that failed.
Focus sessions	No	Total number of Focus sessions.
Focus failure rate	No	Percentage of Focus sessions that failed.
MCU sessions	No	Total number of MCU sessions.
MCU failure rate	No	Percentage of MCU sessions that failed.
MCU sessions by modality	No	Total number of MCU sessions, grouped by modality (for example, IM conferencing).
Failure rate by modality	No	Percentage of MCU sessions that failed, grouped by modality (for example, IM conferencing).

P2P Summary Subreport

Using Monitoring Reports > Call Diagnostic Reports > Call Diagnostic Summary Report >

Topic Last Modified: *2012-10-21*

The P2P Summary Subreport provides an overall view of your failed peer-to-peer communication sessions.

Filters

Filters provide a way for you to return a more finely targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the P2P Summary Subreport.

P2P Summary Subreport Filters

Name	Description
From	Start date and time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date and time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month):

	7/3/2012 Weeks always run from Sunday through Saturday.
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click **[All]** to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.

Metrics

The following table lists the information provided in the P2P Summary Subreport.

P2P Summary Subreport Metrics

Name	Can you sort on this item?	Description
Total sessions	No	Total number of sessions, including successful sessions, failed sessions (both expected failures and unexpected failures), and uncategorized sessions.
Failure rate	No	Percentage of peer-to-peer sessions that failed.
Sessions by Modality	No	Total number of sessions grouped by modality (for example, instant messaging).
Failure rate by modality	No	Total number of failed sessions grouped by modality (for example, instant messaging).

1.7.20.4.4.2 Peer-to-Peer Activity Diagnostic Report

Peer-to-Peer Activity Diagnostic Report

Monitoring and Health Configuration > Using Monitoring Reports > Call Diagnostic Reports >

Topic Last Modified: *2012-10-01*

The Peer-to-Peer Activity Diagnostic Report provides information about the success and failure of your peer-to-peer communication sessions. Note that Microsoft Lync Server 2013 distinguishes between different kinds of failure:

- **Expected failure**. An expected failure is typically a failure only in the most technical sense. For example, suppose you call someone, but he or she is away from the office and is unable to answer the phone. Because the call was not answered, the call is technically considered a failure. On the other hand, this was an expected failure: Microsoft Lync Server 2013 does not expect you to answer the phone if you're not available to answer the phone. Likewise, an expected failure will occur if you attempt to send an instant message to a user

who is offline, or is logged on only to a phone that does not support instant messaging.
- **Unexpected failure**. An unexpected error is exactly what the name implies: an error that, based on the circumstances, you would not expect to occur. For example, suppose you call someone and that person is available to answer the call; however, when Lync Server 2013 tries to route your call to voicemail the call fails because connectivity to Exchange Unified Messaging has been lost. That's an unexpected error: you would expect that calls could always be routed to voicemail. As a general rule, unexpected failures are true failures: they are problems that likely cannot be remedied through user education or similar measures.

Note that the Success, Expected failure, and Unexpected failure metrics might not add up to the Total sessions metric. For example, in the preceding illustration, we have the following values:

Successes	Expected failures	Unexpected failures	Total sessions
2024	469	16	2521

If you add 2024 + 469 + 16 you get a total of 2,509 sessions, yet the Total sessions column shows a total of 2,521 sessions. The "missing" 12 sessions are sessions that the system was unable to categorize as successful or unsuccessful. That will sometimes be the case when a third-party product introduces a new diagnostic code that is unfamiliar to Lync Server. When that happens, calls made using that product, and reporting that diagnostic code, cannot always be categorized as being a Success, an Expected failure, or an Unexpected failure.

Accessing the Peer-to-Peer Activity Diagnostic Report

The Peer-to-Peer Diagnostic Report is accessed from the Monitoring Reports home page. You can access the Failure Distribution Report by clicking either of the following metrics:

- Unexpected failure volume
- Expected failure volume

Making the Best Use of the Peer-to-Peer Activity Diagnostic Report

There are a number of ways you can filter the Peer-to-Peer Activity Diagnostic Report but, by default, those filtering options are hidden from view. To view the filtering options available to you, click the Show/Hide Parameters button in the upper right-hand corner of the report window. Once you do that the filtering options will be available for use.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Peer-to-Peer Activity Diagnostic Report enables you to filter on such things as the session modality (for example, instant messaging, file transfer, or application sharing). You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Peer-to-Peer Activity Diagnostic Report.

Peer-to-Peer Activity Diagnostic Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is

	displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click **[All]** to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.
Modality	Indicates the type of communication activity that took place. Select one of the following: • [All] • Instant messaging • File transfer • Application sharing • Audio • Video

Metrics (per modality)

The following table lists the information provided in the Peer-to-Peer Activity Diagnostic Report for each modality.

Metrics (per modality)

Name	Can you sort on this item?	Description
Success volume	No	Total number of successful peer-to-peer sessions.
Success percentage	No	Percentage of peer-to-peer sessions that completed with significant problems. Calculated by dividing the Success volume by the Total sessions.
Expected failure volume	No	Total number of sessions where an "expected failure" occurred. An expected failure is a failure that is expected to happen. For example, if a user has set his or her status to Do Not Disturb you would expect any call to that user to fail.
Expected failure percentage	No	Percentage of peer-to-peer sessions that experienced an expected error. Calculated by dividing the Expected failure volume by the Total sessions.
Unexpected failure volume	No	Total number of sessions where an "unexpected failure" occurred.

		An unexpected failure is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.
Unexpected failure percentage	No	Percentage of peer-to-peer sessions that experienced an unexpected error. Calculated by dividing the Unexpected failure volume by the Total sessions.
Total sessions	No	Total number of sessions, including successful sessions, failed sessions (both expected failures and unexpected failures), and uncategorized sessions.

1.7.20.4.4.3 Conference Diagnostic Report

Conference Diagnostic Report

Monitoring and Health Configuration > Using Monitoring Reports > Call Diagnostic Reports >

***Topic Last Modified:** 2012-10-22*

The Conference Diagnostic Report provides information about the success and failure of all conferencing sessions. Note that Microsoft Lync Server distinguishes between different kinds of failure:

- **Expected failure**. An expected failure is typically a failure only in the most technical sense. For example, suppose someone starts a conference but hangs up before anyone can join. Technically that's a failure: the conference was initiated, but not completed. However, that's a failure that you would expect to happen: if the organizer cancels the conference before anyone can join then you would not expect that conference to be completed.
- **Unexpected failure**. An unexpected error is exactly what the name implies: an error that, based on the circumstances, you would not expect to occur. For example, suppose a conference could not be held because the organizer's meeting policy could not be retrieved. That's an unexpected error: after all, you should always be able to retrieve a user's meeting policy.

Note that the Success, Expected failure, and Unexpected failure metrics might not add up to the Total sessions metric. For example, you might see the following values in the Report:

Successes	Expected failures	Unexpected failures	Total sessions
2024	469	16	2521

If you add 2024 + 469 + 16 you get a total of 2,509 sessions and yet, the Total sessions column shows a total of 2,521 sessions. The "missing" 12 sessions for are sessions that the system was unable to categorize as successful or unsuccessful. That will sometimes be the case when a third-party product introduces a new diagnostic code that is unfamiliar to Monitoring Server. When that happens, calls made using that product, and reporting that diagnostic code, cannot always be categorized as being a Success, an Expected failure, or an Unexpected failure.

Accessing the Conference Diagnostic Report

The Conference Diagnostic Report is accessed from the Monitoring Reports home page. You can access the Failure Distribution Report by clicking either of the following metrics:

- Unexpected failure volume
- Expected failure volume

Making the Best Use of the Conference Diagnostic Report

The Conference Diagnostic Report includes a series of graphs. Each of the columns shown in the graph is actually a hyperlink. If you click a column, you'll drill down to the Failure Distribution Report for that time period and that conference type.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Conference Diagnostic Report enables you to filter on such things as the type of conference being conducted (for example, a Focus-based conference) or by the Edge Server used in the conference. You can also choose how data should be grouped. In this case, conferences are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Conference Diagnostic Report.

Conference Diagnostic Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012

	Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) • Monthly (a maximum of 12 months can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click **[All]** to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.
Conference sessions	Indicates the type of conferencing session. Select one of the following: • [All] • Focus sessions • All MCU sessions • IM conferencing • Application sharing • A/V conferencing

Metrics

The following table lists the information provided in the Conference Diagnostic Report for each type of conferencing session.

Conference Diagnostic Report Metrics

Name	Can you sort on this item?	Description
Success volume	No	Total number of successful conferences.
Success percentage	No	Percentage of conferences that completed with significant problems. Calculated by dividing the Success volume by the Total sessions.
Expected failure volume	No	Total number of conferences where an "expected failure" occurred. An expected failure is a failure that is expected to happen. For example, if a user has set his or her status to Do Not Disturb you would expect any call to that user to fail.
Expected failure percentage	No	Percentage of conferences that experienced an expected error. Calculated by dividing the Expected failure volume by the Total sessions.
Unexpected failure volume	No	Total number of conferences where an "unexpected failure" occurred. An unexpected failure is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.
Unexpected failure percentage	No	Percentage of conferences that experienced an unexpected error. Calculated by dividing the Unexpected failure volume by the Total sessions.
Total sessions	No	Total number of conferences, including successful conferences, failed

		conferences (both expected failures and unexpected failures), and uncategorized conferences.

1.7.20.4.4.4 Top Failures Report

Top Failures Report

Monitoring and Health Configuration > Using Monitoring Reports > Call Diagnostic Reports >

Topic Last Modified: *2012-10-01*

The Top Failures Report provides a look at the most-commonly reported failures and their trends over time. Failures are based on a combination of the following two metrics:

- **Diagnostic ID**. Unique identifier (in the form of an ms-diagnostics header) that is attached to a SIP message. Diagnostic IDs provide information useful in troubleshooting call-related problems.
- **Response code**. Response codes are used in SIP communication sessions to respond to SIP requests. For example, suppose Ken sends the INVITE request to Pilar Ackerman (that is, suppose Ken Myer calls Pilar Ackerman). If Pilar answers, her phone will send the response code 200 (OK), letting Ken's phone know that Pilar has answered. The Top Failures Report only includes response codes that were sent in response to a call failure; Lync Server does not keep track of all the response codes issued during the course of a call.

Information is reported not only for the total number of sessions where a failure occurred but also for the total number of users who were impacted by the failure.

Accessing the Top Failures Report

The Top Failures Report is accessed from the Monitoring Reports home page. Clicking the Reported sessions metric will take you to the Failure Distribution Report.

Making the Best Use of the Top Failures Report

The Top Failures Report is unusual in one regard: it allows you to filter on as many as 5 diagnostic IDs at once. (Typically you can only filter on one item – such as one user SIP address – at a time.) To filter on multiple diagnostic IDs, simply enter each ID in the Diagnostic IDs box, separating the IDs by using commas. (If you want to, you can leave a blank space after each comma.) For example:

1011, 2412, 1033, 52116, 1008

Do that, and only failed calls that reported at least one of those five diagnostic IDs will be displayed.

If you hold your mouse over a Response code you'll see a tooltip that tells you what the Response code in question means. For example, if you hold the mouse over the Response code 486 you'll see this message:

Busy Here.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Top Failures Report enables you to filter the returned data based on such things as the activity type (peer-to-peer session or conferencing session) or by the SIP response code that accompanied the failed session. You can also choose how data should be grouped. In this case, usages are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Top Failures Report.

Top Failures Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Activity type	Type of activity. Select one of the following: • [All] • Peer-to-peer

	- Conference
Modality	At this time the only option available is **[All]**.
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click **[All]** to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.
Category	Type of failure experienced. Select one of the following: • Both expected and unexpected failure • Unexpected failure An "expected failure" is a failure that is expected to happen. For example, if a user has set his or her status to Do Not Disturb you would expect any call to that user to fail. An "unexpected failure" is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.
Response code	SIP response code sent when the conference failed. Enter the entire response code For example: 400
Diagnostic ID	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

Metrics

The following table lists the information provided in the Top Failures Report.

Top Failures Report Metrics

Name	Can you sort on this item?	Description
Rank	Yes	Relative rank based on the number of reported sessions.
Reported sessions	Yes	Total number of failed sessions based on diagnostic ID and SIP response code.
Users impacted	Yes	Total number of users affected by the failed session.
Failure information	No	Detailed information about

		the failure, including diagnostic ID, SIP response code, and description of why the session failed.
Trend in the past	No	Graphs failed sessions over time.

1.7.20.4.4.5 Failure Distribution Report

Failure Distribution Report

Monitoring and Health Configuration > Using Monitoring Reports > Call Diagnostic Reports >

Topic Last Modified: *2012-10-21*

The Failure Distribution Report ranks failed sessions in the following categories:

- Top diagnostic reasons
- Top modalities
- Top pools
- Top sources
- Top components
- Top from users
- Top to users
- Top from user agents

You can use these categories to determine exactly where a problem is occurring and, in some cases, why the problem is occurring. For example, suppose you recorded 242 failed audio/video sessions during a given day. If you look at the Failure Distribution Report, it might show that 237 of those failed sessions took place in your Dublin pool. That gives you a good place to start when it comes to tracking down and diagnosing the causes behind those failures. If you click on the Dublin pool under the **Top pools** category, you will see a Failure Distribution Report just for that pool. You can then begin analyzing why the Dublin pool was experiencing so many difficulties.

Viewing the Failure Distribution Report

You can access the Failure Distribution Report from any of the following reports by clicking either the **Expected failure volume** or the **Unexpected failure volume** metric:

- Top Failures Report
- Conference Diagnostic Report
- Peer-to-Peer Activity Diagnostic Report

From the Failure Distribution Report, you can click any of the following metrics to view the Failure List Report:

- Top diagnostic reasons (sessions)
- Top modalities (sessions)
- Top pools (sessions)
- Top sources (sessions)
- Top components (sessions)
- Top from users (sessions)
- Top to users (sessions)
- Top from user agents (sessions)

Using the Failure Distribution Report

Depending on your monitor size and screen resolution, it's possible that some of the data shown in the Failure Distribution Report might be truncated when you view it onscreen. This is especially true for metrics such as user agents, which can have very long labels. For example, a user agent with a name like "UCCAPI/4.0.7400.0 OC/4.0.7400.0 (Microsoft Lync 2013)" might only partially appear onscreen:

UCCAPI/4.0.7400.0 OC/4.0.7400.0 (Microsoft Ly...

Fortunately, you can see the entire label simply by holding your mouse over the truncated value.

One interesting metric that you can filter on by using the Failure Distribution Report is Diagnostic ID. If you see the same Diagnostic ID cropping up in other reports you can filter on that ID in the Failure Distribution Report and get a very detailed look at exactly where, and how often, that ID has been reported during a failed session.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Failed Distribution Report enables you to filter on such things as the activity type (peer-to-peer session or conferencing session) or by the diagnostic ID that accompanied each failed session.

The following table lists the filters that you can use with the Failure Distribution Report.

Failure Distribution Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012

	To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Pool	Fully qualified domain name (FQDN) of the Registrar pool or Edge Server. You can either select an individual pool or click **[All]** to view data for all the pools. This drop-down list is automatically populated for you based on the records in the database.
Activity type	Type of activity to filter on. Select one of the following: • [All] • Peer-to-peer • Conference
Session category	Indicates whether the activity in question succeeded or failed. Select one of the following: • [All] • Success • Expected failure • Unexpected failure An "expected failure" is a failure that is expected to happen. For example, if a user has set his or her status to Do Not Disturb you would expect any call to that user to fail. An "unexpected failure" is a failure that occurs in what would appear to be an otherwise healthy system. For example, a call should not be terminated if the caller is placed on hold. If that occurs, that would be flagged as an unexpected failure.
Diagnostic ID	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors. Diagnostics headers are optional (it is possible to have SIP sessions that do not include these headers), and diagnostic IDs are reported only for sessions that experienced problems of some kind.

Metrics for Top Diagnostic Reasons

The following table lists the information provided in the Failure Distribution Report based on the most frequently reported diagnostic ID.

Metrics for Top Diagnostic Reasons

Name	Can you sort on this item?	Description
Rank	No	Relative ranking of failed sessions based on diagnostic

		IDs. The diagnostic ID is a unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.
Top diagnostic reasons	No	Diagnostic ID generated in a session.
Sessions	No	Total number of failed sessions where the specified diagnostic ID was generated.

Metrics for Top Modalities

The following table lists the information provided in the Failure Distribution Report based on the session modalities that experienced the most failures.

Metrics for Top Modalities

Name	Can you sort on this item?	Description
Rank	No	Relative ranking based of failed session based on session type (for example, an audio/video conference or a peer-to-peer file transfer session).
Top modalities	No	Session type.
Sessions	No	Total number of failed sessions involving the specified modality.

Metrics for Top Pools

The following table lists the information provided in the Failure Distribution Report based on the pools that experienced the most failures.

Metrics for Top Pools

Name	Can you sort on this item?	Description
Rank	No	Relative ranking of failed sessions based on the Registrar pool or Edge Server where the session was conducted.
Top pools	No	Name of the Registrar pool or Edge Server.
Sessions	No	Total number of failed sessions per Registrar pool or Edge Server.

Metrics for Top Sources

The following table lists the information provided in the Failure Distribution Report based on the computers that experienced the most failures.

Metrics for Top Sources

Name	Can you sort on this item?	Description
Rank	No	Relative ranking failed sessions per computer.
Top sources	No	Name of the computer involved in the failed session.
Sessions	No	Total number of failed sessions per computer.

Metrics for Top Components

The following table lists the information provided in the Failure Distribution Report based on the Microsoft Lync Server 2010 components that experienced the most failures.

Metrics for Top Components

Name	Can you sort on this item?	Description
Rank	No	Relative ranking of failed sessions based on Lync Server 2010 component (for example, ExumRouting, GroupChat, or MediationServer).
Top components	No	Name of the component involved in the failed session.
Sessions	No	Total number of failed sessions per component.

Metrics for Top From Users

The following table lists the information provided in the Failure Distribution Report based on users who experienced the most failures when they tried to call someone else (known as "From" users).

Metrics for Top From Users

Name	Can you sort on this item?	Description
Rank	No	Relative ranking of failed sessions based on the user who was invited to join the session.
Top from users	No	SIP address of the user invited to join the session.
Sessions	No	Total number of failed sessions per user.

Metrics for Top To Users

The following table lists the information provided in the Failure Distribution Report based on the users who experienced the most failures when another user tried to call them (known as "To" users).

Name	Can you sort on this item?	Description
Rank	No	Relative ranking of failed sessions based on the user who initiated the session.
Top to users	No	SIP address of the user who initiated the session.
Sessions	No	Total number of failed sessions per user.

Metrics for Top User Agents

The following table lists the information provided in the Failure Distribution Report based on the endpoint software that experienced the most failures.

Metrics for Top User Agents

Name	Can you sort on this item?	Description
Rank	No	Relative ranking of failed sessions based on the user agent (software) involved in the session. For example: RTCC/4.0.0.0 Inbound Routing/4.0.0.0.
Top user agents	No	Name of the user agent involved in the failed session.
Sessions	No	Total number of failed sessions per user agent.

1.7.20.4.4.6 Failure List Report

Failure List Report

Monitoring and Health Configuration > Using Monitoring Reports > Call Diagnostic Reports >

Topic Last Modified: *2012-07-02*

The Failure List report provides information about the individual participants who took part in a failed peer-to-peer or conferencing session. This information includes the URI of the user who experienced the problem, as well as the SIP Response code and Diagnostic ID associated with the failure.

Accessing the Failure List Report

The Failure List Report is accessed by clicking any of the following metrics on the Failure Distribution Report:

- Top diagnostic reasons (sessions)
- Top modalities (sessions)

- Top pools (sessions)
- Top sources (sessions)
- Top components (sessions)
- Top from users (sessions)
- Top to users (sessions)
- Top from user agents (sessions)

From the Failure List Report you can access the Peer-to-Peer Session Detail Report by clicking the Session detail metric for a peer-to-peer session. You can also access the Conference Detail Report by clicking the Conference metric for a conference.

Making the Best Use of the Failure List Report

In the Failure List Report, you can view a description for each Response code or each Diagnostic ID simply by holding your mouse over that value. For example, if you hold your mouse over Diagnostic ID 7025 you'll see the following displayed in a tooltip:

Internal server error creating media for user.

It's important to note that the Failure List Report does not provide a straightforward way to directly retrieve a list of all the users who participated in at least one failed session, nor does it provide a way to determine which users were most-often involved in a failed session. (For one thing, the Failure List Report has no filtering capabilities.) However, if you export the data and then convert it to a comma-separated values file, you can use Windows PowerShell to find the answers to questions like those. For example, suppose you save the data to a .CSV file named C:\Data\Failure_List.csv. Based on the data saved in that file, this command lists all the users who were involved in at least one failed session:

```
$failures = Import-Csv -Path " C:\Data\Failure_List.csv"
$failure |Sort-Object "From user" | Select-Object "From user" -Unique
```

That command will return a list similar to this:

```
From user
----
Pilar.Ackerman@litwareinc.com
Henrik.Jensen@litwareinc.com
Gilead.Amosnino@litwareinc.com
David.Ahs@litwareinc.com
Ken.Myer@litwareinc.com
```

These two commands report back the total number of failed sessions that each user was involved in:

```
$failures = Import-Csv -Path "C:\Data\Failure_List.csv"
$failures | Group-Object "From user" | Select-Object Count, Name | Sort-Object -P
```

That will return data similar to this:

```
Count    Name
 -----    ----
    20    Pilar.Ackerman@litwareinc.com
    20    David.Ahs@litwareinc.com
    16    Gilead.Amosnino@litwareinc.com
    16    Ken.Myero@litwareinc.com
    14    Henrik.Jensen@litwareinc.com
```

Filters

None. You cannot filter the Failure List Report.

Metrics

The following table lists the information provided in the Failure List Report for each failed call.

Failure List Report Metrics

Name	Can you sort on this item?	Description
Reported time	No	Date and time the report was recorded.
Request	No	SIP request type that failed. For example, INVITE or BYE.
Response code	No	SIP response code sent when the conference failed.
Diagnostic ID	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.
Join cost time (ms)	No	Amount of time (in milliseconds) required for the user to join the conference.
From user	No	SIP address of the user who initiated the call.
From user agent	No	Software used by the endpoint of the user who initiated the call.
To user	No	SIP address of the user who was being called.

1.7.20.4.4.7 Diagnostic Report

Diagnostic Report

Monitoring and Health Configuration > Using Monitoring Reports > Call Diagnostic Reports >

Topic Last Modified: *2012-07-02*

The Diagnostic Report provides diagnostic and troubleshooting information for a failed session. This information includes both the Diagnostic ID and the Diagnostic header that were reported when the session failed. The Diagnostic ID is a unique identifier (in the form of an ms-diagnostics header) that gets attached to a SIP message, while the Diagnostic header provides an accompanying description for the Diagnostic ID. The report might also contain valuable troubleshooting details that are known by the reporting component. For example:

- The cause code provided by the PSTN gateway that generated the failure. When an outgoing call fails on the PSTN network, an ISDN User Part (ISUP) cause code is automatically generated. For example, a PSTN gateway might send cause code 34 to indicate that no circuit or channel was available for

completing the call.
- Peer FQDN, port, and Winsock errors for connectivity failures.
- Names being looked up for DNS resolution failures. DNS resolution takes place any time a client contacts a name server and requests the IP address that corresponds to specified device name.

Accessing the Diagnostic Report

The Diagnostic Report can be accessed by clicking the Diagnostic Report (Detail) metric on either the Peer-to-Peer Session Detail Report or the Conference Detail Report.

Filters

None. You cannot filter the Diagnostic Report.

Metrics

The following table lists the information provided in the Diagnostic Report for each session.

Diagnostic Report Metrics

Name	Can you sort on this item?	Description
Report time	No	Date and time that the report was recorded.
Response code	No	SIP response code sent when the session failed.
Request type	No	SIP request type that failed. For example, INVITE, BYE, or SERVICE.
Source	No	Source of the error.
From user URI	No	SIP address of the user who initiated the session.
From user agent	No	Software used by the endpoint of the user who initiated the session.
Diagnostic ID	No	Unique identifier (in the form of an ms-diagnostics header) attached to a SIP message that often provides information useful in troubleshooting errors.
Content type	No	Type of media content that failed. For example, a common content type is Application/sdp. Session Description Protocol (SDP) is a standard Internet protocol used for session announcements, session invitations, and other forms

		of multimedia session initiation.
Application	No	Application involved in the error.
To user URI	No	SIP address of the user who was invited to the session.
Conference join times (ms)	No	Amount of time (in milliseconds) it took for the user to join the conference.
Diagnostic header	No	Diagnostic ID description.

1.7.20.4.5 Media Quality Diagnostic Reports

Media Quality Diagnostic Reports

Operations > Monitoring and Health Configuration > Using Monitoring Reports >

Topic Last Modified: *2013-02-22*

The Media Quality Diagnostic Reports provide information about call quality, and diagnostic and troubleshooting information for failed calls.

- Media Quality Summary Report Provides overall quality data for different endpoint types, including Enterprise Voice peer-to-peer calls, Enterprise Voice conference calls, and calls that rely, at least in part, on the public switched telephone network (PSTN).
- Media Quality Comparison Report Provides a comparison of call quality values for different types of audio calls (for example, calls made over a wireless network vs. calls made across a wired connection).
- Server Performance Report Lists the servers that have experienced the most problems, based on measurements of such key quality metrics as degradation, packet loss, and jitter.
- Location Report Provides a list of network locations and a summary of the media quality of the calls that occur at each location. For purposes of this report, locations are based on IP subnets.
- Device Report Provides a summary of devices that are used for Enterprise Voice calls and it includes the average media quality of the calls by device.
- Call List Report Provides detailed information about phone calls made or received within your organization.
- Call Detail Report Provides detailed information about phone calls made from or received within your organization.
- Server Media Quality Trend Report Provides a way for you to graphically compare up to 5 servers on Quality of Experience metrics such as call volume, poor call percentage, packet loss, and jitter.
- The Media Quality Metrics Distribution Report Provides a graph that shows the distribution values for a Quality of Experience metric such as jitter or packet loss.
- Location Trend Report Provides call quality trend information for network locations.

1.7.20.4.5.1 Media Quality Summary Report

Media Quality Summary Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic Reports >

Topic Last Modified: *2012-10-22*

The Media Quality Summary Report is perhaps your best bet for analyzing call quality in your organization: this report provides detailed Quality of Experience (QoE) call metrics broken down into the following categories:

- UC Peer to Peer Calls (such as a Microsoft Lync 2013 to Microsoft Lync 2013 call)
- UC Conference Sessions
- PSTN Conference Sessions
- PSTN Calls: Media Bypass
- PSTN Calls (Non-Bypass): UC Leg
- PSTN Calls (Non-Bypass): Gateway Leg
- Other Call Types

When you first open the report, you see summary information for each of these categories. Without leaving the report, you can expand each category to look at subcategories such as calls made from Office Communicator 2007 R2 to Lync 2013. In turn, you can then drill down into these subcategories to see details about each call made within that subcategory.

In Microsoft Lync Server 2013 the Media Quality Summary Report further breaks the data down into three call types: audio calls, video calls, and application sharing calls. Each call type has its own section in the report, and its own custom set of call metrics.

The Media Quality Summary Report also allows you to apply filters that enable you to compare the call quality of wired calls vs. wireless calls, internal calls vs. external calls, and VPN calls vs. non-VPN calls.

Accessing the Media Quality Summary Report

The Media Quality Summary Report is accessed from the Monitoring Reports home page. You can drill down to the Call List Report by clicking either of the following metrics:

- Call volume
- Poor call percentage

In addition, you can access the Media Quality Metrics Distribution Report by clicking any of the following audio call metrics:

- Round trip (ms)
- Degradation (MOS)
- Packet loss
- Jitter (ms)
- Healer concealed ratio
- Healer stretched ratio
- Healer compressed ratio

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Media Quality Summary Report enables you to filter the returned data by such things as access type (that is, interval access vs.

external access) or by wired/wireless network connection. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Media Quality Summary Report.

Media Quality Summary Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Access type	Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following: • [All] • Internal • External
Network type	Indicates the type of network the client was connected to when the call was placed. Select one of the following:

	- [All] - Wired - Wireless
VPN	Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: - [All] - VPN - Non-VPN

Metrics

The following table lists the information provided in the Media Quality Summary Report.

Media Quality Summary Report Metrics: Audio Call Summary

Name	**Can you sort on this item?**	**Description**
Call type/Endpoint type	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: - UC Peer-to-Peer Calls - UC Conference Sessions - PSTN Conference Sessions - PSTN Calls: Media Bypass - PSTN Calls (Non-Bypass): UC Leg - PSTN Calls (Non-Bypass): Gateway Leg - Other Call Types
Call volume	No	Total number of calls per call type.
Poor call percentage	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Call volume (wireless call)	No	Total number of calls that used a wireless connection.
Call volume (VPN call)	No	Total number of calls that used a VPN connection.
Call volume (external call)	No	Number of calls that used an external connection (that is, a connection outside the internal network).
Round trip (ms)	No	Average amount of (in milliseconds) required for a real-time transport protocol (RTP) packet to travel to another endpoint and then back. Round-trip times of 100 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing, a routing

		misconfiguration, or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.
Degradation (MOS)	No	Average amount of mean opinion score (MOS) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0. A value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users rate the quality of a call on a scale of 1-to-5. In Lync Server, Lync Server uses a set of algorithms to predict how users would have rated a call. High degradation values can be caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.
Packet loss	No	Average rate of RTP packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.
Jitter (ms)	No	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
Healer concealed ratio	No	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.
Healer stretched ratio	No	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio

		is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.
Healer compressed ratio	No	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

Media Quality Summary Report Metrics: Video Call Summary

Name	Can you sort on this item?	Description
Call type/Endpoint type	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: • UC Peer-to-Peer Calls • UC Conference Sessions • PSTN Conference Sessions • PSTN Calls: Media Bypass • PSTN Calls (Non-Bypass): UC Leg • PSTN Calls (Non-Bypass): Gateway Leg • Other Call Types
Call volume	No	Total number of calls per call type.
Poor call percentage	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Call volume (wireless call)	No	Total number of calls that used a wireless connection.
Call volume (VPN call)	No	Total number of calls that used a VPN connection.
Call volume (external call)	No	Number of calls that used an external connection (that is, a connection outside the internal network).
Avg bit-rate (Kbits/s)	No	Average video bit rate (in kilobits per second).
Low bit-rate %	No	Percentage of the call where the bit rate was low.

Outbound packet loss	No	Real-Time Transport Protocol (RTP) packet loss for outbound packets. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.
Frozen frame %	No	Percentage of "frozen" frames. In a frozen frame, the video stops advancing while the audio portion of the call continues.
Outbound avg frame rate	No	Average frame rate for outbound transmissions during the call.
Inbound avg frame rate	No	Average frame rate for incoming transmissions during the call.
Inbound low frame rate %	No	Percentage of the call where the bit rate for incoming video was low.
Client health %		Indicates the relative health of the client device during the call.

Media Quality Summary Report Metrics: Application Sharing Call Summary

Name	Can you sort on this item?	Description
Call type/Endpoint type	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: • UC Peer-to-Peer Calls • UC Conference Sessions • PSTN Conference Sessions • PSTN Calls: Media Bypass • PSTN Calls (Non-Bypass): UC Leg • PSTN Calls (Non-Bypass): Gateway Leg • Other Call Types
Call volume	No	Total number of calls per call type.
Poor call percentage	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Call volume (wireless call)	No	Total number of calls that used a wireless connection.
Call volume (VPN call)	No	Total number of calls that used a VPN

		connection.
Call volume (external call)	No	Number of calls that used an external connection (that is, a connection outside the internal network).
Jitter (ms)	No	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
Avg. relative one way	No	Average relative one-way delay between two media endpoints. This is a single-hop latency measure.
Avg. RDP tile processing latency	No	The average RDP tile processing latency in the AS Conferencing Server over the duration of the viewing session. This metric does not cover network latency. A high average reflects a longer delay in the viewing experience. An overloaded conferencing server may experience higher average delays.
Total spoiled tile %	No	Total percentage of spoiled RDP tiles.

1.7.20.4.5.2 Media Quality Comparison Report

Media Quality Comparison Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic Reports >

Topic Last Modified: *2012-10-01*

The Media Quality Comparison Report enables you to compare call quality values for different types of audio calls (for example, calls made over a wireless network vs. calls made across a wired connection).

Accessing the Media Quality Comparison Report

The Media Quality Comparison Report is accessed from the Monitoring Reports home page.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Media Quality Comparison Report.

Media Quality Comparison Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Calls	Type of call to be used as the main comparison item. Allowed values are: • [All] • External • Internal • VPN • Non-VPN • Wired • Wireless • External and wired • External and wireless • External and VPN • External and non-VPN • Internal and wired • Internal and wireless

Compare with calls	Type of call to be used as the secondary comparison item. Allowed values are: • [All] • External • Internal • VPN • Non-VPN • Wired • Wireless • External and wired • External and wireless • External and VPN • External and non-VPN • Internal and wired • Internal and wireless
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 7/7/2012 and an end date of 2/28/2012, data is displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).

Metrics

The following table lists the information provided in the Media Quality Comparison Report.

Media Quality Comparison Report Metrics

Name	**Can you sort on this item?**	**Description**
Call volume	No	Total number of calls.
Degradation (MOS)	No	Average amount of MOS (mean option score) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0; a value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users rate the quality of a call on a scale of 1-to-5. Lync Server uses a set of algorithms to predict how users would

		have rated a call. High degradation values can be caused by congestion; lack of bandwidth; wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.
Poor call percentage	No	The total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Round trip (ms)	No	Average amount of (in milliseconds) required for a Real-Time Transport Protocol packet to travel to another endpoint and then back. Round-trip times of 200 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing; a routing misconfiguration; or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.
Packet loss	No	Average rate of Real-Time Transport Protocol (RTP) packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion; lack of bandwidth; wireless congestion or interference; or an overloaded media server. Packet loss typically results in distorted or lost audio.
Jitter (ms)	No	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High

		jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
Healer concealed ratio	No	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.
Healer stretched ratio	No	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.
Healer compressed ratio	No	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

1.7.20.4.5.3 Server Performance Report

Server Performance Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic Reports >

Topic Last Modified: *2012-10-01*

The Server Performance Report provides a list of Microsoft Lync Server 2013 servers that have experienced the highest-percentage of poor calls. The report breaks down servers by server type, reporting separate statistics for the following types:

- Mediation Server
- A/V Conferencing Server
- A/V Edge Server
- Gateway (Mediation Server)
- Gateway (Mediation Server bypass)
- Video (including video metrics for A/V Conferencing servers and A/V Edge servers)
- Application Sharing (including application sharing metrics for A/V Conferencing servers and A/V Edge servers)

It's important to note that the ranking shown in this report as relative rankings. For example, suppose your worst-performing server had one poor call among its 1,000 placed calls. That's a more-than-acceptable percentage of .1%. However, if that's the worst-performing server you have (that is, if all your other servers have a poor call percentage even lower than .1%), then that server will still appear on the Server Performance Report.

Accessing the Server Performance Report

The Server Performance Report is accessed from the Monitoring Reports home page. You can drill down to the Call List Report by clicking either of the following metrics:

- Call volume
- Poor call percentage

In addition, you can drill down to the Server Media Quality Trend Report by clicking the following metric:

- Trend

Making the Best Use of the Server Performance Report

The Server Performance Report provides a number of ways to filter data; for example, you can filter on network type (calls made from a wired connection vs. calls made from a wireless connection) and access type (calls made from inside the firewall vs. calls made from outside the firewall). It's a good idea when viewing the server performance report to make use of these filters. For example, suppose you have a Mediation Server that has a poor call percentage of 3.24%. If you look solely at wireless calls, that same server might have a poor call percentage approaching 20%. That means that the server was having difficulty with wireless calls, a problem that is partially obscured because the server was not having problems with wired calls.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Server Performance Report enables you to do such things as filter the returned data by server type or by network type (that is, wired or wireless). You can also choose how data should be grouped. In this case, data is grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Server Performance Report.

Server Performance Report Filters

Name	Description

From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Server type	Indicates the type of server whose performance should be reported. Select one of the following: 1.[All] 2.Mediation Server 3.A/V Conferencing Server 4.A/V Edge Server
Top N	Indicates the number of servers (based on their poor call percentage) to be displayed in each category. For example, if you select **5** then the five poorest-performing servers are displayed. Select one of the following: 1.[All] 2.5 3.10
Access type	Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following: 1.[All] 2.Internal

	3.External
Network type	Indicates the type of network the client was connected to when the call was placed. Select one of the following: 1.[All] 2.Wired 3.Wireless
VPN	Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: 1.[All] 2.VPN 3.Non-VPN

Metrics

The following table lists the information provided in the Server Performance Report.

Server Performance Report Metrics: Audio Call Summary

Name	Can Sort On	Description
Server	No	Name/IP address of the server.
Call volume	No	Total number of calls made.
Poor call percentage	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Round trip (ms)	Yes	Average amount of (in milliseconds) required for a real-time transport protocol (RTP) packet to travel to another endpoint and then back. Round-trip times of 100 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing; a routing misconfiguration; or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.
Degradation (MOS)	Yes	Average amount of mean opinion score (MOS) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0. A

		value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users rate the quality of a call on a scale of 1-to-5. In Lync Server, the Monitoring Server uses a set of algorithms to predict how users would have rated a call. High degradation values can be caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.
Packet loss	Yes	Average rate of real-time transport protocol (RTP) packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.
Jitter (ms)	Yes	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
Healer concealed ratio	Yes	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost

		audio.
Healer stretched ratio	Yes	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.
Healer compressed ratio	Yes	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

Server Performance Report Metrics: Video Call Summary

Name	**Can you sort on this item?**	**Description**
Call type/Endpoint type	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: • UC Peer-to-Peer Calls • UC Conference Sessions • PSTN Conference Sessions • PSTN Calls: Media Bypass • PSTN Calls (Non-Bypass): UC Leg • PSTN Calls (Non-Bypass): Gateway Leg • Other Call Types
Call volume	No	Total number of calls per call type.
Poor call percentage	No	Total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Call volume (wireless call)	No	Total number of calls that used a wireless connection.
Call volume (VPN call)	No	Total number of calls that used a VPN connection.

Call volume (external call)	No	Number of calls that used an external connection (that is, a connection outside the internal network).
Avg bit-rate (Kbits/s)	No	Average video bit rate (in kilobits per second).
Low bit-rate %	No	Percentage of the call where the bit rate was low.
Outbound packet loss	No	Real-Time Transport Protocol (RTP) packet loss for outbound packets. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion; lack of bandwidth; wireless congestion or interference; or an overloaded media server. Packet loss typically results in distorted or lost audio.
Frozen frame %	No	Percentage of "frozen" frames. In a frozen frame, the video stops advancing while the audio portion of the call continues.
Outbound avg frame rate	No	Average frame rate for outbound transmissions during the call.
Inbound avg frame rate	No	Average frame rate for incoming transmissions during the call.
Inbound low frame rate %	No	Percentage of the call where the bit rate for incoming video was low.
Client health %		Indicates the relative health of the client device during the call.

Server Performance Report Metrics: Application Sharing Call Summary

Name	Can you sort on this item?	Description
Call type/Endpoint type	No	When you click this item, the report shows detailed information about calls based on that type. Call types include: • UC Peer-to-Peer Calls • UC Conference Sessions • PSTN Conference Sessions • PSTN Calls: Media Bypass • PSTN Calls (Non-Bypass): UC Leg • PSTN Calls (Non-Bypass): Gateway Leg • Other Call Types
Call volume	No	Total number of calls per call type.
Poor call percentage	No	Total number of calls classified as

		poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Call volume (wireless call)	No	Total number of calls that used a wireless connection.
Call volume (VPN call)	No	Total number of calls that used a VPN connection.
Call volume (external call)	No	Number of calls that used an external connection (that is, a connection outside the internal network).
Jitter (ms)	No	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
Avg. relative one way	No	Average relative one-way delay between two media endpoints. This is a single-hop latency measure.
Avg. RDP tile processing latency	No	The average RDP tile processing latency in the AS Conferencing Server over the duration of the viewing session. This metric does not cover network latency. A high average reflects a longer delay in the viewing experience. An overloaded conferencing server may experience higher average delays.
Total spoiled tile %	No	Total percentage of spoiled RDP tiles.

1.7.20.4.5.4 Location Report

Location Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic Reports >

Topic Last Modified: *2012-10-01*

The Location Report provides information about call quality metrics grouped by network location (that is, by network subnet). If your users are experiencing problems with their calls, this report can help you determine if those problems are widespread or if they are largely confined to a given network segment.

Accessing the Location Report

The Location Report is accessed from the Monitoring Reports home page. You can drill down to the Call List Report by clicking either of the following metrics:

- Call volume
- Poor call percentage

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Location Report enables you to filter on such things as the location where a call was originated or whether the call took place on a wireless or a wired connection. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Location Report.

Location Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Caller location	IP subnet of the user who placed the call. You can only select **[All]** to indicate all subnets.
Callee location	IP subnet of the user who received the call. You can only select **[All]** to indicate all subnets.

Network type	Indicates the type of network the client was connected to when the call was placed. Select one of the following: 1. [All] 2. Wired 3. Wireless
VPN	Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: 1. [All] 2. VPN 3. Non-VPN

Metrics

The following table lists the information provided in the Location Report.

Location Report Metrics

Name	Can you sort on this item?	Description
Caller subnet	No	IP subnet of the user who placed the call.
Callee subnet	No	IP subnet of the user who received the call.
Call volume	Yes	Total number of calls placed.
Poor call percentage	Yes	Percentage of calls classified as poor calls. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Round trip (ms)	Yes	Average amount of (in milliseconds) required for a real-time transport protocol (RTP) packet to travel to another endpoint and then back. Round-trip times of 100 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing, a routing misconfiguration, or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.
Degradation (MOS)	Yes	Average amount of mean opinion score (MOS) degradation experienced during a call. Degradation

		values can range from a low of 0.0 to a high of 5.0. A value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users rate the quality of a call on a scale of 1-to-5. In Lync Server, Lync Server uses a set of algorithms to predict how users would have rated a call. High degradation values can be caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.
Packet loss	Yes	Average rate of RTP packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.
Jitter	Yes	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
Healer concealed ratio	Yes	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused

		by packet loss or jitter, and results in distorted or lost audio.
Healer stretched ratio	Yes	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.
Healer compressed ratio	Yes	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

1.7.20.4.5.5 Device Report

Device Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic Reports >

Topic Last Modified: *2012-07-02*

The Device Report might be better titled the Microphone and Speakers Report; that's because the Device Report retrieves call-related metrics (such as poor call percentage, echo, and voice switch time) grouped by the microphones and speakers used in the call. If you are interested in IP phones (also commonly referred to as "devices"), use the IP Phone Inventory Report instead.

The Device Report is extremely useful for administrators in determining if a specific type of device is experiencing high volumes of poor quality calls than others. In turn, this could influence any decisions you must make when it comes time to buy new devices or to replace existing devices.

By default, the information displayed in the Device Report is also based on the microphone (the capture device) and speakers/headset (the render device) used in the call. For example, suppose you have several users who use the following capture device and the following render device: By default, the information displayed in the Device Report is also based on the microphone (the capture device) and speakers/headset (the render device) used in the call. For example, suppose you have several users who use the following capture device and the following render device:

- Capture device -- Microphone (SoundMAX Integrated Digital HD Audio)
- Render device -- Headset Earphone (Microsoft LifeChat LX-3000)

If those users made a total of 254 calls you'll see an entry like this in the report:

Capture device	Render device	Call volume
Microphone (SoundMAX Integrated Digital HD Audio)	Headset Earphone (Microsoft LifeChat LX-3000)	254

Now, suppose you have a number of users who use that same capture device but a different render device. In that case, you'll have a second line entry in the report, one for that unique combination of capture device and render device:

Capture device	Render device	Call volume
Microphone (SoundMAX Integrated Digital HD Audio)	Headset Earphone (Microsoft LifeChat LX-3000)	254
Microphone (SoundMAX Integrated Digital HD Audio)	Speakers (SoundMAX Integrated Digital HD Audio)	319

If you would rather see combined totals for a given device (for example, for the SoundMAX capture device, regardless of the render device used), select the appropriate option from the Device type dropdown list (either Capture device or Render device). If you select Capture device in this example, that will give you output similar to this:

Capture device	Call volume
Microphone (SoundMAX Integrated Digital HD Audio)	573

Accessing the Device Report

The Device Report is typically accessed from the Monitoring Reports home page. However, if you are viewing the Call Detail Report you can drill down to the Device Report for a specific device by clicking either of the following metrics:

- Capture Device
- Render Device

From the Device Report you can drill down to the Call List Report by clicking either of the following metrics:

- Call volume
- Poor call percentage

Making the Best Use of the Device Report

When it comes to device names, the Device Report is extremely detailed; for example, suppose you have the following capture devices:

- Aastra 3002 Microphone (2- Aastra 3002)
- Aastra 3002 Microphone (3- Aastra 3002)
- Aastra 3002 Microphone (Aastra 3002)
- Aastra 6725ip
- Aastra 6725ip Microphone (10- Aastra 6725ip)
- Aastra 6725ip Microphone (10- Aastra 6725ip)-V0
- Aastra 6725ip Microphone (2- Aastra 6725ip)
- Aastra 6725ip Microphone (3- Aastra 6725ip)
- Aastra 6725ip Microphone (4- Aastra 6725ip)
- Aastra 6725ip Microphone (5- Aastra 6725ip)
- Aastra 6725ip Microphone (6- Aastra 6725ip)

- Aastra 6725ip Microphone (7- Aastra 6725ip)
- Aastra 6725ip Microphone (9- Aastra 6725ip)
- Aastra 6725ip Microphone (9- Aastra 6725ip)-V0
- Aastra 6725ip Microphone (Aastra 6725ip)
- Aastra 6725ip Microphone (Aastra 6725ip)-V0
- Aastra 6725ip Microphone (USB Audio Device)
- Aastra 6725ip Microphone (USB Audio Device)-V0

Note:

Keep in mind that capture device names might not be the same if you are running localized versions of Lync Server 2013. A device named Aastra 6725ip Microphone (Aastra 6725ip)-V0 in US English could have a different name in French or Spanish.

Often times you'll want that level of detail; at other times, however, you might only be interested in how many calls use any Aastra microphone, regardless of model number. One way to get information like that is to export the Device Report data to Microsoft Excel and then save that data to a comma-separated values file (for example, C:\Data\Devices_Report.csv). You can then use a set of commands similar to these to import the .CSV file into Windows PowerShell and report back the total number of calls made using an Aastra capture device:

```
$devices = Import-Csv "C:\Data\Device_Report.csv
$sum = $devices | Where-Object {$_."Capture device" -match "Aastra"}
$sum | foreach-object {[Int]$x = [Int]$x + [Int]$_."call volume"}
$x
```

That will return a single value representing the total number of calls made using an Aastra capture device. For example:

```
384
```

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Device Report enables you to filter on such things as call type (that is, was the call a client call), a conference call, or a public switched telephone network (PSTN) call. You can also choose how data should be grouped. In this case, devices are grouped by hour, day, week, or month.

The following table lists the filters that you can use with the Device Report.

Device Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month):

	7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Voice switch cause	Reason why a call had to be placed into half duplex mode in order to prevent echo. In half duplex mode, communication can travel in only one direction at a time, similar to the way users take turns when communicating with a walkie-talkie. Select one of the following: • [All] • None • Bad timestamp • Echo • DNLP (dynamic nonlinear processor) • Low complexity • Bad device state • Post-AEC echo (acoustic echo cancellation)
Echo cause	Reason why echo above the accepted level was detected in a call. (In telecommunications, echo is a reflection of sound, the same phenomenon you will hear if you yell down to the bottom of a well.) Select one of the following: • [All] • None • Bad timestamp • Post-AEC echo (acoustic echo cancellation) • ANLP (adaptive nonlinear processor) • DNLP (dynamic nonlinear processor) • Microphone clipping
Call type	Indicates the type of call that was made. Select one of the following: • [All] • Client call

	- PSTN call - Conference call
Access type	Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following: - [All] - Internal - External
Network type	Indicates the type of network the client was connected to when the call was placed. Select one of the following: - [All] - Wired - Wireless
VPN	Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: - [All] - VPN - Non-VPN
Device type	Indicates the type of device. Select one of the following: - Capture device - Render device - Capture/Render device pair
Device name	Name of the capture or render device. You can enter the complete device name or any portion of the device name. For example, to find the device Microphone (Microsoft LifeCam VX-1000.), you can enter the complete device name as follows: Microphone (Microsoft LifeCam VX-1000.) Or, you can enter just a portion of the name. For example: LifeCam Note that the preceding filter returns any device that contains the string "LifeCam" anywhere in its name.

Metrics

The following table lists the information provided in the Device Report.

Device Report Metrics

Name	Can you sort on this item?	Description
Capture device	Yes	Device (for example, a microphone or webcam) used for transmitting audio.
Render device	Yes	Device (for example, a headset or speakers) used for receiving audio.

Call volume	Yes	Total number of calls placed.
Poor call percentage	Yes	Percentage of calls that were classified as "poor." A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Unique users	Yes	Unique users who used the device. If a user used the device 13 times he or she would count as one unique user, the same as a user who only used the device a single time.
Ratio of voice switch time	Yes	Percentage of the call that had to be conducted in half duplex mode in order to prevent echo. In half duplex mode, communication can travel in only one direction at a time, similar to the way users take turns when communicating with a walkie-talkie.
Ratio of microphone not functioning	Yes	Percentage of the call in which the capture device was not functioning at an acceptable level. A high values suggests that quality issues with the call were primarily due to the capture device not working as expected.
Ratio of speaker not functioning	Yes	Percentage of the call in which the render device was not functioning at an acceptable level. A high values suggests that quality issues with the call were primarily due to the render device not working as expected.
Calls with voice switch (%)	Yes	Percentage of the total calls which had to be placed into half duplex mode. In half duplex mode, communication can travel in only one direction at a time, similar to the way users take turns when communicating with a walkie-talkie.
Echo microphone in (%)	Yes	Percentage of echo that was

		present in the microphone. (In telecommunications, echo is a reflection of sound, the same phenomenon you will hear if you yell down to the bottom of a well.) Typically you will see low values for headsets or handsets, and higher values for speaker phones or stand-alone speakers.
Echo send (%)	Yes	Percentage of echo transmitted to other users.
Calls with echo (%)	Yes	Percentage of the total calls that had echo exceeding the acceptable level.

1.7.20.4.5.6 Call List Report

Call List Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic Reports >

Topic Last Modified: *2012-10-01*

The Call List Report provides Quality of Experience (QoE) metrics for individual calls made and received in your organization. Note that the actual metrics reported will depend on how you access the Call List report. For example, if you open the report from the Device Report, you'll see metrics such as the following, metrics that are also reported on the Device Report:

- Caller's microphone
- Caller's speaker
- Callee's microphone
- Callee's speaker
- Ratio of voice switch time

However, if you open the Call List Report from the Location Report, you won't see any of those metrics; instead, you'll see metrics like these:

- Round trip (ms)
- Degradation (MOS)
- Packet loss
- Jitter (ms)

Those are the metrics reported on the Location Report. However, from the Call List Report you can always click the Detail metric to provide complete QoE information for any call.

Accessing the Call List Report

The Call List Report can be accessed from any of the following reports:

- The Location Report (by clicking the Call volume or Poor call percentage metric)
- The Device Report (by clicking the Call volume or Poor call percentage metric)
- The Media Quality Summary Report (by clicking the Call volume or Poor call percentage metric)
- The Server Performance Report (by clicking the Call volume or Poor call percentage metric)

From within the Call List Report you can access the Call Detail Report by clicking the Detail metric.

Making the Best Use of the Call List Report

If you can't remember what some of the Call List Report metrics (such as Ratio voice switch time) actually measure, hold your mouse over the metric label; a tool tip will then appear giving you a brief description of the metric.

Filters

None. You cannot filter the Call List Report.

Metrics

The following table lists the information provided in the Call List Report for each call.

Call List Report Metrics

Name	Can you sort on this item?	Description
Details	No	When you click this item, the report shows additional information on the call.
Caller	Yes	SIP address of the person who initiated the call.
Callee	Yes	SIP address of the person who was called.
Start time	Yes	Date and time that the call started.
End time	Yes	Date and time that the call ended.
Caller user agent	Yes	Software used by the endpoint of the person who initiated the call.
Callee user agent	Yes	Software used by the endpoint of the person who was called.
Round trip (ms)	Yes	Average amount of (in milliseconds) required for a real-time transport protocol (RTP) packet to travel to another endpoint and then back. Round-trip times of 100 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing, a routing misconfiguration, or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.

Degradation (MOS)	Yes	Average amount of mean opinion score (MOS) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0. A value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users rate the quality of a call on a scale of 1-to-5. In Lync Server, Lync Server uses a set of algorithms to predict how users would have rated a call. High degradation values can be caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.
Packet loss	Yes	Average rate of RTP packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion, lack of bandwidth, wireless congestion or interference, or an overloaded media server. Packet loss typically results in distorted or lost audio.
Jitter	Yes	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
Healer concealed ratio	Yes	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.
Healer stretched ratio	Yes	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio

		sounding robotic or distorted.
Healer compressed ratio	Yes	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.
Connectivity	Yes	Type of wireless communication link. Typically, this is one of the following: • Relay • Direct

1.7.20.4.5.7 Call Detail Report

Call Detail Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic Reports >

Topic Last Modified: *2012-10-01*

The Call Detail Report provides a detailed look at an individual call; the report includes nearly all the Quality of Experience metrics and statistics collected by Lync Server, divided into report sections such as:

- Call Information
- Caller Device and Signal Metrics
- Callee Device and Signal metrics
- Caller Client Event
- Callee Client Event
- Audio Stream (Caller to Callee)
- Video Stream (Caller to Callee)
- Audio Stream (Callee to Caller)
- Video Stream (Callee to Caller)

Keep in mind that the categories and the metrics you see on a given report depend on two things: the type of session and the type of endpoints used in the session. For example, an audio-only call will not report metrics for video streams; that's because the call didn't have a video stream. Likewise, you might have a report that lists caller statistics but not callee statistics. That's typically because the callee was not using a SIP-compliant device. Endpoints are responsible for reporting statistics at the end of a call; however, a cell phone (which knows nothing about SIP or SIP statistics) is unable to report that kind of information. If you call someone and they answer you on their cell phone, you will not get a report from that cell phone when the call ends.

The Call Detail Report is most useful when you are trying to determine exactly why a given call experienced media quality problems.

Accessing the Call Detail Report

The Call Detail Report can be accessed from any of the following reports:

- The Location Report (by clicking either the Call volume or the Poor call percentage metric)
- The Media Quality Summary Report (by clicking either the Call volume or Poor call percentage metric)
- The Media Quality Comparison Report (by clicking the Call List Report and then clicking the Detail metric).
- The Server Performance Report (by clicking either the Call volume or Poor call percentage metric)
- The Call List Report (by clicking the Detail metric)

From within the Call Detail Report you can access the Device Report by clicking either of the following metrics:

- Capture device
- Render device

You can also access the Server Media Quality Trend Report by clicking the A/V edge server metric.

Making the Best Use of the Call Detail Report

The Call Detail Report typically includes over 250 different metrics, including such items as Microphone timestamp drift, Low SNR time, and Near end to echo time. If you can't remember what all of these metrics actually measure, try holding your mouse over the metric label; often-times, a tooltip will appear describing that metric.

If you have problems locating a metric, type part of the metric label in the search box and then click Find. For example, if you can't find the Low SNR time metric, type SNR in the search box and then click Find.

Filters

None. You cannot filter the Call Detail Report.

Metrics

The following table lists the information provided in the Call Detail Report for each call.

Call Detail Report Metrics

Name	Can you sort on this item?	Description
Caller PAI	No	P-Asserted-Identity of the user who initiated the call. The P-Asserted-Identity is used to convey the proven identity of a user within a trusted network.
Caller URI	No	SIP address of the user who initiated the call.
Caller endpoint	No	Device used to make the call.
Caller user agent	No	Software used on the device that made the call.

Call start	No	Date and time that the call was initially placed.
Mediation Server bypass call	No	Indicates whether the call connected to a PSTN voice gateway or qualified IP-PBX without passing through the Mediation Server.
Caller OS	No	Operating system of the caller's computer.
Callee CPU	No	CPU installed in the computer of the user who initiated the call.
Caller CPU core number	No	Processor number in the computer used by the person who initiated the call.
Caller CPU speed	No	Clock speed of the CPU of the computer used by the person who initiated the call.
Caller CPU virtualization	No	Virtualization (if any) used on the computer used by the person who initiated the call.
Callee PAI	No	P-Asserted-Identity of the user who was invited to join the call. The P-Asserted-Identity is used to convey the proven identity of a user within a trusted network.
Callee URI	No	SIP address of the user who was called.
Callee endpoint	No	Device used to receive the call.
Callee user agent	No	Software used on the device that received the call.
Duration	No	Length of time for the call.
Media bypass warning flag	No	Warning issued when the Mediation Server was bypassed.
Callee OS	No	Operating system of the computer for the user who was called.
Callee CPU	No	CPU installed in the computer of the user who was called.
Callee core number	No	Processor number in the computer used by the person who was called.
Callee CPU speed	No	Clock speed of the CPU of

		the computer used by the person who was called.
Callee CPU virtualization	No	Virtualization (if any) used on the computer used by the person who was called.

1.7.20.4.5.8 Server Media Quality Trend Report

Server Media Quality Trend Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic Reports >

Topic Last Modified: *2012-11-12*

The Server Media Quality Trend Report provides a way for you to graphically compare up to 5 servers on Quality of Experience metrics such as call volume, poor call percentage, packet loss, and jitter. This makes it easier to do such things as identify servers that are performing poorly, identify servers that are underutilized, or identify servers that are being overused.

Accessing the Server Media Quality Trend Report

The Server Media Quality Trend Report can be accessed from either one of the following report:

- Server Performance Report (by clicking the Trend metric)
- Call Detail Report (by clicking the A/V edge server metric. If the caller or callee is a server, you can also reach the Server Quality Media Trend Report by clicking the endpoint name.)

Making the Best Use of Server Media Quality Trend Report

When you click the Trend metric on the Server Performance Report for a specific server, the Server Media Quality Trend Report will open. However, you will see only a blank instance of that report; the server you selected on the Server Performance Report will not be displayed onscreen. Instead, you will need to select that server from the Servers dropdown. Note, too that the Servers dropdown includes a Select All option. This option will not work if you have more than 5 servers; the Server Media Quality Trend Report can only display data for a maximum of 5 servers at a time.

On the graphs displayed by the Server Media Quality Trend Report, the points labeled Call Volume and Poor Call Percentage are hotlinks; clicking a point on the graph will open an instance of the Call List Report showing the total calls (or poor calls) for the specified time period.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Server Media Quality Trend Report.

Server Media Quality Trend Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 8/7/2012 and an end date of 9/28/2012, data is

	displayed for the days 8/7/2012 12:00 AM to 9/7/2012 12:00 AM (that is, a total of 31 days' worth of data).
Server type	Type of server involved in the call. Allowed values are: • Mediation Server • A/V Conferencing Server • A/V Edge Server • Gateway (Mediation Server) • Gateway (Mediation Server Bypass) • AS Conferencing Server
Servers	Name of the server involved in the session; this dropdown list is automatically populated for you based on the value of the Server type filter. You can select up to 5 different servers when compiling a report.
Access type	Indicates whether the participant was logged on to the internal network or from the external network. Allowed values are: • [All] • Internal • External
Network type	Indicates the type of network the participant was connected to. Allowed values are: • [All] • Wired • Wireless
VPN	Indicates whether an external participant was using a virtual private network (VPN) connection during the session. Allowed values are: • [All] • VPN • Non-VPN

Metrics

The following table lists the information provided in the Server Media Quality Trend Report.

Server Media Quality Trend Report Metrics

Name	Can you sort on this item?	Description
Call volume	No	Total number of calls.
Degradation (MOS)	No	Average amount of MOS (mean option score) degradation experienced during a call. Degradation values can range from a low of 0.0 to a high of 5.0; a value of 0.5 or less represents acceptable degradation. Historically, mean options scores were calculated by having users

		rate the quality of a call on a scale of 1-to-5. Lync Server uses a set of algorithms to predict how users would have rated a call. High degradation values can be caused by congestion; lack of bandwidth; wireless congestion or interference, or an overloaded media server or endpoint. High degradation results in distorted or lost audio.
Poor call percentage	No	The total number of calls classified as poor. A poor call is any call which at least one of the measured metrics exceeded the allowed value (for example, a call that experienced excessive jitter).
Round trip (ms)	No	Average amount of time (in milliseconds) required for a Real-Time Transport Protocol packet to travel to one endpoint and then back. Round-trip times of 200 milliseconds or less are considered of acceptable quality. High round-trip values can be caused by international call routing; a routing misconfiguration; or an overloaded media server. High round-trip times result in difficulties with two-way, real-time audio conversations.
Packet loss	No	Average rate of Real-Time Transport Protocol (RTP) packet loss. (Packet loss occurs when RTP packets, a protocol used for transmitting audio and video across the Internet, failed to reach their destination.) High loss rates are generally caused by congestion; lack of bandwidth; wireless congestion or interference; or an overloaded media server. Packet loss typically results in distorted or lost audio.

Jitter (ms)	No	Average jitter detected between RTP packet arrivals. (Jitter is a measure of the "shakiness" of a call.) High jitter values are typically caused by congestion or an overloaded media server, and result in distorted or lost audio.
Healer concealed ratio	No	Average ratio of concealed audio samples to the total to the total number of samples. (A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets.) High values indicate significant levels of loss concealment applied caused by packet loss or jitter, and results in distorted or lost audio.
Healer stretched ratio	No	Average ratio of stretched audio samples to the total to the total number of samples. (Stretched audio is audio that has been expanded to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample stretching caused by jitter, and result in audio sounding robotic or distorted.
Healer compressed ratio	No	Average ratio of compressed audio samples to the total number of samples. (Compressed audio is audio that has been compressed to help maintain call quality when a dropped network packet has been detected.) High values indicate significant levels of sample compression caused by jitter, and result in audio sounding accelerated or distorted.

1.7.20.4.5.9 Media Quality Metrics Distribution Report

The Media Quality Metrics Distribution Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic

Reports >

Topic Last Modified: *2012-06-06*

The Media Quality Metrics Distribution Report enables you to see a graph that shows the distribution values for a Quality of Experience metric such as jitter or packet loss. For example, suppose your users make a total of 10 phone calls; those 10 calls report the following roundtrip times:

Call Number	Roundtrip Time (milliseconds)
1	50
2	50
3	50
4	50
5	50
6	50
7	50
8	4550
9	50
10	50

The average for those roundtrip times is 500 milliseconds (5000 divided by 10). Five hundred milliseconds is an extremely large roundtrip time; as a result, you might believe that you have a serious problem with network congestion. (Long roundtrip times are typically the result of overloaded networks.)

In reality, of course, 90% of your calls had excellent round trip times; you merely had one bad call that skewed the overall results. If you only look at the average roundtrip time you might jump to a very wrong conclusion.

The Media Quality Metrics Distribution Report helps you avoid jumping to wrong conclusions by showing you a graphical distribution of a specified metric (such as round trip time). These graphs can help make it clear that you had nine very good calls and one very bad call. Admittedly, you might still want to further investigate that one call; however, the fact that 9 out of the 10 calls were very good suggests that there is no reason to make any drastic changes to your network, at least not at this point in time.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. The following table lists the filters that you can use with the Media Quality Metrics Distribution Report.

Media Quality Metrics Distribution Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM

	If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Minimum in x axis	Lowest value to be displayed on the X axis of the graph.
Maximum in x axis	Highest value to be displayed on the X axis of the graph.
Access type	Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following: • [All] • Internal • External
VPN	Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: • [All] • VPN • Non-VPN
Network type	Indicates the type of network the client was connected to when the call was placed. Select one of the following: • [All] • Wired

	- Wireless

1.7.20.4.5.10 Location Trend Report

Location Trend Report

Monitoring and Health Configuration > Using Monitoring Reports > Media Quality Diagnostic Reports >

Topic Last Modified: *2012-06-06*

The Location Trend Report provides call quality trend information for network locations.

Filters

Filters provide a way for you to return a more finely-targeted set of data or to view the returned data in different ways. For example, the Location Trend Report enables you to filter the returned data by such things as access type (that is, interval access vs. external access) or by wired/wireless network connection. You can also choose how data should be grouped. In this case, calls are grouped by hour, day, or week.

The following table lists the filters that you can use with the Location Trend Report.

Location Trend Report Filters

Name	Description
From	Start date/time for the time range. To view data by hours, enter both the start date and time as follows: 7/7/2012 1:00 PM If you do not enter a start time, the report automatically begins at 12:00 AM on the specified day. To view data by day, enter just the date: 7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
To	End date/time for the time range. To view data by hours, enter both the end date and time as follows: 7/7/2012 1:00 PM If you do not enter an end time, the report automatically ends at 12:00 AM on the specified day. To view data by day, enter just the date:

	7/7/2012 To view by week or by month, enter a date that falls anywhere within the week or month that you want to view (you do not have to enter the first day of the week or month): 7/3/2012 Weeks always run from Sunday through Saturday.
Interval	Time interval. Select one of the following: • Hourly (a maximum of 25 hours can be displayed) • Daily (a maximum of 31 days can be displayed) • Weekly (a maximum of 12 weeks can be displayed) If the start and end dates exceed the maximum number of values allowed for the selected interval, only the maximum number of values (starting from the start date) is displayed. For example, if you select the Daily interval with a start date of 1/1/2011 and an end date of 2/28/2011, data is displayed for the days 8/1/2011 12:00 AM to 9/1/2011 12:00 AM (that is, a total of 31 days' worth of data).
Access type	Indicates whether the client was logged on to the internal network or the external network when the call was placed. Select one of the following: • [All] • Internal • External
Network type	Indicates the type of network the client was connected to when the call was placed. Select one of the following: • [All] • Wired • Wireless
VPN	Indicates whether an external client was using a virtual private network (VPN) connection when the call was placed. Select one of the following: • [All] • VPN • Non-VPN

1.7.21 Lync Server 2013 Best Practices Analyzer

Lync Server 2013 Best Practices Analyzer

Microsoft Lync Server 2013 > Operations >

Topic Last Modified: *2012-06-13*

Lync Server 2013, Best Practices Analyzer is a diagnostic tool that gathers configuration information from Lync Server 2013 environments and determines whether the configuration is set according to Microsoft best practices.

> **Note:**
>
> Lync Server 2013, Best Practices Analyzer scans and reports issues only with Lync Server 2013 components. If your deployment includes Lync Server 2010 or Office Communications Server 2007 R2 components, use the previous version of Best Practices Analyzer to analyze those components. For details, see Requirements for Running Best Practices Analyzer.

- Overview of Best Practices Analyzer
- Preparing for and Installing Best Practices Analyzer
- Using Best Practices Analyzer to Identify Potential Issues in Your Deployment
- Using Scan Results to Analyze and Resolve Issues Reported by Best Practices Analyzer

1.7.21.1 Overview of Best Practices Analyzer

Overview of Best Practices Analyzer

Microsoft Lync Server 2013 > Operations > Lync Server 2013 Best Practices Analyzer >

Topic Last Modified: *2012-09-19*

You can use Lync Server 2013, Best Practices Analyzer to identify and resolve problems with your Lync Server 2013 deployment. The Lync Server 2013, Best Practices Analyzer gathers configuration information from Lync Server 2013 components.

With the proper network access, the Best Practices Analyzer can examine servers running Active Directory Domain Services, Exchange Server Unified Messaging (UM), and Lync Server 2013. You can use Best Practices Analyzer to do the following:

- Proactively perform checks, verifying that the configuration is set according to recommended best practices.
- Automatically detect required updates to Lync Server 2013.
- Generate a list of issues, such as suboptimal configuration settings, unsupported options, missing updates, or practices that we do not recommend.
- Help you troubleshoot and fix specific problems.

Best Practices Analyzer provides the following features:

- Minimal installation prerequisites.
- Online documentation about reported issues, including troubleshooting tips.
- Configuration information that you can save for later review.
- State-of-the-art system analysis.

Best Practices Analyzer uses a set of XML configuration files to determine the information to gather from your Lync Server 2013 environment. In addition to checking Active Directory Domain Services, it checks sources such as the Windows Server operating system registry and settings in Windows Management Instrumentation (WMI).

Best Practices Analyzer compares the data it gathers with a set of predefined rules for the settings and configurations of Lync Server 2013 deployments.

After comparing the collected data with the predefined rules, the tool reports issues. For every issue that it reports, Best Practices Analyzer provides information about what was found in the scanned Lync Server 2013 environment and the recommended configuration. Best Practices Analyzer also provides links to more detailed information about the specific issues.

Note:
The Lync Server 2013, Best Practices Analyzer gathers configuration information only from Lync Server 2013 components. You can use the previous versions of the tool to scan previous environments. For details, see Requirements for Running Best Practices Analyzer.

1.7.21.2 Preparing for and Installing Best Practices Analyzer

Preparing for and Installing Best Practices Analyzer

Microsoft Lync Server 2013 > Operations > Lync Server 2013 Best Practices Analyzer >

Topic Last Modified: *2012-10-21*

You must be logged on as a member of the Administrators group to perform the tasks that are described in this topic.

System Requirements for Best Practices Analyzer Installation

To run Lync Server 2013, Best Practices Analyzer to scan your environment, the computer must be running a 64-bit edition of one of the following operating systems:

- Windows Server 2008 R2 with Service Pack 1 (SP1) Standard operating system
- Windows Server 2008 R2 with SP1 Enterprise operating system
- Windows Server 2008 R2 with SP1 Datacenter operating system
- Windows Server 2012 Standard operating system
- Windows Server 2012 Enterprise operating system
- Windows Server 2012 Datacenter operating system
- Windows 8 operating system
- Windows 7 operating system

The computer must also be running the following:

- Microsoft .NET Framework 4.5. For Lync Server 2013, you must manually install the 64-bit edition of Microsoft .NET Framework 4.5 on the server prior to installing Lync Server 2013.
- Lync Server 2013, Core Components.
- WMI Backward Compatibility Package. For details, see Install WMI Backward Compatibility Package in the Migration documentation.
- Windows PowerShell 3.0. For details, see Installing Windows PowerShell 3.0 in the Deployment documentation.

You can install Best Practices Analyzer on computers with a supported operating system that are not running Lync Server 2013, Core Components or WMI Backward Compatibility Package, but you can use Best Practices Analyzer on those computers only to view reports, not to run scans.

Choosing a Computer for Installation

We recommend that you install Lync Server 2013, Best Practices Analyzer on a computer that is dedicated to Lync Server 2013 management. You can install the tool on a server running Lync Server 2013 or an administrative computer running Lync Server 2013 administrative tools. If you install the tool on a server that is running Lync Server, we recommend that you use the tool to scan only that server.

Installing Best Practices Analyzer

You can download the Best Practices Analyzer for Lync Server 2013 at http://go.microsoft.com/fwlink/p/?linkId=266539.

To install Best Practices Analyzer, start the Microsoft Installer file RtcBPA.msi on the computer where you want to install the tool, and then follow the instructions on the screen. The default location for installing the program files is <*system drive*>\Program Files\Lync Server 2013\BPA.

1.7.21.3 Using Best Practices Analyzer to Identify Potential Issues in Your Deployment

Using Best Practices Analyzer to Identify Potential Issues in Your Deployment

Microsoft Lync Server 2013 > Operations > Lync Server 2013 Best Practices Analyzer >

Topic Last Modified: *2012-09-21*

To use Best Practices Analyzer to scan your Lync Server 2013 environment, your system must meet specific prerequisites before you start the scan. After you ensure that your system meets the prerequisites, you can complete the scan process by using Best Practices Analyzer.

- Prerequisites for Running Best Practices Analyzer
- Checking for Updates to Best Practices Analyzer
- Using Best Practices Analyzer to Scan Your Deployment for Potential Issues

1.7.21.3.1 Prerequisites for Running Best Practices Analyzer

Prerequisites for Running Best Practices Analyzer

Operations > Lync Server 2013 Best Practices Analyzer > Using Best Practices Analyzer to Identify Potential Issues in Your Deployment >

Topic Last Modified: *2012-06-25*

You can use Best Practices Analyzer to scan your Lync Server 2013 environment for issues and create reports, and to view results of a current or previous scan. Prior to running Best Practices Analyzer to scan your environment, you need to verify that the account that you plan to use to run the scan has the required rights and permissions and that all installation prerequisites have been met.

- Group Memberships and User Rights Requirements for Best Practices Analyzer
- Requirements for Running Best Practices Analyzer

1.7.21.3.1.1 Group Memberships and User Rights Requirements for Best Practices Analyzer

Group Memberships and User Rights Requirements for Best Practices Analyzer

Lync Server 2013 Best Practices Analyzer > Using Best Practices Analyzer to Identify Potential Issues in Your Deployment > Prerequisites for Running Best Practices Analyzer >

Topic Last Modified: *2012-10-21*

To successfully run Best Practices Analyzer, the user account that you use to log on must be a member of the Administrators group on the local computer. Additionally, to scan your environment, the user account must be a member of the following groups:

- **Domain Admins** To enumerate Active Directory Domain Services information and to call the Windows Management Instrumentation (WMI) providers on domain controllers and global catalog servers.
- **Administrators** Required on each Lync Server 2013 internal computer and each Edge Server to call the Windows Management Instrumentation (WMI) providers and to access the registry.
- **RTCUniversalReadOnlyAdmins** Full or delegated read only Lync Server 2013 administrative rights.
- **Exchange View Only Administrator** Full or delegated Exchange View Only Administrator on the Microsoft Exchange organization.

If your user account does not have sufficient user rights, you have two options:

- At a command prompt, use the **runas** command to run the tool under an account that does have sufficient user rights. The syntax is as follows:

  ```
  runas /netonly /user:<domain>\<userName> rtcbpa.exe
  ```

- On the **Connect to Active Directory** page, set the credentials for the accounts that you plan to use to run Best Practices Analyzer. Click **Show advanced login options**. You can enter three accounts: one for connecting to Active Directory Domain Services, one for connecting to Lync Server 2013 Edge Servers, and one for connecting to the Exchange Servers. If you do not specify any of these accounts, the user account that you used to log on and run Best Practices Analyzer is used.

1.7.21.3.1.2 Requirements for Running Best Practices Analyzer

Requirements for Running Best Practices Analyzer

Lync Server 2013 Best Practices Analyzer > Using Best Practices Analyzer to Identify Potential Issues in Your Deployment > Prerequisites for Running Best Practices Analyzer >

Topic Last Modified: *2012-09-19*

You can use Lync Server 2013, Best Practices Analyzer to scan your Lync Server 2013 environment. You cannot use it to scan previous environments, but you can use the previous versions of the tool to scan those environments. For details about downloading and using the Lync Server 2010 and Office Communications Server 2007 R2 versions of Best Practices Analyzer, see "Lync Server 2010, Best Practices Analyzer" at http://go.microsoft.com/fwlink/p/?linkId=210536 and "Best Practices Analyzer for Office Communications Server 2007 and Office Communications Server 2007 R2" at http://go.microsoft.com/fwlink/p/?linkId=256358.

Prior to starting your scan, you should ensure that all components in your Lync Server 2013 environment are running and online.

Note:

Depending on the configuration of your Edge Servers and any related perimeter network settings, including firewall settings and permissions, Best Practices Analyzer might not be able to access and scan your Edge Servers. If you include Edge Servers in your scan and the reports indicate that there is an issue with accessing Edge Servers, you might want to remove Edge Servers from the scan options and run the scan again so that the issues do not show up in the report.

1.7.21.3.2 Checking for Updates to Best Practices Analyzer

Checking for Updates to Best Practices Analyzer

Operations > Lync Server 2013 Best Practices Analyzer > Using Best Practices Analyzer to Identify Potential Issues in Your Deployment >

Topic Last Modified: *2012-10-02*

When you start Best Practices Analyzer, the tool provides you with an option to search for the latest updates to the tool. If an update is available, you can download the update. If you choose not to download updates, or if Best Practices Analyzer cannot access the Internet, you can continue to use the version that is already on the computer.

Note:

If you need proxy authentication to access the Internet, Best Practices Analyzer cannot access new updates for you to download. However, you can manually download the latest version of RtcBPA.msi from the Microsoft Download Center at http://go.microsoft.com/fwlink/p/?linkId=266539. After downloading the file, you can copy it to the computer on which you want to update Best Practices Analyzer and use the .msi file to install the new version of the tool on that computer.

To update Best Practices Analyzer rules, you must run the tool as an Administrator on the local computer. If you are not logged on using an account that is a member of the Administrators group and updates are detected, close Best Practices Analyzer, and then use the following procedure to start the program.

To open Best Practices Analyzer as Administrator to check for updates

1. On a computer on which Best Practices Analyzer is installed, click **Start**, point to **Microsoft Lync Server 2013**, right-click **Best Practices Analyzer**, and then click **Run as administrator**.
2. Specify credentials of an account that is a member of the Administrators group.

1.7.21.3.3 Using Best Practices Analyzer to Scan Your Deployment for Potential Issues

Using Best Practices Analyzer to Scan Your Deployment for Potential Issues

Operations > Lync Server 2013 Best Practices Analyzer > Using Best Practices Analyzer to Identify Potential Issues in Your Deployment >

Topic Last Modified: *2012-10-21*

To run a Best Practices Analyzer scan, you must specify the following:

- **Credentials** To run a scan, you must log on to a computer on which Best Practices Analyzer is installed by using an account that is a member of the local Administrators group. Additionally, you need to log on by using a user account that has the user rights and permissions required to run the appropriate scans, or you must specify credentials that have the appropriate user rights and permissions when you run Best Practices Analyzer. For details, see Group Memberships and User Rights Requirements for Best Practices Analyzer.
- **Scope of scan** To specify the scope of the scan, select the categories and

servers that you want to scan. You can select all categories, one or more categories, or one or more servers within a specific category in your Lync Server environment.

- **Type of scan** Currently, the Health Check scan is the only type of scan available (selected by default). The Health Check scan generates a report that includes errors, warnings, and other information for all servers specified in the scope.
- **Network speed** Network speed options include Fast LAN (100 Mbps or more), LAN (10 Mbps), Fast WAN (1.5 Mbps), or WAN (64 kbps). The estimated time to complete the scan is based on this setting. This setting is also used to set the time-out period. During the scan, the Best Practices Analyzer waits for a response from a server for a specified time. If it does not receive a response within the specified time-out period, it moves to the next server in the scan. On slower networks, this specified time-out period is longer to account for longer network latencies. We recommend that you select the slowest link in your topology for this parameter so that the tool does not time out too quickly.

⊟To scan your Lync Server 2013 deployment

1. Log on to a computer on which Best Practices Analyzer is installed by using an account that is a member of the local Administrators group, and has other required user rights and permissions.
2. Click **Start**, point to **All Programs**, click **Microsoft Lync Server 2013**, and then click **Best Practices Analyzer**.
3. On the **Welcome** screen, click **Select options for a new scan**.
4. On the **Connect to Active Directory** page, verify the name specified in **Active Directory Server**, and then do one of the following:
   - To run a scan using the credentials that you used to log on to the computer, click **Connect to the Active Directory server**.
   - To specify different credentials that you want to use for Active Directory Domain Services, Edge Server, or Exchange Server, click **Show advanced logon options**, select each check box for which separate credentials are required, specify the credentials for each selected check box, and then click **Connect to the Active Directory server**.

   Note:
   Before beginning the scan, Best Practices Analyzer performs a network and permissions check to ensure that the specified account credentials are valid and that Best Practices Analyzer can connect to Active Directory Domain Services. If the tool is running on a workgroup server, the tool also verifies that it can connect to Edge Servers in the perimeter network (that is, if they are included in the scan).
5. On the **Start a new Best Practices scan** page, select the options that you want to include in the scan, specify the network speed, and then click **Start scanning**.
6. On the **Scanning Completed** page, click **View a report of this Best Practices scan**.
7. On the **View Best Practices Report** page, do one of the following:
   - To view reports in a list organized by server component, click **List Reports**, and then click either the **All Issues** tab or the **Informational Items** tab.
   - To view reports as a hierarchical list organized by types of results, click **Tree Reports**, and then click either the **Detailed View** tab or the **Summary View** tab.
   - To view other reports, click **Other Reports**.

   Note:
   For details about the Best Practices Analyzer reports and the issues they identify, see Viewing and Working with Reports Created by Best Practices Analyzer and Analyzing and Resolving Issues Identified by Best Practices Analyzer.

1.7.21.4 Using Scan Results to Analyze and Resolve Issues Reported by Best Practices Analyzer

Using Scan Results to Analyze and Resolve Issues Reported by Best Practices Analyzer

Microsoft Lync Server 2013 > Operations > Lync Server 2013 Best Practices Analyzer >

Topic Last Modified: *2012-06-14*

When you run Lync Server 2013, Best Practices Analyzer in your Lync Server 2013 environment, the tool uses the scan results to generate reports of issues with your deployment. You can use the reports generated by Best Practices Analyzer to identify and resolve specific issues.

> **Note:**
> Lync Server 2013, Best Practices Analyzer scans and reports issues only with Lync Server 2013 components. If your deployment includes Microsoft Lync Server 2010 or Office Communications Server 2007 R2 components, use the previous version of Best Practices Analyzer to analyze those components. For details, see Requirements for Running Best Practices Analyzer.

- Viewing and Working with Reports Created by Best Practices Analyzer
- Analyzing and Resolving Issues Identified by Best Practices Analyzer

1.7.21.4.1 Viewing and Working with Reports Created by Best Practices Analyzer

Viewing and Working with Reports Created by Best Practices Analyzer

Operations > Lync Server 2013 Best Practices Analyzer > Using Scan Results to Analyze and Resolve Issues Reported by Best Practices Analyzer >

Topic Last Modified: *2012-06-14*

When you use Best Practices Analyzer to scan your environment, Best Practices Analyzer creates reports that identify issues and other information about your deployment. You can use Best Practices Analyzer to view the reports that contain the scan results and understand the issues identified in the reports.

- Viewing Reports from Best Practices Analyzer
- Understanding Reports Created by Best Practices Analyzer

1.7.21.4.1.1 Viewing Reports from Best Practices Analyzer

Viewing Reports from Best Practices Analyzer

Lync Server 2013 Best Practices Analyzer > Using Scan Results to Analyze and Resolve Issues Reported by Best Practices Analyzer > Viewing and Working with Reports Created by Best Practices Analyzer >

Topic Last Modified: *2012-09-21*

When you use Best Practices Analyzer to scan your environment, you specify a name for the scan. After Best Practices Analyzer completes a scan, it stores the scan results in reports and saves them under the name of the scan. Upon completion of the scan, you can view the reports generated for that scan by clicking **View a report of this Best Practices scan** directly from the **Scanning Completed** page. You can also view the reports from that scan or previous scans at a later time. You can view reports on the local computer on which the scan was run, import scan results from another computer, or export scan results to view the reports on another computer on which Best Practices Analyzer is installed.

Scan results are presented in the following types of reports:

- List reports
- Tree reports
- Other reports

These reports include errors, warnings, and other information. For details about each of these types of reports and issues, see Understanding Reports Created by Best Practices Analyzer.

Use the following procedure to view scan results previously generated by Best Practices Analyzer.

⊟To view reports from a previous scan

1. Log on to a computer on which Best Practices Analyzer is installed using an account that is a member of the local User account.

   Note:
   You can view the results of a scan using an account that is a member of the local Administrators group, but you cannot run a scan unless you have appropriate user rights and permissions. For details, see Group Memberships and User Rights Requirements for Best Practices Analyzer.

2. Click **Start**, point to **All Programs**, click **Microsoft Lync Server 2013**, and then click **Best Practices Analyzer**.
3. On the **Welcome** screen, click **Select the scan results to view**.
4. On the **Select a Best Practices Scan to View** page, do one of the following:
   - To view reports from the list of locally stored scan results, click the name of scan, and then click **View a report of this scan**.

     Note:
     The Best Practices Analyzer creates the list of local files from the folder <*systemDrive*>\Documents and Settings\<*user*>\Application Data\Microsoft\RtcBPA.

   - To view reports for results of a scan that are stored at another location, click **Import scan**, locate the file containing the scan results, and then click **Open**.

     Note:
     If the version of Best Practices Analyzer on this computer does not match the version that was used to collect the data in the imported file, the tool on your computer might analyze the file again, after it is imported.

5. On the **View Best Practices Report** page, do one of the following:
   - To view reports in a list organized by server component, click **List Reports**, and then click either the **All Issues** tab or the **Informational Items** tab.
   - To view reports as a hierarchical list organized by types of results, click **Tree Reports**, and then click either the **Detailed View** tab or the **Summary View** tab.
   - To view other reports, click **Other Reports**.

   Note:
   For details about the Best Practices Analyzer reports and the issues that they identify, see Viewing and Working with Reports Created by Best Practices Analyzer and Analyzing and Resolving Issues Identified by Best Practices Analyzer.

Understanding Reports Created by Best Practices Analyzer

Lync Server 2013 Best Practices Analyzer > Using Scan Results to Analyze and Resolve Issues Reported by Best Practices Analyzer > Viewing and Working with Reports Created by Best Practices Analyzer >

Topic Last Modified: *2012-10-10*

Best Practices Analyzer provides multiple types of reports that are organized to facilitate the analysis and resolution of issues. Best Practices Analyzer identifies issues such as errors, warnings, and other information.

Reports

You can access the results of a scan by viewing each of the following reports:

- **List reports** List reports are organized by specific criteria. You can arrange the results by class, severity, or issue. For example, if you organize results by class, issues related to Directors are included under the Directors section of the report. You can view all of the issues, or just the informational items. You can search a list report for specific items, such as memory. You can also print the report or export it.
- **Tree reports** Tree reports are organized by the rules that are used to run the scan and other options that you specified at the time the scan was run. For example, issues related to the Test Topology rules are included under the Test Topology section of the report. You can view the details of all the issues, or just a summary of the issues. You can search a tree report for specific items, such as memory. You can also print the report or export it.
- **Other reports** Items in other reports include the run-time log of tasks that were included in the scan. You can search the items in other reports for specific items, such as memory. You can also print the report or export it.

Issues

The reports generated by Best Practices Analyzer indicate specific issues that are identified during the scan of your environment, including following types of issues:

- **Errors** Critical issues that require you to make a change in your environment. For example, if Lync Server 2013 Core Components are not installed, an error is logged.
  Issues that are classified as errors are identified in the report by a red X symbol. Errors are displayed on the **All Issues** tab of the **List Reports** view, and on the **Detailed View** tab and the **Summary View** tab of the **Tree Reports** view. If you do not want to see a specific error in a report, you can specify that the error not be shown for a single instance or for all instances of that error in the report. The error is then displayed only on the **Hidden Items** tab of the **Other Reports** view, unless you change the setting and specify that the error be displayed in the report.
- **Warnings** Issues that are not consistent with the implementation of a best practice. This may or may not indicate the need for a change in your environment. The issue could be a known issue with a specific setting that you do not need to change. For example, services that are not started on a server are logged as warnings.
  Issues that are classified as warnings are identified in the report by a triangular yellow warning symbol. Warnings are displayed on the **All Issues** tab of the **List Reports** view, as well as on the **Detailed View** tab and the **Summary View** tab of the **Tree Reports** view. If you do not want to see a specific error in a report, you can specify that the error not be shown for a

single instance or for all instances of that error in the report. The warning is then displayed only on the **Hidden Items** tab of the **Other Reports** view, unless you change the setting and specify that the warning be displayed in the report.

- **Information** Includes all issues that are not classified as errors or warnings. For example, the number of Lync Server 2013 Standard Edition server objects in Active Directory Domain Services (AD DS) is classified as an information issue.
  Information issues are displayed on the **All Issues** tab of the **List Reports** view, and on the **Detailed View** tab of the **Tree Reports** view.

The Lync Server 2013, Best Practices Analyzer does not make changes to your environment to resolve issues. The scan only detects potential issues and provides reports that contain information about how to resolve each issue.

If you click an issue, an explanation and some options are displayed for specific issues. Then, you can do any of the following:

- Find more detailed information about the issue, and how to resolve it.
- Stop showing issues in reports:
  - Stop showing issues for the selected instance.
  - Stop showing issues for all instances of that issue.

  To see the issues you have stopped showing in reports, go to the **Hidden Items** tab of the **Other Reports** view. From there, you can specify to start showing issues in reports again.

For details about resolving specific issues, see Analyzing and Resolving Issues Identified by Best Practices Analyzer.

1.7.21.4.2 Analyzing and Resolving Issues Identified by Best Practices Analyzer

Analyzing and Resolving Issues Identified by Best Practices Analyzer

Operations > Lync Server 2013 Best Practices Analyzer > Using Scan Results to Analyze and Resolve Issues Reported by Best Practices Analyzer >

Topic Last Modified: *2012-06-25*

Best Practices Analyzer does not make changes to your environment to resolve issues. It only detects potential issues and displays information about how to resolve them. If you identify issues that you need to resolve, you must determine the appropriate solution. The topics in this section help you identify and resolve some of the most significant potential issues.

- Issues with the Environment Test
- Issues with the Topology Test

1.7.21.4.2.1 Issues with the Environment Test

Issues with the Environment Test

Lync Server 2013 Best Practices Analyzer > Using Scan Results to Analyze and Resolve Issues Reported by Best Practices Analyzer > Analyzing and Resolving Issues Identified by Best Practices Analyzer >

Topic Last Modified: *2012-09-21*

Best Practices Analyzer provides a way for you to verify that your Lync Server 2013 environment is a supported configuration. As part of the Active Directory Domain Services check, Best Practices Analyzer does the following:

- Verifies the Active Directory Domain Services forest and schema preparation.
- Identifies the number of Active Directory Domain Services sites and domains in the deployment.
- Checks the forest and domain levels.
- Checks the domain controller version.
- Identifies the domain, configuration, and schema naming context.
- Identifies the number of enabled users.
- Checks where the global Active Directory Domain Services settings are stored.
- Checks for the service connection points (SCPs) for Lync Server.
- Identifies the database version.

Resolving Issues with the Environment

If the environment test found problems with your environment, these problems are probably caused by issues with your Active Directory configuration or the level of software running on specific servers. For example, if Best Practices Analyzer identifies any domain controllers in your environment that are running Windows Server 2000, it will issue a warning and you will need to upgrade those domain controllers to a supported version of Windows Server.

1.7.21.4.2.2 Issues with the Topology Test

Issues with the Topology Test

Lync Server 2013 Best Practices Analyzer > Using Scan Results to Analyze and Resolve Issues Reported by Best Practices Analyzer > Analyzing and Resolving Issues Identified by Best Practices Analyzer >

Topic Last Modified: *2012-09-21*

Like the **Test-CsTopology** cmdlet, Best Practice Analyzer provides a way for you to verify that Lync Server 2013 is functioning correctly at a global level. By default, Best Practice Analyzer, like the cmdlet, checks your entire Lync Server 2013 infrastructure, verifying that the required services are running, and that the appropriate user rights and permissions have been set for these services and for the universal security groups created when you install Lync Server 2013.

In addition to verifying the validity of Lync Server as a whole, **Test-CsTopology** also checks the validity of a specific service. For details about using the cmdlet to test specific services, see Test-CsTopology in the Lync Server Management Shell documentation. Use the following information to help resolve issues with your topology.

Note:
Depending on the configuration of your Edge Servers and any related perimeter network settings, including firewall settings and permissions, Best Practices Analyzer might not be able to access and scan your Edge Servers. If you include Edge Servers in your scan and the reports indicate that there is an issue accessing Edge Servers, clear the **Edge Servers** check box and run the scan again to prevent the issue from showing up in reports.

Resolving Issues with Your Topology

If the topology test found issues with your topology, these issues are probably caused by issues that occurred when you published or enabled your topology.

When you make changes to your topology, the changes take effect only when they have been both published and enabled. You must use Topology Builder to make topology changes. After you make changes, you can then publish and enable those changes by using Topology Builder.

When you publish the changes, the new information (for example, a new site or a new server role) is written to the Central Management store. However, these new (or the newly modified) objects do not immediately join your topology. Objects join your topology only when you enable the updated topology. If you select the Publish option in Topology Builder both of these steps occur: the changes are published (that is, they are written to the Central Management store) and then the new topology is enabled.

By default, members of the RTCUniversalServerAdmins group are authorized to run the **Publish-CsTopology** cmdlet and the **Enable-CsTopology** cmdlet. However, if setup permissions have not been delegated, you must be logged on as a domain administrator to run **Publish-CsTopology**. To give RTCUniversalServerAdmins the right to actually use the **Publish-CsTopology** cmdlet, you must run the **Grant-CsSetupPermission** cmdlet on every Active Directory container that contains computers running Lync Server services. To give RTCUniversalServerAdmins the right to use the **Enable-CsTopology** cmdlet, you must run the **Set-CsSetupPermission** cmdlet against every Active Directory Domain Services container that contains computers running Lync Server services. Note that this applies to enabling and publishing a topology by using Topology Builder. If you have not delegated permissions by using **Set-CsSetupPermission**, only a domain administrator can enable and publish a topology through Topology Builder.

1.8 Glossary

Glossary

Microsoft Lync Server 2013 >

Topic Last Modified: *2013-01-11*

This topic contains terms and definitions that pertain to Microsoft Lync Server 2013 and Microsoft Lync 2013.

Term	Definition
A/V Edge server	Enables internal users to share audio and video data with external users (that is, users who are not logged on to your internal network).
ACP	A third-party organization that provides audio conferencing services over public switched telephone network (PSTN).
active monitoring	Gives Lync system administrators the ability to monitor pools, servers, and networks across data centers through the public Internet.
audio conferencing provider	A third-party organization that provides audio conferencing services over public switched telephone network (PSTN).
Audio Test service	A built-in tool whereby a test call can be made before the actual call is. This ensures that there aren't any severe network or other issues that could affect call quality.

broadcast	Sent to more than one recipient. In communications and on networks, a broadcast message is one distributed to all stations.
bypass call	A call that bypasses the Mediation Server.
Call Park orbit	A number assigned to a parked call by the Call Park application.
Call via Work	A callback option whereby an outgoing call can be made by using the work number. The person who is receiving the call will see the work number of the caller, in their caller ID.
callee	The person whom, or place that, a caller is calling.
caller	The person who is calling another person or place.
camera	A digital video device that is used for recording moving images and audio in a digital format.
Central Management Server	The server role (one per organization) on one Front End pool in the deployment that manages and deploys basic configuration data to all servers that are running Lync Server. Also provides Lync Server Management Shell and file transfer capabilities.
client version filter	Restricts the client versions that are used in a Lync Server environment.
client version policy	A set of client version rules that defines the actions to be taken when users try to log on with specific clients and client versions.
conference call	A telephone conversation between three or more people.
conferencing service	An internally or externally hosted service for users to host multiparty conferences from their computers.
Contacts list	A list of people, groups, or organizations with whom you communicate.
Conversation History	The folder in Outlook where instant messages and phone conversations are stored.
data conferencing	A method of real-time communication wherein participants share and collaborate on several data and document types. The session can be hosted on an in-house server, an Internet-based service, or both.
dial-out conferencing	A feature whereby the A/V Conferencing Server calls the user, and the user answers the phone to join the conference.
dual-tone multiple-frequency	The signaling system used in telephones with touchtone keypads, in which each digit is associated with two specific frequencies.
Dynamic Memory	A Hyper-V feature in which the memory available to

	a running virtual machine is adjusted in response to changes in the amount of memory required by the virtual machine.
Edge pool	A single computer pool or a multiple computer pool that, by default, supports remote users in your organization who sign in to Lync Server from outside the firewall by using a virtual private network (VPN).
Enhanced 9-1-1	A service that provides information about the location of a caller who calls 9-1-1.
enhanced presenter controls	A collection of Lync Meeting host and presenter controls that optimizes for the type of meeting, size of audience, content, and/or video sources available to participants.
Front End pool	A set of Front End Servers, configured identically, that work together to provide services for a common group of users.
IM Conferencing service	A service that runs on a Lync Server or Office Communications Server front-end server to mix and manage inputs from multiple clients in a multiparty instant messaging (IM) session.
Join Launcher	Part of the existing Lync Web App IIS web component. Lets users optionally join meetings by using a mobile device.
Location Information Server	A network node originally defined in the National Emergency Number Association i2 network architecture that addresses the intermediate solution for providing Enhanced 9-1-1 (E9-1-1) service for VoIP telephony users.
Location Information service	A web service that manages a table of network elements and locations for use by clients of Enhanced 9-1-1 (E9-1-1).
long message	A message in a persistent chat room that exceeds the character limit. If the character limit is exceeded, the message will show as "long message."
Lync 2013 VDI plug-in	Provides the ability to have softphone-based audio, video, and meetings (peer-to-peer and multiparty) without the problems of latency, jitter, and packet loss.
Lync Meeting	Denotes the experience with Lync that can be scheduled, or ad-hoc. A Lync Meeting provides the ability to interact with people through video, audio, instant messaging, and content sharing.
Lync Meeting window	Denotes the Conversation window that handles escalations (peer-to-peer to conference) and scalable views that display people and content together inside a Lync Meeting.

Lync Server Management Shell	The management command line interface built on Windows PowerShell technology that includes a set of cmdlets to help control administration and automation.
Lync Web Scheduler	A web-based meeting scheduling and management tool for users who don't have access to Microsoft Outlook, or are on an operating system not based on Windows. With Lync Web Scheduler, you can create new meetings, change your existing meetings, and send invitations using your favorite email program.
Lync-to-phone	An optional feature of Lync Online that enables users to make calls to, and receive calls from, the traditional network by using Lync. This feature is available to Voice Plan customers only, and administrators must sign in with a Lync-to-phone provider to get the feature.
mic	A device that converts sound waves into analog electrical signals. Additional hardware can convert the microphone's output into digital data that a computer can process; for example, to record multimedia documents or analyze the sound signal.
Microsoft Lync Server Mobility Service	This service supports Lync functionality, such as instant messaging (IM), presence, and contacts on the following mobile devices: iPhone, iPad, Android, Windows Phone, and Nokia.
Microsoft Push Notification Service	A notification service that sends new events, such as an instant messaging invitation or a missed call, to the Windows Phone mobile device.
multiple points of presence	The ability of a single user to sign in to a Lync Server or Office Communications Server server with multiple clients.
network inter-site policy	Defines bandwidth limitations between sites that are directly linked within a call admission control (CAC) configuration.
network regions	The network hubs or backbones that are used in the configuration of call admission control, E9-1-1, and media bypass. They interconnect parts of a network across multiple geographic areas, and every network region must be associated with a central site.
network site	A collections of subnets with similar bandwidth, for example, a branch office location, a set of buildings, or a campus.
Office Web Apps Server	A server role used with Office Web Applications in Lync Server to handle the sharing and rendering of PowerPoint presentations.
OneNote share	The feature that lets users create and share OneNote meeting notes in a Lync Meeting. Notes appear as docked in a Lync Meeting, with

	participant lists that can be updated in meeting notes for participants to see.
outbound translation rule	A rule that converts phone numbers to the local dialing format for interaction with private branch exchange (PBX) systems.
persistent chat	A type of chat in which messages are posted to a chat room where they can be viewed and responded to in real time by multiple participants. Users can search for other rooms by name, member/owner, keywords, and content across groups from Lync.
personal preview	A video preview for a Lync user that provides options to answer with video from within the notification.
presence status	One of the attributes that makes up presence and that indicates a person’s availability and willingness to communicate.
present	Indicates the sharing activity of presenting a PowerPoint presentation. Only the PowerPoint document is shown and only the presenter can edit the content being presented.
PSTN usage records	Public switched telephone network (PSTN) usage records specify a class of call (such as internal, local, or long distance) that can be made by various users or groups of users in an organization.
public cloud	A cloud infrastructure typically owned and managed by an organization that sells cloud services. The resources are shared by the general public or a group of customers in order to optimize utilization rates.
public IM connectivity contact	A contact who uses an instant messenger client from AOL, Yahoo!, MSN, or the Windows Live network of Internet services. ◆**Important:** • As of September 1st, 2012, the Microsoft Lync Public IM Connectivity User Subscription License (“PIC USL”) is no longer available for purchase for new or renewing agreements. Customers with active licenses will be able to continue to federate with Yahoo! Messenger until the service shut down date (exact date TBD, but no sooner than June 2013). • The PIC USL is a per-user per-month subscription license that is required for Lync Server or Office Communications Server to federate with Yahoo! Messenger. Microsoft’s ability to provide this service has been contingent upon support from Yahoo!, the underlying agreement for which is

	winding down. • More than ever, Lync is a powerful tool for connecting across organizations and with individuals around the world. Federation with Windows Live Messenger requires no additional user/ device licenses beyond the Lync Standard CAL. Skype federation will be added to this list, enabling Lync users to reach hundreds of millions of people with IM and voice.
Quick Lync	A menu bar that appears beside the picture area of a contact in the Lync Contacts list that shows the available communication modes: IM, Call, Video, and View card.
ringback	A feature that transfers a call back to the person who parked it, after a specified amount of time, so a caller doesn't remain on hold indefinitely.
Scalable Video Coding	A video compression standard that encodes high-quality video bitstreams. Support for the capability enables the conferencing server to determine how bitstreams should flow among receiving clients, based on the capabilities and bandwidth of the receiving endpoint.
secret chat room	In the Lync persistent chat feature, a room that has been set up with the most restricted level of privacy. Only members of a secret chat room can find it, see who is participating in it, follow it, or read and post in it.
Survivable Branch Server	A server running Windows Server that meets specified hardware requirements, and that has Lync Server Registrar and Mediation Server software installed on it. Like Survivable Branch Appliances, this device can provide voice mail survivability for branch users during a WAN outage.
topic feeds	Feeds that provide information and notifications based on the persistent chat room that you are following.
Topology Builder	An installation component of Lync Server used to display, adjust, and validate a planned topology.
User Services	Configuration settings that are used to help maintain presence information and manage conferencing.
User Services pool	Provides presence information and helps to manage preferences.
User Services service	A Lync Server service that is used to help maintain presence information for users and to manage meetings and conferences.
video call	A call that connects Lync users with peer-to-peer capabilities. Users can start a video call by pointing

	to a contact in the Contacts view and then clicking the video call icon.
Video Capable	A status on a Lync contact card that indicates a camera is enabled.
video quality notifications	Alerts to Lync users about the quality of the network, computer, camera, and lighting conditions.
Video Spotlight	A mode that enables presenters to select one person’s video feed so that every participant in the meeting sees that participant only.
voice policies	Define the following for each user, site, or organization that is assigned the policy: A set of calling features that can be enabled or disabled to determine the Enterprise Voice functionality that is available to users. Also, a set of PSTN usage records that define what types of calls are authorized.
voice route	A route that contains instructions that tell Lync Server how to route calls from Enterprise Voice users to phone numbers on the public switched telephone network (PSTN), or a private branch exchange (PBX).
web conferencing	Functionality supplied by the Web Conferencing service such as data sharing, and uploading documents and PowerPoint presentations, by using whiteboards and desktop sharing.

Back Cover