SOLUTION GUIDE

Wave 8 | August 2013 | 3725-00675-002 Rev A

Polycom® Unified Communications Deployment Guide for Microsoft® Environments

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks

End User License Agreement

By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product.

Patent Information

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Open Source Software Used in this Product

This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

Disclaimer

While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability

Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided “as is” without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

Visit the Polycom® Unified Communications Solution for Microsoft® Environments for information on Polycom software versions and products supporting Microsoft Lync Server, administrative documentation, and Polycom release notes.

Contents

About This Guide

This partner solution guide uses a number of conventions that help you to understand information and perform tasks.

Conventions Used in this Guide

This user guide contains terms, graphical elements, and a few typographic conventions. Familiarizing yourself with these terms, elements, and conventions will help you perform phone tasks.

Information Elements

The following icons are used to alert you to various types of important information in this guide:

Icons Used in this Guide

Name	*Icon*	*Description*
Note		The Note icon highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.
Administrator Tip		The Administrator Tip icon highlights techniques, shortcuts, or productivity related tips.
Caution		The Caution icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.
Warning		The Warning icon highlights an action you must perform (or avoid) to prevent issues that may cause you to lose information or your configuration setup, and/or affect phone or network performance.
Web Info		The Web Info icon highlights supplementary information available online such as documents or downloads on support.polycom.com or other locations.
Timesaver		The Timesaver icon highlights a faster or alternative method for accomplishing a method or operation.
Power Tip		The Power Tip icon highlights faster, alternative procedures for advanced administrators already familiar with the techniques being discussed.
Troubleshooting		The Troubleshooting icon highlights information that may help you solve a relevant problem or to refer you to other relevant troubleshooting resources.

Name	*Icon*	*Description*
Settings		The Settings icon highlights settings you may need to choose for a specific behavior, to enable a specific feature, or to access customization options.

Typographic Conventions

A few typographic conventions, listed next, are used in this guide to distinguish types of in-text information.

Typographic Conventions

Convention	*Description*
Bold	Highlights interface items such as menus, soft keys, file names, and directories. Also used to represent menu selections and text entry to the phone.
Italics	Used to emphasize text, to show example values or inputs, and to show titles of reference documents available from the Polycom Support Web site and other reference sites.
Blue Text	Used for cross references to other sections within this document. If you click on text in this style, you will be taken to another part of this document.
Fixed-width-font	Used for code fragments and parameter names.

What's in This Guide?

Use this list to get an overview of each chapter and quickly navigate to a specific chapter.

Getting Started with Polycom® Unified Communications for Microsoft® Use this chapter to get an introduction and an overview of the Lync Server 2013 solution, Polycom Unified Communications, and Polycom Calendaring for Outlook (PCO). This section provides information you need to begin your deployment, and supported hardware and software versions.

Using Polycom®-Enabled Unified Communications with Microsoft® Lync™ Server 2010 and 2013 This chapter gives you an overview of the Polycom-enabled unified communications solution for Microsoft Lync Server 2010 and 2013 environments.

Deploying Polycom® Group Series Systems This chapter shows you how to deploy RealPresence Group Series systems in a Microsoft Lync Server 2010 and 2013 environment.

Deploying Polycom® HDX Systems This chapter shows you how to deploy Polycom HDX systems in a Microsoft Lync Server 2010 and 2013 environment.

Deploying Polycom® Immersive Telepresence (ITP) Systems This chapter shows you how to deploy Polycom ITP systems in a Microsoft Lync Server 2010 and 2013 environment.

Deploying Polycom® RMX Systems This chapter shows you how to deploy the Polycom RMX conference platform in a Microsoft Lync Server 2010 and 2013 environment.

Deploying Polycom® DMA Systems This chapter shows you how to deploy Polycom DMA conference solution in a Microsoft Lync Server 2010 and 2013 environment.

Polycom® Calendaring for Outlook This chapter shows you how to deploy Polycom Calendaring for Outlook.

Appendix A: Polycom® HDX System Configuration Files Use this appendix to understand Polycom HDX system configuration files and permissible values.

Appendix B: Exchange Calendar Polling Information Use this appendix to get information on Microsoft exchange calendar polling.

Troubleshooting This section lists troubleshooting tips to common problems you may run across with this solution.

Getting Help This section directs you to further documentation and resources that apply to this solution.You will also find links to the Polycom Community, which contains a number of discussion forums you can use to share ideas with your colleagues.

1: Getting Started with Polycom® Unified Communications for Microsoft®

This Polycom solutions guide shows you how to deploy Polycom® Unified Communications (UC) software and products in a Microsoft® environment. The purpose of this guide is to assist administrators deploying Polycom products in a Microsoft environment and explain a number of Microsoft deployment models, architectures, and limitations of the solution.

Introducing Support for Lync Server 2013

The Wave 8 releases for HDX (3.1.2), Group Series (4.1.1), DMA (6.0.2) and RMX (8.1.7) deliver backwards compatibility with Lync Server 2013. This phase leverages the existing support for the Microsoft RTV codec delivering the same experience provided with Lync Server 2010, specifically up to 720p for point-to-point calling (and multipoint calls held on the RMX) and up to VGA for multipoint calls on Lync Server.

Lync Server 2013 introduces support for a new video codec Microsoft H.264 SVC (not to be confused with standards-based H.264 or SVC which is not compatible) and removes the existing H.263 codec within the Lync 2013 client. This new Scalable Video Coding (SVC) technology delivers a Continuous Presence style experience that is limited to up to 5 active speakers, Microsoft refers to this as “Gallery View” (see below).

Polycom plans to introduce support for this codec within Group Series endpoints and RMX bridge infrastructure, with HDX continuing to leverage the existing support for the RTV codec. This backwards compatibility release will enable Lync 2010 use cases with Lync 2013, with the existing RTV codec.

The Wave 8 releases also support Lync Server 2010, with support for Office Communications Server 2007 R2 being removed. For customers requiring on-going support from Polycom on this version, it is recommended that Wave 7 releases continue to be used.

From an administratrative perspective, both Lync Server 2010 and 2013 utilize similar administration tools, as such the Lync Server sections refer to both Lync Server 2010 and 2013 – screen shot user interfaces may reflect a Lync Server 2010 design.

Before You Begin

Deploying Polycom Unified Communications in a Microsoft environment requires planning and knowledge of session initiation protocol (SIP) video conferencing and video conferencing administration. You should also have knowledge of the following Microsoft infrastructure:

- A domain name server
- Lync Server 2010 or 2013 Management Shell and in particular, the Windows PowerShell feature
- Microsoft Active Directory server
- Microsoft Exchange Server

This document assumes that these systems are already deployed and that Microsoft administrators are available to administrators of Polycom Unified Communications.

What's New?

New features for Lync Server 2013 include the following:

- Support for HDX system, Group Series system, DMA conference solution, and RMX conference platform
- Support for Polycom RealPresence Group Series systems

Hardware and Software Dependencies

- Lync Server 2010
- Lync Server 2010 Cumulative Update 9 (March 2013)
- Lync Server 2013
- Lync Server 2013 Cumulative Update 1 (February 2013)

Polycom-Enabled Unified Communications

The Polycom Unified Communications solution for Microsoft is a suite of Polycom hardware devices and session initiation protocol (SIP) software applications that enable you to integrate high-quality video and audio conferencing across Microsoft® platforms.

Polycom Unified Communications for Microsoft includes the following integrations:

- **Polycom-enabled Unified Communications** enables you to integrate the Microsoft SIP infrastructure that includes presence-based, real-time instant messaging (IM), voice, video, and data communications.

- **Polycom Calendaring for Outlook** offers an integrated and enhanced calendaring experience for both Polycom and Microsoft endpoints.

Polycom Unified Communications (UC) software 4.1.0 enables you to deploy your Polycom video infrastructure and endpoints with Lync Server 2010 or 2013. The Microsoft Lync Server manages presence for each registered Polycom endpoint or component. The Microsoft UC infrastructure provides full-featured video calls between Lync clients and Polycom components, including point-to-point calls and video conferencing, high-quality video, and calling directly from a contact list.

End User Advantages

The solution explained in this guide enables end users to:

- Launch video calls from Lync or Office Communicator clients by clicking links included in meeting invitations provided by Polycom Calendaring for Outlook
- Initiate video calls to Polycom endpoints from a contact list in Microsoft Outlook or SharePoint (Polycom endpoints or the Exchange or SharePoint server must be provisioned with Lync Server.)
- Integrate Lync users into Polycom HDX or Group Series system favorites list and call them directly from the list
- Employ enhanced presence features of Lync Server in a Polycom infrastructure environment
- Call a Lync user with a Companion Mode Polycom HDX or Group Series system registered to the same Lync Server account. The call rings at both devices (call forking), and the recipient can answer using either device.

System Administrator Advantages

The solution explained in this guide enables administrators to:

- Provide logistical support for large-scale deployment of Polycom HDX or Group Series systems in a Lync Server environment. The Polycom CMA system provisions the Lync Server integration and Polycom Calendaring for Outlook settings, and the Polycom DMA system provides scalable, fault-tolerant multipoint conferencing.
- Use Polycom's SIP expertise to integrate Lync clients with your Polycom video network and endpoints in a way that requires a minimum of network administration and maintenance

Polycom Calendaring for Outlook

Polycom Calendaring for Outlook is an add-in for Microsoft Outlook that enables you to create meeting schedules and send instantly send meeting invitations. This feature requires Polycom Calendaring for Outlook which offers an integrated and enhanced experience for all video conference participants.

End User Advantages

- Users can easily add video to meetings as well as record meetings without the direct help of IT or a video conferencing administrator. Users can join a video conference with a single click from an Outlook calendar entry.
- Meeting participants can track their video- and audio-enabled meetings on the same calendar they use to track their other meetings.

- Meeting participants can join conferences by clicking a link in a calendar entry on their associated video or audio endpoint system.
- Makes real-time calendar information available for Polycom HDX and Group Series endpoints. Conferencing enables smart rooms that automatically display meeting details so users can immediately identify the video conference.
- Incorporates virtual meeting rooms (VMRs) that ensure a reliable experience for end users. End users can connect to unique VMRs instead of re-using video bridge numbers.

System Administrator Advantages

- Decreases user dependency on administrators by offering users a simple procedure for scheduling video- and audio-enabled meetings.
- Maximizes the use of visual communication assets and return on investment (ROI).

Getting Help and Support Resources

This partner solution guide includes a Getting Help section where you can find links to Polycom product and support sites and partner sites. You can also find information about The Polycom Community, which provides access to discussion forums you can use to discuss hardware, software, and partner solution topics with your colleagues. To register with the Polycom Community, you will need to create a Polycom online account.

The Polycom Community includes access to Polycom support personnel, as well as user-generated hardware, software, and partner solutions topics. You can view top blog posts and participate in threads on any number of recent topics.

- Polycom Calendaring for Outlook enables administrators to deploy scalable video infrastructure into an existing Exchange environment.

2: Using Polycom®-Enabled Unified Communications with Microsoft® Lync™ Server 2010 and 2013

This chapter provides an overview of the Polycom®-enabled Unified Communications solution for Microsoft® Lync™ Server 2010 and 2013 environments. Lync Server 2010 and 2013 provide presence-based, real-time instant messaging (IM), voice, video, and data communications. This chapter gives you an overview of Polycom products and versions you can use with this solution and details features available with Lync Server.

Note: Using Microsoft Lync

This guide does not provide full administration or maintenance procedures for Microsoft Lync Server 2010 or 2013. For full administrative procedures, see Microsoft Lync Server 2013.

This section includes the following tasks:

- Features of the Polycom-Enabled Lync Server Solution
- Supported Lync Server Versions
- Before You Begin
- Getting Help from Polycom Solution Support Services
- Polycom Products Tested for Use with this Solution
- Setting Up Dial Plans for a Lync Server Environment
- Supporting Remote and Federated Users in Lync Server Environments
- Understanding Microsoft Domains and Application Pools

Features of the Polycom-Enabled Lync Server Solution

Integrating Polycom products with Microsoft Lync Server 2010 and 2013 enables:

- Point-to-point calls between Polycom HDX systems and Microsoft Lync clients
- Real-time presence information between Polycom devices and Microsoft Lync clients
- Support for remote and federated endpoints to participate in point-to-point calls and video conference calls
- High-quality video (720p) between Lync clients and Polycom endpoints
- Participation in Lync Server-hosted multi-point conferences using Polycom endpoints

- Microsoft Lync clients to view the presence for Polycom RMX meeting rooms and start one-click conferences. Note this is an optional feature.

Supported Lync Server Versions

Polycom supports the following Lync Server environments:

- Lync Server 2010
- Lync Server 2010 Cumulative Update 9 (March 2013)
- Lync Server 2013
- Lync Server 2013 Cumulative Update 1 (February 2013)

Before You Begin

Administrators require the knowledge of the following to successfully perform the tasks in this guide.

General Knowledge

- Prior knowledge and experience with Lync Server components. In particular, you should be familiar with Lync Server Management Shell.
- Prior knowledge and experience with the Polycom RMX systems, HDX systems, and DMA systems. You can access Polycom systems product documentation and relevant software at Polycom Support.
- Lync Server product documentation and relevant software.
  - To view Lync Server 2010 documentation, see Microsoft's Lync Server 2010 Planning Guide and Microsoft Lync Server 2010 on the Microsoft TechNet Library.
  - To view Lync Server 2013 documentation, see Microsoft's Lync Server 2013 documentation library on the Microsoft TechNet Library.
- Administrators also require specific knowledge of the following components of Microsoft Lync Server:
  - **Microsoft Domain Accounts** To participate in calls with Microsoft components, including Lync clients and Lync-hosted multipoint calls, your Polycom devices must have an account in a Windows domain accessible by the Lync Server environment. You can create a new Lync account for your Polycom device, or you can set up your Polycom device with an existing Lync account. This Windows domain can be an Active Directory domain or a SIP domain. You will need to configure the proper capabilities and settings in the domain; you will need to configure these settings at the domain level, with policies, and at the account level.

Encryption and Security

- Microsoft environments require TLS, which means you must use SSL certificates
- You can configure call encryption using compatible encryption settings between the Lync server and Polycom components.

Remote and Federated Users

You can register remote Polycom components to your Microsoft Lync Edge server to support remote users. Polycom components also support federation with the use of a Microsoft Lync Edge server.

Microsoft Call Admission Control

The Polycom HDX system and RealPresence Group Series system and the RMX conference platform can take advantage of Microsoft Call Admission Control (CAC). The following requirements apply:

- Your Microsoft environment must include an Edge Server.
- Your RMX system must be configured for an Edge Server, as well as Microsoft Call Admission Control. See Enabling Edge Server Integration with Your Polycom RMX System.
- You do not need to set up Microsoft CAC on a Polycom HDX or RealPresence Group Series system.

Microsoft Real-Time Video (RTV)

Polycom HDX systems and RMX conferencing bridges include support for Microsoft's RTV media codec and Lync multiparty calling.

Note: RTV support for Lync Server 2013

The H.263 codec has been deprecated for Lync Server 2013, and RTV support is required to deploy HDX systems, RealPresence Group Series systems, and RMX conference platforms with Lync Server 2013.

- Polycom HDX systems now support all RTV video resolutions for peer-to-peer Lync video calls and multi-party video conferences that you host on the Lync Audio video AVMCU. You do need to obtain the RTV option key:
  - To support Lync conferencing
  - To support RTV video resolutions beyond CIF resolution using H.263 codec when registering with Lync Server 2010. (The H.263 codec has been deprecated for Lync Server 2013)
  - RTV is supported on an RMX system only if you have an MPMx card.

Getting Help from Polycom Solution Support Services

Polycom provides support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and certified partners. These services are intended to help customers successfully design, deploy, optimize, and manage Polycom visual communication within their third-party UC environments. If you want to deploy Polycom Calendaring for Outlook (PCO) or Microsoft Lync

Server, you will need to contact Polycom Services or contact your local Polycom representative for more information.

Polycom Products Tested for Use with this Solution

The following table summarizes Polycom products that have been tested for use with Lync Server 2010 and 2013.

Table 1: Polycom Products and Supported Lync Versions

Product	*Version*	*Description*
Microsoft Lync 2013 Server	5.0.8308.291	February 2013 Cumulative Update
Microsoft Lync 2013 Client	15.0.4454.1509	February 2013 Cumulative Update
Microsoft Lync 2010 Server	4.0.7577.216	March 2013 Cumulative Update
Microsoft Lync 2010 Client	4.0.7577.4378	March 2013 Cumulative Update
Microsoft Lync Attendee	7577.4391	June 2013 Cumulative Update
Microsoft Lync for Mac	14.0.5 (130524)	June 2013 Cumulative Update
Microsoft Exchange 2007 SP3	8.3.264.0	
Microsoft Exchange 2010 SP2	14.2.342.3	
Microsoft Outlook 2007	12.0.6557.5001 SP2	
Microsoft Outlook 2010	14.0.6129.5000	
F5 BIG-IP Load Balancer 1500	11.2.0.2557	
Polycom HDX 8006	3.1.2	
Polycom HDX 9006	3.1.2	
Polycom HDX 9004	3.1.2	
Polycom HDX 7000	3.1.2	
Polycom HDX 8000	3.1.2	
Polycom HDX 4500	3.1.2	
Polycom HDX 6000	3.1.2	
Polycom HDX 4003	3.1.2	

Product	*Version*	*Description*
Polycom Group Series 300	4.1.1	
Polycom Group Series 500	4.1.1	
Polycom Group Series 700	4.1.1	
Polycom RSS 4000	8.5.0	
Polycom DMA 7000	6.0.2	
Polycom RMX 4000 / 2000 / 1500 MPMx	8.1.7	
Polycom RMX 800s	8.1.7	
Polycom XMA	7.3.0	
Polycom CMA Desktop (PC and Mac)	5.2.4.29384	
Polycom RealPresence Desktop	3.0.38914	
Polycom TPX 306	3.1.2	
Polycom TPX 408	3.1.2	
Polycom OTX 306	3.1.2	
Polycom CX100, CX200 CX500, CX600, CX5000 and CX7000	CX100, 200 – no version number CX500 - 7577.4397 CX600 - 7577.4397 CX3000 - 7577.4397 CX5000 - 1.5.5029.0 CX7000 - 1.2.0.5544	
Polycom Calendaring for Outlook	1.4.0	

Setting Up Dial Plans for a Lync Server Environment

You can include and use several dialing plans concurrently in your Lync environment depending on your deployment scenario.

Matched URI Dialing

Enables users to dial the full SIP URI of the conference room or endpoint. Include this dialing method if you need to support federated users. Matched URI dialing is also required to use connect links included in meeting invitations generated from Polycom Calendaring for Outlook.

Matched URI dialing is enabled as part of the process of creating a static route for the RMX system or for the DMA system you are using. See Deploying Polycom® RMX Systems or Set the Routing for the Polycom DMA System, respectively.

Supporting Remote and Federated Users in Lync Server Environments

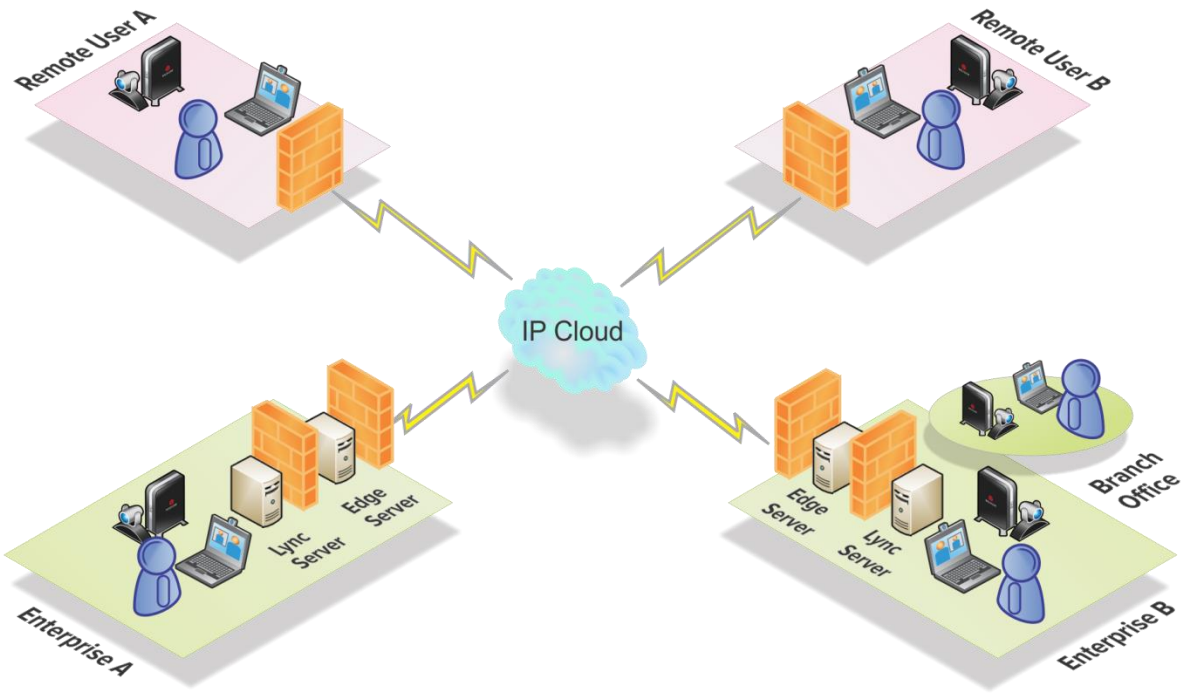
You can support remote and federated users by including a Lync Server edge server in your environment.

- Remote users are users located outside of an organization's firewall. A remote user registered to an enterprise's Lync Server 2010 or 2013 edge server can make and receive calls to and from enterprise users without the use of a VPN or additional firewall traversal device.
- Federation is a trust relationship between two or more SIP domains that permits users in separate organizations to communicate in real-time across network boundaries as federated partners. Federated users registered to a separate Lync Server on a separate enterprise network are able to make and receive calls to endpoints and video infrastructure on an external network that is behind one or more firewalls.

Lync Server with an installed access edge server role supports the Interactive Connectivity Establishment (ICE) protocol. The ICE protocol enables devices outside an organization's network to call other devices that are also part of the Polycom-enabled unified communications solution. This functionality is supported with Lync Server 2010 or 2013, the Polycom video infrastructure, and Polycom video systems.

The following figure illustrates a possible edge server deployment scenario. In this example scenario, enterprises A and B are federated, meaning that users in Enterprise A can communicate with users in Enterprise B, and vice versa. Enterprise B also contains a branch office, which in this example is a Polycom HDX user behind more than one firewall. The user in the Branch Office can also place and receive calls to and from other enterprises and remote users.

Figure 1: Lync Server Environment with a Lync Server Edge Server



Users in enterprise A and B can place calls to remote users (Remote User C and Remote User D). The remote users can call each other and users in both enterprises.

In a Lync Server 2010 or 2013 edge server environment, calls are supported to the following devices:

- Polycom HDX and Group Series systems
- Lync 2010 clients or Lync 2013 clients
- Polycom RMX systems
- Polycom DMA systems

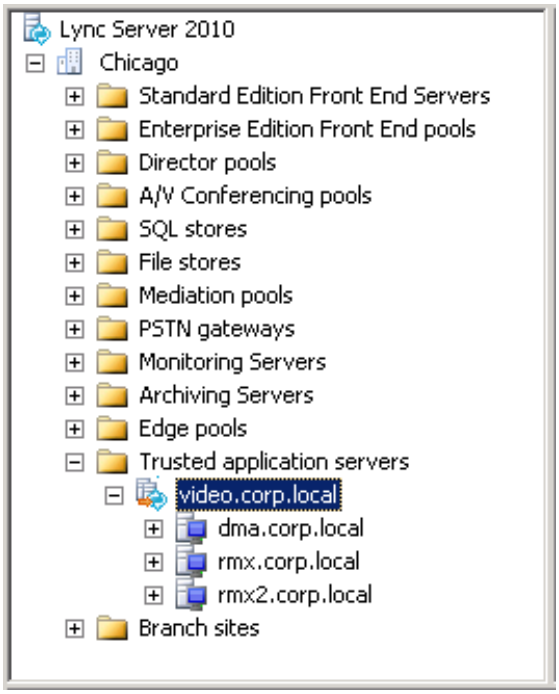
Understanding Microsoft Domains and Application Pools

It is important to understand how the domains are set up in your Microsoft environment. Polycom recommends the following best practices when configuring your application pools within Lync Server and when configuring DNS.

Using Multiple Computer Application Pools

As a best practice, you should create a multiple computer-trusted application server pool and include your DMA system or RMX system SIP signaling domains as nodes under this pool, as shown in the following figure.

Figure 2: Using a Multiple Computer Trusted Application Server Pool



In this example, `video.corp.local` is the pool name. This method simplifies your Microsoft unified communications environment and also allows you to add additional RMX systems or DMA systems at a later time. Refer to Microsoft documentation for more information about pool names.

The FQDNs of the DMA SIP signaling interface (`dma.corp.local`) and the two RMX SIP signaling domains are `rmx.corp.local` and `rmx2.corp.local` and are used as destination routes.

Static Routes and the Match URI

When you configure a Polycom RMX or Polycom DMA system for integration with Microsoft unified communications, you must define a static destination route as well as a Match URI that is used to direct SIP traffic.

Although both the route's Match URI and the destination route can be set to the same domain name, Polycom recommends using unique values for each. You can do using a multiple computer application pool.

Microsoft Domains and DNS Entries

If the primary SIP domain is in a different namespace than the Active Directory domain, Polycom recommends placing the DNS host record for the RMX Signaling Host IP Address or DMA system in the Active Directory domain, for example, `rmx.corp.local`.

A DNS host record can also be created in the SIP domain if a Forward Lookup Zone is available for that domain to add the record.

The RMX conference platform, DMA system, and Lync Server need to resolve the RMX / DMA host record identically, regardless of the domain selected to store the DNS Host record.

The following table provides examples of different Microsoft environments and example values for an environment that has different namespaces for SIP and Active Directory domains.

Table 2: Microsoft Environments with Different SIP and Active Directory Domain Namespaces

Domain	*Example*	*Usage Notes*
Primary SIP domain for Lync	sipdomain.com	This domain should be used as the match URI in federated environments.
Active Directory domain	corp.local	
DMA system FQDN	dma.corp.local	DMA virtual signaling IP address. FQDN must match security certificate
RMX system FQDN	rmx.corp.local	RMX SIP signaling IP address. FQDN used for DNS must match security certificate.
Additional RMX system FQDN	rmx2.corp.local	RMX SIP signaling IP address. FQDN used for DNS must match security certificate.
Application Pool	video.corp.local	Make this domain a friendly name for users to use to dial into conferences. Does not need DNS representation.

3: Deploying Polycom® Group Series Systems

When deploying a Polycom® Group Series system for use with the solution, you must complete tasks in Lync™ Server 2010 or 2013 and the Group Series system.

This section contains the following major tasks:

- Configuring Lync Server for Use with a Group Series System
- Configuring Your Polycom Group Series System for Lync Server
- Supporting Microsoft Real-Time Video (RTV)

Configuring Lync Server for Use with a Group Series System

This section explains how to configure Lync Server settings to use a Polycom Group Series within a Microsoft environment. You must perform these tasks in the following order:

1. Configuring Authentication in Lync Server
2. Using Microsoft Call Admission Control
3. Enabling RTV on the Lync Server
4. Adding Calendar and Scheduling Features to Polycom Group Series Systems
5. Enabling Conference Rooms for the Lync Server
6. Enabling Conference Room Access for Remote and Federated Users
7. Adding Lync Contacts to Conference Room Local Address Book

Note: Configure Lync Client Users in Microsoft Active Directory

Before completing tasks in this section, you must have configured Lync client users in Microsoft Active Directory and enabled Lync Server. Talk to your Microsoft Active Directory and Lync Server administrators or visit Preparing Active Directory Domain Services for Lync Server 2013.

Configuring Authentication in Lync Server

If you want to include a Group Series system within your Microsoft environment, you must enable NTLM on your Microsoft Lync Server. By default, NTLM is enabled in Lync Server. If NTLM has been disabled for any reason, you need to enable it.

Polycom HDX and Group Series systems support only NTLM authentication, and do not support Kerberos.

Using Microsoft Call Admission Control

Microsoft Call Admission Control policies are supported and enforced when your Group Series system is registered to a Microsoft Lync environment that includes an Edge server.

When a Microsoft Call Admission Control policy is enforced in a Microsoft Lync Server Environment, the following limitations apply:

- SIP calls between Group Series systems are unable to support dual-stream People+Content™.
- The maximum available bandwidth for SIP calls is 2 Mbps.

Enabling RTV on the Lync Server

If you want to support high-quality RTV, you need to change the default video settings of your Lync Server. Lync Server 2013 is by default enabled for full HD 1080p, however this is only whereby the Microsoft H.264 SVC codec is used. For Wave 8 (Polycom's Lync 2013 compatibility release or version 4.1.1 for Group Series), the RTV codec is used, therefore the changes outlined below still apply whereby resolutions beyond VGA are desired.

To change the default video settings for your Lync Server:

1. Access Lync PowerShell.
2. Change the video settings for your Lync Server. For example,
   ```
   Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M
   ```
3. Restart the Lync Server to apply your changes.

Adding Calendar and Scheduling Features to Polycom Group Series Systems

If you want to add a scheduling feature to your Group Series system, you need to configure a conference room user account in Active Directory. To create a conference room user account, you can use a script, the Active Directory Users and Computers management console, or custom software. The following procedure shows you how to add a conference room user manually in the Active Directory Users and Computers management console.

If your deployment includes Polycom Calendaring for Outlook, you will need to perform further procedures outlined in Configuring Mailboxes for Room-based HDX Systems.

Note: Set Passwords to Never Expire

If these conference room users have an expiring password, you will need to keep track of the users and passwords and make sure to update the accounts as required. Polycom recommends setting the passwords to never expire.

To add a conference room user to the Active Directory:

1. Go to **Start > Run** and open the Active Directory Users and Computers console by entering: dsa.msc
2. In the console tree, select **Users > New > User**.
3. In the New User wizard, enter the required conference room user information and click **Next**.
4. Set the user password. Polycom recommends that you also set the **Password never expires** option.
5. Click **Next** and **Finish**.
6. Repeat for each conference room that has a Polycom Group Series system.

Enabling Conference Rooms for the Lync Server

After adding the conference room user accounts to Active Directory, you must enable and configure them for use with Lync Server.

Polycom recommends using Lync PowerShell to do this. For more information, see Windows PowerShell and Lync Server Management Tools.

To enable a conference room user for the Lync Server:

1. Access Lync PowerShell.
2. Enable a conference room user for Lync. For example,

```
Enable-CsUser -Identity Ken Myer -RegistrarPool lync.corp.local
-SipAddressType FirstNameLastName -SipDomain sipdomain.com
```

Enabling Conference Room Access for Remote and Federated Users

If you are supporting remote users and federated users, you need to configure the following on the Lync Server edge server:

- Enable support for external users for your organization
- Configure and assign one or more policies to support external user access

Once you have configured the Lync Server edge server, you can enable Lync Server to support remote and federated user access to a conference room.

To enable remote and federated user access to a conference room:

For detailed instructions on configuring support for external users in Lync Server, see Microsoft Configuring Support for External User Access.

Adding Lync Contacts to Conference Room Local Address Book

To add Lync contacts to your Polycom system local address book, use the Polycom system user account and password to log on to a Lync client. You can then use the Lync client to add the contacts to the Polycom system account.

After adding contacts through the Lync client, contacts display on the Group Series system the next time you log on.

For more information about displaying contacts on your Group Series system, see Configuring Display Options for the Group Series System Contact List.

Note: Configure a Maximum of 200 Personal Contacts per Group Series System User

Polycom recommends that you configure the Lync Server to allow no more than 200 contacts per user (the default setting is 250). The Group Series system displays a maximum of 200 contacts per user.

Configuring Your Polycom Group Series System for Lync Server

Before you begin configuring your Polycom Group Series system for a Microsoft environment, you should ensure that the Group Series system is installed according to standard installation procedures. Consult the Administrator's Guide for Polycom Group Series Systems to identify the installation required for your Group Series model. Configuring your Group Series system for a Microsoft environment requires the following tasks:

- Installing the RTV Option Key on your Group Series System
- Register a Polycom Group Series System with the Lync Server
- Understanding SIP Settings
- Configuring the Polycom Group Series System LAN Properties
- Configuring Display Options for the Group Series System Contact List
- Configuring AES Encryption
- Supporting Lync-hosted Video Conferencing and or Lync Server 2013
- Supporting Microsoft Real-Time Video (RTV)

Installing the RTV Option Key on your Group Series System

Without an RTV option key, your RealPresence Group Series system is capable of CIF resolution for point-to-point Lync 2010 calling using H.263. RTV must be enabled for enabling Lync Server 2010 multi-party calling and/or higher quality video (up to 720p for point-to-point and VGA for multi-party). For Lync 2013 support the RTV option key is mandatory (for both point-to-point and multi-party calling scenarios).

Note: Register Polycom endpoints to Lync Server for RTV Video and Conferencing

RTV video and Lync-hosted conferencing are only supported when you directly register Polycom endpoints to Lync Server.

Register a Polycom Group Series System with the Lync Server

When you register a Group Series system with a Lync Server, the Polycom Group Series system user can see a list of Lync 2010 or 2013 contacts and whether contacts are online or offline. Contacts display in the directory and users can choose to display contacts on the home screen (up to 5) or call a contact. You can find descriptions of all SIP settings shown in this procedure in the following section Understanding SIP Settings.

To configure a Group Series system to register with Lync Server:

1. Open a browser window and in the Address field enter the Polycom system IP address or host name.
2. Go to **Admin Settings > Network > IP Network** and select **SIP**.
3. Configure the settings in the **SIP Settings** section of the **IP Network** screen shown in the next section Understanding SIP Settings.
4. Click **Save**.

   Once the Polycom Group Series system registers with Lync Server, you can continue on to Configuring the Polycom Group Series System LAN Properties.

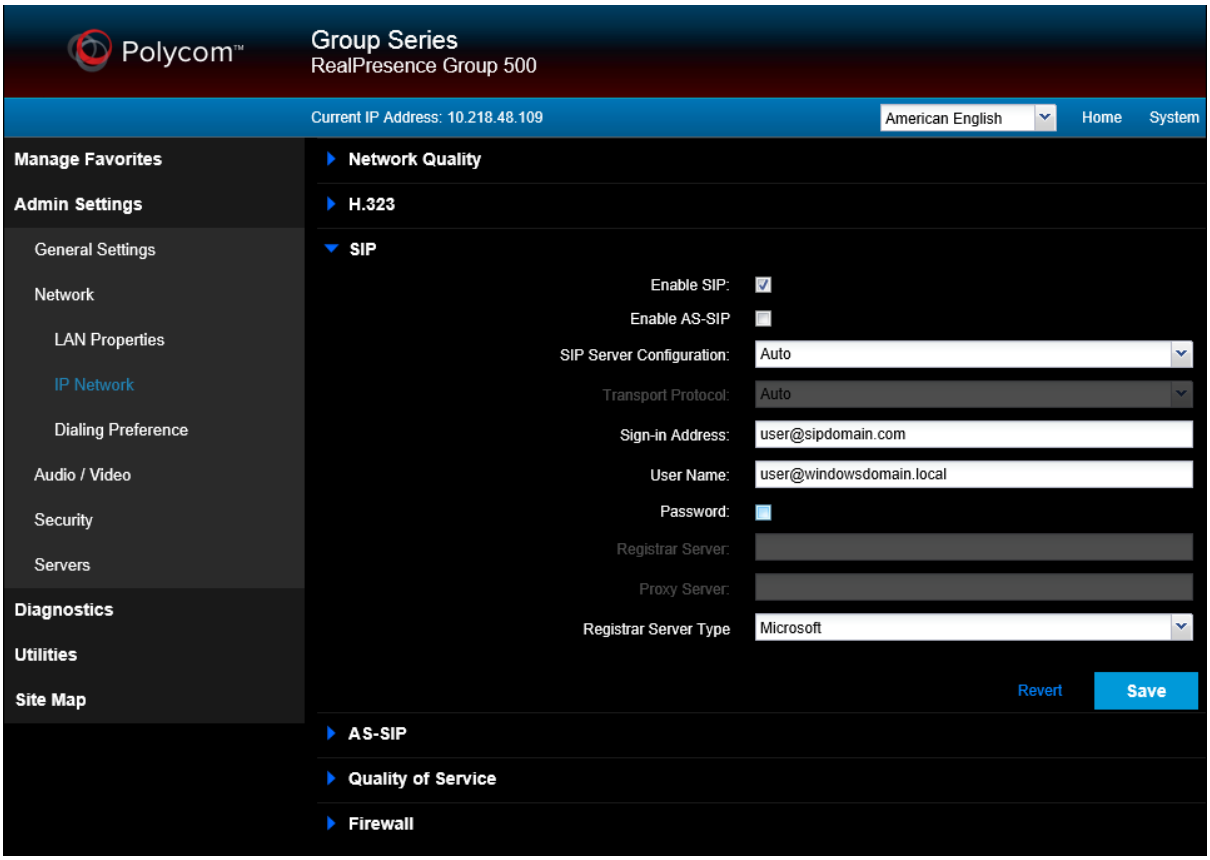
Note: Registering Polycom endpoints to Lync Server 2013 requires an RTV option key

An RTV option key is a requirement for integration with Lync Server 2013 as the H.263 codec has been deprecated. Support for Microsoft H.264 SVC is planned within a future Group Series system update.

Understanding SIP Settings

This section provides an overview of the SIP settings available on the RealPresence Group Series system shown in Figure 3.

Figure 3: RealPresence Goup Series System SIP Settings



The following list describes all SIP settings on the **IP** Network screen that you need for Lync Server.

- **Enable SIP** Check to enable the RealPresence Group Series system to make and receive SIP calls.
- **SIP Server Configuration** Select Auto if your Microsoft Lync Server configuration is set up for automatic discovery, which requires you to correctly configure Lync SRV records. If the Microsoft Lync Server is not configured for automatic discover, select Specify.
- **Registrar Server** If you selected Specify in the SIP Server Configuration field, you need to specify the DNS name of the SIP Registrar Server.
  - In a Lync Server environment, specify the DNS name of the Lync Front End, Pool or Director. The default port is 5061.
  - If registering a remote RealPresence Group Series system with a Lync Server Edge server, use the fully qualified domain name of the Access Edge server. The port for the Edge server role is usually 443 and must be entered explicitly.

Polycom recommends using the DNS name. The format for entering the address and port is the following: `<DNS_NAME>:<TCP_Port>:<TLS_Port>`

Syntax Examples:

- To use the default port for the protocol you have selected: `lyncserver.corp.local`
- To specify a different TLS port (and use the default TCP port): `lyncserver.corp.local:443`

- **Proxy Server** Specify the DNS name or IP address of the SIP Proxy Server. If you leave this field blank, the Registrar Server is used. If you selected Auto for your SIP Server Configuration and leave the Proxy Server field blank, no Proxy Server is used.

  By default for TCP, the SIP signaling is sent to port 5060 on the proxy server. By default for TLS, the SIP signaling is sent to port 5061 on the proxy server.

  The syntax used for this field is the same as for the Registrar Server field.

  Note: In a Microsoft environment, the Proxy server and the Registrar server are always the same server, so only one server address field is required.

- **Transport Protocol** The SIP network infrastructure in which your Polycom Group Series system is operating determines which protocol is required.
  - **Auto** enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for Microsoft environments.
  - **TLS** provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060. TLS is required when connecting to Microsoft Lync.
  - **TCP** provides reliable transport via TCP for SIP signaling.
  - **UDP** provides best-effort transport via UDP for SIP signaling.
- **Sign-in Address** Specify the system's SIP name. This is the SIP URI or Lync sign-in address. Specify the address for the conference room or user account created for the Polycom system.
- **User Name** Specifies the name and Windows Domain to use for authentication when registering with a SIP Registrar Server, for example, `user@windowsdomain.local`.

  Polycom Group Series systems supports the User Principal Name format (username@domain.com) as well as the legacy Microsoft DOMAIN\username format. If the SIP server requires authentication, this field and the password cannot be blank.
- **Password** When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP Server.
- **Registrar Server Type** For Lync Server this must be set to Microsoft.

Configuring the Polycom Group Series System LAN Properties

To register with Lync Server, the Polycom Group Series system must be able to access a DNS server whereby the name for the Lync Pool or Lync edge server has a valid domain name resolution.

To configure the Polycom system LAN properties:

1. Open a browser window and in the Address field enter the Polycom system IP address or host name.
2. Go to **Admin Settings > Network > LAN Properties**.
3. If needed, enter the **Domain Name** for the domain to which the Polycom system belongs.
4. In the DNS Servers field enter the IP address for a DNS server that shares DNS zone information with the Lync Server. If you are registering a remote Polycom system, use a public DNS server that shares DNS zone information with the Lync Server Edge server.
5. Click **Update**.

Configuring Display Options for the Group Series System Contact List

You can display your Microsoft contacts in your Group Series system contact list.

To configure display options for contact list information:

1. Open a browser window and in the Address field enter the Polycom Group Series system IP address or host name.
2. Go to **Admin Settings > Servers > Directory Servers**.
3. In the Lync Server section of the Directory Servers page, configure these settings:
   - **Server Type** Specifies whether the SIP Registrar Server is a Lync Server. Enabling this setting activates integration features such as the Microsoft global directory and Lync contact sharing with presence.
   - **Registration Status** Upon successful authentication this should display as Registered (see below).

- **Domain Name** Specifies the Windows Domain to use for Directory lookup, for example, `windowsdomain.local`.
  - Polycom Group Series systems supports the User Principal Name format (windowsdomain.local) as well as the legacy Microsoft NETBIOS domain format.

4. Click **Save.**

Note: Personal Lync contacts are not displayed until Directory Services configuration is completed

Without completing the Directory Services configuration neither Lync Directory search, personal favorites or contacts list are displayed within the contacts menu.

Configuring AES Encryption

Polycom endpoint systems support AES media encryption. You need to set your system encryption settings to be compatible with your Lync Server settings.

Polycom recommends that you use automatic discovery, which requires you to ensure that each Polycom endpoint has compatible encryption settings and requires you to correctly configure Lync SRV records. If Lync Server is not configured for automatic discover, you need to select Specify.

Each codec within Polycom systems must have the same settings.

- If both Microsoft Lync and Polycom endpoints have encryption turned off, calls connect without encryption.
- If Microsoft Lync or a Polycom endpoint is set to require encryption and the other is not, calls fail to connect.

To configure AES encryption:

1. Open a browser window and in the Address field enter the Polycom system IP address or host name.
2. Go to **Admin Settings > Security > Global Security**.
3. In the Encryption menu select the Require AES for Encryption for Calls drop-down menu, select **When Available** or **Required**.

Supporting Lync-hosted Video Conferencing and or Lync Server 2013

Lync-hosted conferencing is supported only when Polycom endpoints are registered to Lync Server. To participate in Lync-hosted video conferences using a Polycom Group Series system or register the system to Lync Server 2013, you must install the RTV option key on the Polycom Group Series system. If you want to use the call management features, you will need to pair your Group Series system with a Polycom Touch Control.

When using Lync-hosted video conferencing, keep in mind the following points:

- When in a Lync-hosted call, the Polycom Group Series system displays a Busy presence state. It rejects any inbound calls.
- When in a Lync-hosted call, other multipoint calling methods, such as internal multipoint hosting, RMX/DMA hosted conferencing, and Conference on Demand, are disabled.
- You need to install the RTV option key on your Group Series system to support Lync-hosted conference calls and 720p high-definition video between a Group Series system and a Lync client.

- You will need the RTV option key to enable support for Lync Server 2013

A Polycom Touch Control is required for the following Group Series system functionality:

- View the participants in a Lync-hosted conference.
- Add participants to the Lync-hosted conference.
- Organize and initiate Lync-hosted conferences with Polycom Group Series and Microsoft Lync clients and groups.

Using the Polycom Touch Control with Lync Conferencing

A Polycom Group Series system must be paired with a Polycom Touch Control to initiate, view, add, and organize participants in a Lync-hosted video conference call.

To initiate a Lync-hosted call:

1. From the Call screen on the Polycom Touch Control, touch **Conference.**
2. Set up the call with the participants you want. You can add participants using any one of the following methods.
   a. Touch **Keypad** and enter the participant SIP addresses. Each time you enter a SIP address, touch **Add** to add it to the list of conference participants.
   b. Touch **Directory**, then touch the names you want to include in the list of participants. If you touch a group, the group opens and you can touch individual names to add them.
   c. Touch **Favorites**, then touch the names you want to include in the list of participants.
3. Touch **Join** when your list of participants is complete.

   The conference call is initiated.

   If you want to add another participant during a conference call, touch **Add Participant** and repeat any one of the methods in step 2. You do not need to put other participants on hold though there may be a brief audio or video pause.
4. To view all participants in a call, touch **Participants** from the call screen.

Understanding Roles in Lync-hosted Calls

Participants in a Lync-hosted call can have one of three roles depending on the level of user rights granted within the call. The privileges associated with each role are shown in Table 4-1 and 4-2. You set up these roles on Microsoft Lync Server, but if you are the conference organizer, you can change the roles of other participants using the Lync client.

The organizer of a Lync-hosted conference can choose to leave the conference by touching **Hang Up**. The other participants can continue with the call.

Table 3: Managing Participants in a Lync-hosted Call

Role	*Add a Participant*	*View Participants*
Organizer	Y	Y
Presenter	Y	Y
Attendee	N	Y

Table 4: Managing a Lync-hosted Call

Role	*Remove a Participant*	*End a Conference*	*Leave a Conference*	*Mute a Participant*	*Mute a Conference*	*Mute Self*
Organizer	Y	Y	Y	Y	Y	Y
Presenter	N	N	Y	Y	Y	Y
Attendee	N	N	Y	N	N	Y

Supporting Microsoft Real-Time Video (RTV)

Microsoft Lync 2010 clients use the RTV protocol by default, which provides VGA and HD 720p video. Polycom supports high-quality RTV video among Microsoft components, Polycom ITP, Polycom HDX and Group Series endpoints, and the Polycom RMX system. RTV video is only supported when Polycom endpoints are registered to Lync Server.

If you do not use RTV, Lync Server 2010 can provide H.263, CIF resolution, and does not support multi-party conference calls.

Microsoft Lync 2013 client utilizes both RTV protocol and H.264 SVC, Polycom continues to support the RTV protocol for both Lync 2010 and 2013 and plans to include support for the Microsoft H.264 SVC codec in Group Series and RMX. Enabling the RTV protocol for Group Series is mandatory when registering with Lync Server 2013.

The following Polycom systems support the RTV protocol:

- Polycom HDX and Group Series systems with the RTV option key.
- Polycom ITP systems.
- Polycom RMX system with the MPMx card

Call Quality Scenarios for RTV Video

The quality of video used depends on the capabilities of the endpoint you are using.

- RTV video requires a minimum call rate of 112 kbps. Calls below this rate connect with audio only.
- Multipoint calls initiated by a Microsoft Lync client are hosted on the Microsoft AVMCU. Polycom Group Series systems must have the RTV key installed in order to connect. Multipoint calls initiated by a Group Series system with the RTV key installed are also hosted on the Microsoft AVMCU.
- Multipoint calls initiated by a RealPresence Group Series system that does not have the RTV key are hosted on the Group Series system's internal multipoint control unit (MCU) and do not use RTV. If a Lync 2010 client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Microsoft clients, the Polycom Group Series system uses RTV when the RTV option key is installed. If the Polycom Group Series system does not have the RTV option, the Lync 2010 client can use H.263/CIF. You must install an RTV option key to make point-to-point calls with Lync 2013.
- When you call into an RMX conference that includes participants uisng a RealPresence Group Series, HDX system, or Polycom ITP, the Polycom systems can use H.264 while Lync uses RTV.
- Polycom ITP systems use RTV only on point-to-point calls with a Lync client and connect with only the primary codec.

4: Deploying Polycom® HDX Systems

When deploying a Polycom® HDX system for use with Lync Server, you must complete tasks in Lync™ Server 2010 or 2013, and the HDX system.

This section contains the following major tasks:

- Configuring Lync Server for use with an HDX System
- Register Polycom HDX System with the Lync Server
- Supporting Microsoft Real-Time Video (RTV)

Configuring Lync Server for use with an HDX System

This section explains how to configure Lync Server settings to use a Polycom HDX in a Microsoft environment. You must perform these tasks in the following order:

1. Configuring Authentication in Lync Server
2. Using Microsoft Call Admission Control
3. Enabling RTV on the Lync Server
4. Adding Calendar and Scheduling Features to Polycom HDX Systems
5. Enabling Conference Rooms for the Lync Server
6. Enabling Conference Room Access for Remote and Federated Users
7. Adding Lync Contacts to Conference Room Local Address Book

Note: Configure Lync Client Users in Microsoft Active Directory

Before completing tasks in this section, you must have configured Lync client users in Microsoft Active Directory and enabled Lync Server. Talk to your Microsoft Active Directory and Lync Server administrators or visit Preparing Active Directory Domain Services for Lync Server 2013.

Configuring Authentication in Lync Server

If you want to include an HDX system in your Microsoft environment, you must enable NTLM on your Microsoft Lync Server. By default, NTLM is enabled in Lync Server. If NTLM has been disabled for any reason, you need to enable it.

Polycom HDX systems and RealPresence Group Series systems support only NTLM authentication, and do not support Kerberos.

Using Microsoft Call Admission Control

Microsoft Call Admission Control policies are supported and enforced when your HDX system is registered to a Microsoft Lync edge server.

When a Microsoft Call Admission Control policy is enforced in a Microsoft Lync Server Environment, the following limitations apply:

- SIP calls between HDX systems are unable to support dual-stream H.239 or BFCP content.
- The maximum available bandwidth for SIP calls is 2 Mbps.

Enabling RTV on the Lync Server

If you want to support high-quality RTV, you need to change the default video settings of your Lync Server. Lync Server 2013 is by default enabled for full HD 1080p only when you are using the Microsoft H.264 SVC codec. Because Polycom products currently leverage the RTV codec, you must change Lync Server 2013 video settings when using resolutions beyond VGA.

To change the default video settings for your Lync Server:

1. Access Lync PowerShell.
2. Change the video settings for your Lync Server. For example,

   ```
   Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M
   ```

3. Restart Lync Server to apply your changes.

Adding Calendar and Scheduling Features to Polycom HDX Systems

If you want to add a scheduling feature to your HDX system, you need to configure a conference room user account in Active Directory. To create a conference room user account, you can use a script, the Active Directory Users and Computers management console, or custom software. The following procedure shows you how to add a conference room user manually in the Active Directory Users and Computers management console.

If your deployment includes Polycom Calendaring for Outlook, you will need to perform further procedures outlined in Configuring Mailboxes for Room-based HDX or Group Series Systems.

Note: Set Passwords to Never Expire

If these conference room users have an expiring password, you will need to keep track of the users and passwords and make sure to update the accounts as required. Polycom recommends setting the passwords to never expire.

To add a conference room user to the Active Directory:

1. Go to **Start > Run** and open the Active Directory Users and Computers console by entering: dsa.msc

2 In the console tree, select **Users > New > User**.

3 In the New User wizard, enter the required conference room user information and click **Next**.

4 Set the user password. Polycom recommends that you also set the **Password never expires** option.

5 Click **Next** and **Finish**.

6 Repeat for each conference room that has a Polycom HDX system.

Enabling Conference Rooms for the Lync Server

After adding the conference room user accounts to Active Directory, you must enable and configure them for use with Lync Server.

Polycom recommends using Lync PowerShell to do this. For more information, see Windows PowerShell and Lync Server Management Tools.

To enable a conference room user for the Lync Server:

1 Access Lync PowerShell.

2 Enable a conference room user for Lync. For example,

```
Enable-CsUser -Identity Ken Myer -RegistrarPool lync.corp.local
-SipAddressType FirstNameLastName -SipDomain sipdomain.com
```

Enabling Conference Room Access for Remote and Federated Users

If you are supporting remote users and federated users, you need to configure the following on the Lync Server edge server:

- Enable support for external users for your organization
- Configure and assign one or more policies to support external user access

Once you have configured the Lync Server edge server, you can enable Lync Server to support remote and federated user access to a conference room.

To enable remote and federated user access to a conference room:

For detailed instructions on configuring support for external users in Lync Server, see Microsoft's Configuring Support for External User Access.

Adding Lync Contacts to Conference Room Local Address Book

To add Lync contacts to your Polycom system local address book, use the Polycom system user account and password to log on to a Lync client. You can then use the Lync client to add the contacts to the Polycom system account.

After adding contacts through the Lync client, contacts display in the HDX system the next time you log on.

For more information about displaying contacts in your HDX system, see Configuring Display Options for the HDX System Contact List.

Note: Configure a Maximum of 200 Contacts per HDX System User

Polycom recommends that you configure the Lync Server to allow no more than 200 contacts per user (the default setting is 250). The HDX system displays a maximum of 200 contacts per user.

Configuring Your Polycom HDX System for Lync Server

Before you begin configuring your Polycom HDX system for a Microsoft environment, you should ensure that the HDX system is installed according to standard installation procedures. Consult the Administrator's Guide for Polycom HDX Systems to identify the installation required for your HDX model. Configuring your HDX system for a Microsoft environment requires the following tasks:

- Installing the RTV Option Key on your HDX System
- Register Polycom HDX System with the Lync Server
- Understanding SIP Settings
- Configure the Polycom HDX System LAN Properties
- Configuring Display Options for the HDX System Contact List
- Configuring AES Encryption
- Supporting Lync-hosted Video Conferencing
- Supporting Microsoft Real-Time Video (RTV)

Installing the RTV Option Key on your HDX System

Without an RTV option key, your HDX system uses H.263 and is capable of CIF resolution for point-to-point Lync 2010 calling. RTV must be enabled for enabling Lync Server 2010 multi-party calling and/or higher quality video (up to 720p for point-to-point and VGA for multi-party). For Lync 2013 support the RTV option key is mandatory (for both point-to-point and multi-party calling scenarios).

Note: Register Polycom endpoints to Lync Server for RTV Video and Conferencing

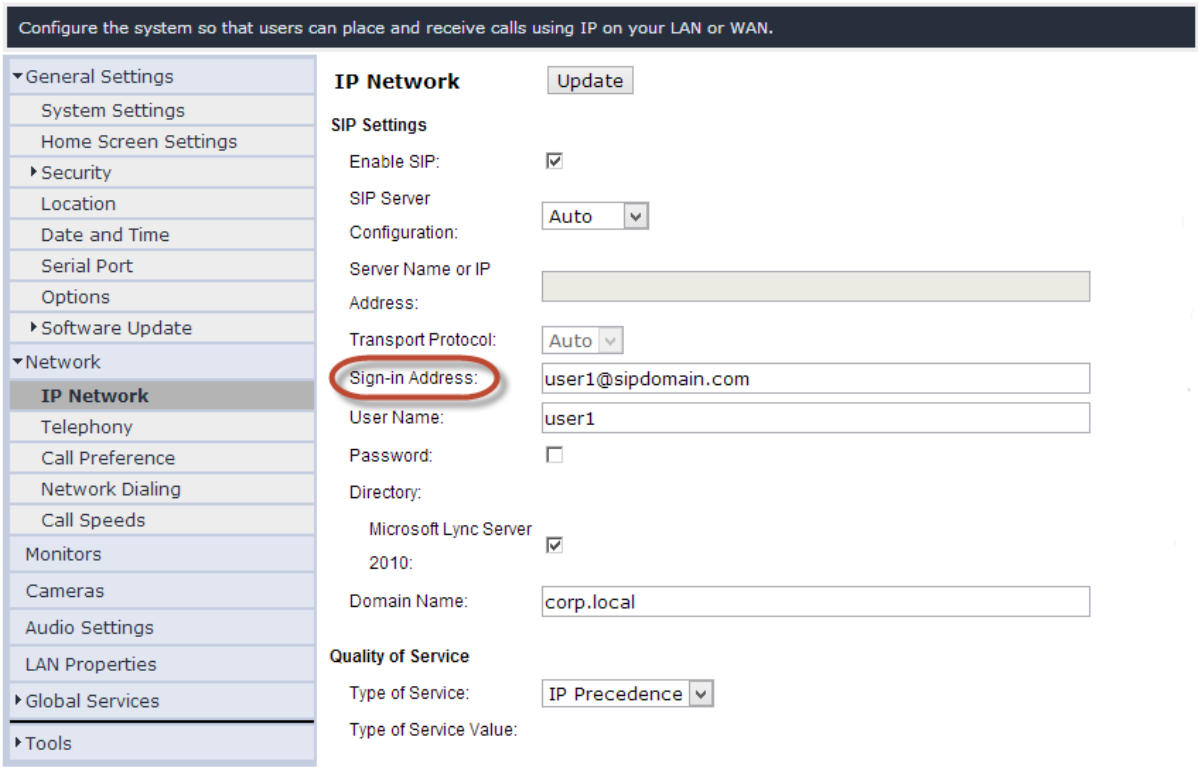
RTV video and Lync-hosted conferencing are only supported when you register Polycom endpoints to Lync Server.

Register Polycom HDX System with the Lync Server

When you register an HDX system with a Lync Server, the Polycom HDX system user can see a list of Lync 2010 contacts and whether contacts are online or offline. Contacts display in the directory and users can choose to display contacts on the home screen or call a contact. You can find descriptions of all SIP settings shown in this procedure in the following section Understanding SIP Settings. If you are using RTV, the options on the SIP Settings screen are different.

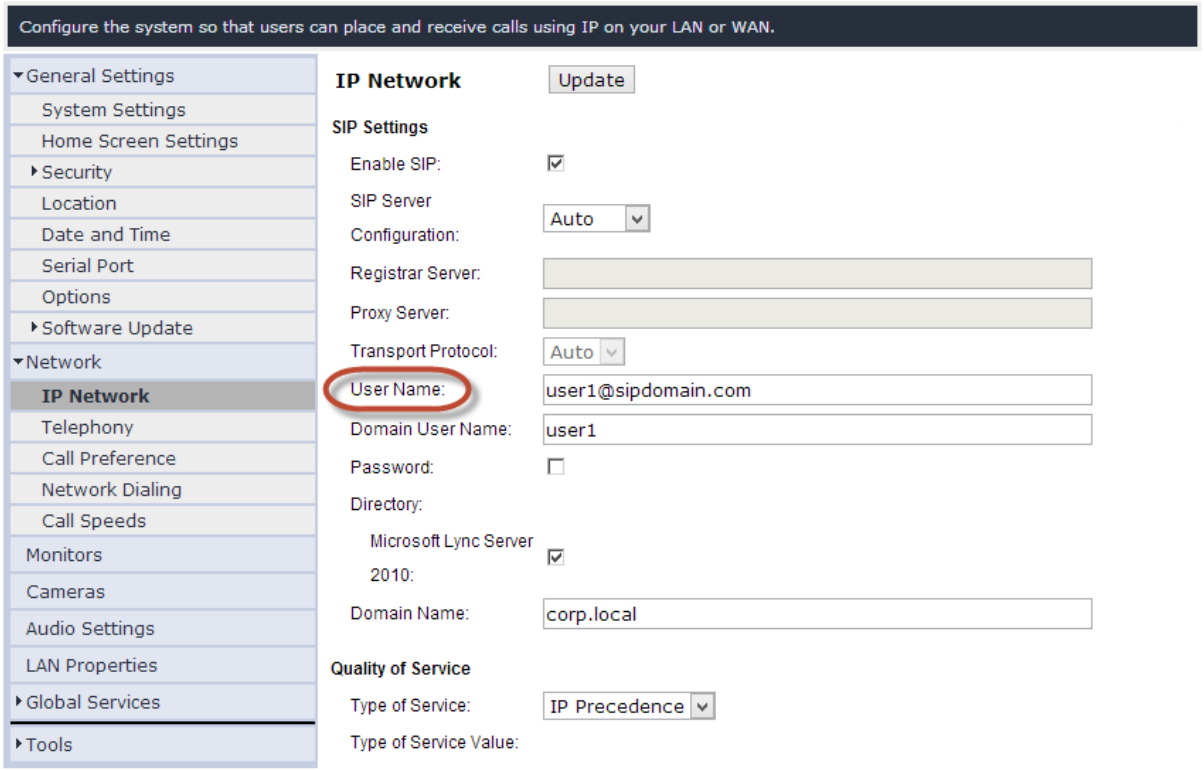
To configure an HDX system to register with Lync Server:

1. Open a browser window and in the Address field enter the Polycom system IP address or host name.
2. Go to **Admin Settings > Network > IP Network** and select **SIP**.
3. Configure the settings in the **SIP Settings** section of the **IP Network** screen. Note that the field Sign-in Address is labeled User Name when you install the RTV option key which is a requirement for Lync Server 2013. Screens illustrating both fields are shown next.



Note: Registering Polycom endpoints to Lync Server 2013 requires an RTV option key

An RTV option key is a requirement for integration with Lync Server 2013 as the H.263 codec has been deprecated. Support for Microsoft H.264 SVC is not planned for HDX series.



4 Click **Update**.

Once the Polycom HDX system registers with Lync Server, you can continue on to Configuring the Polycom HDX System LAN Properties.

Understanding SIP Settings

The following list describes all **SIP Settings on** the **IP** Network screen.

- **Enable SIP** Mark this check box to enable the HDX system to receive and make SIP calls.
- **SIP Server Configuration** Select Auto if your Microsoft Lync Server configuration is set up for automatic discovery, which requires you to correctly configure Lync SRV records. If Microsoft Lync Server is not configured for automatic discover, you need to select Specify.
- **Server Name or IP Address** If you selected Specify in the SIP Server Configuration field, you need to specify the IP address or DNS name of the SIP Registrar Server.
  - In a Lync Server environment, specify the DNS name of the Lync Server. The default port is 5061.

- If registering a remote HDX system with a Lync Server edge server, use the fully qualified domain name of the access edge server role. The port for the edge server role is usually 443 and must be entered explicitly.
- You can also enter the name of a Lync Director Server.

Polycom recommends using the DNS name. The format for entering the address and port is the following: <DNS_NAME>:<TCP_Port>:<TLS_Port>

Syntax Examples:

- To use the default port for the protocol you have selected: `lyncserver.corp.local`
- To specify a different TLS port (and use the default TCP port): `lyncserver.corp.local::443`

Note: If you have not installed the RTV option key, this setting is named Registrar Server.

- **Proxy Server** Specify the DNS name or IP address of the SIP Proxy Server. If you leave this field blank, the Registrar Server is used. If you selected Auto for your SIP Server Configuration and leave the Proxy Server field blank, no Proxy Server is used.

  By default for TCP, the SIP signaling is sent to port 5060 on the proxy server. By default for TLS, the SIP signaling is sent to port 5061 on the proxy server.

  The syntax used for this field is the same as for the Registrar Server field.

  Note: If you have installed the RTV option key, this setting is hidden. In Microsoft networks, the Proxy server and the Registrar server are always the same server, so only one server address field is required.

- **Transport Protocol** The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required.
  - **Auto** enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for Microsoft environments.
  - **TCP** provides reliable transport via TCP for SIP signaling.
  - **UDP** provides best-effort transport via UDP for SIP signaling.
  - **TLS** provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060. TLS is required when connecting to a Microsoft Lync Server.
- **Domain Name** Specifies the domain name for authentication with the LDAP server. You can leave this field blank when you use a UPN (username@domainname.com) in the User Name field (recommended).
- **Sign-in Address** Specify the system's SIP name. This is the SIP URI. Specify the user name for the conference room or user account created for the Polycom system.

  Note: If you have not installed the RTV option key, this setting is named User Address.

- **User Name** Specifies the name to use for authentication when registering with a SIP Registrar Server, for example, `jsmith@company.com`.

  Polycom supports the User Principal Name format (username@domain.com) as well as the legacy Microsoft DOMAIN\username format. If the SIP server requires authentication, this field and the password cannot be blank.

Note: If you have not installed the RTV option key, this setting is named Domain User Name.

- **Password** When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP Server.
- **Directory: Microsoft Lync Server** Specifies whether the SIP Registrar Server is a Lync Server. Enabling this setting activates integration features such as the Microsoft global directory and Lync contact sharing with presence.

Configuring the Polycom HDX System LAN Properties

To register with Lync Server, the Polycom HDX system must be able to access a DNS server whereby the name for the Lync Pool or Lync edge server has a valid domain name resolution.

To configure the Polycom system LAN properties:

1. Open a browser window and in the Address field enter the Polycom system IP address or host name.
2. Go to **Admin Settings > LAN Properties**.
3. If needed, enter the **Domain Name** for the domain to which the Polycom system belongs.
4. In the DNS Servers field enter the IP address for a DNS server that shares DNS zone information with the Lync Server. If you are registering a remote Polycom system, use a public DNS server that shares DNS zone information with the Lync Server Edge server.
5. Click **Update**.

Configuring Display Options for the HDX System Contact List

You can display your Microsoft contacts in your HDX system contact list.

To configure display options for contact list information:

1. Open a browser window and in the Address field enter the Polycom HDX system IP address or host name.
2. Go to **Admin Settings > Global Services > Directory Servers**.
3. In the Lync Server section of the Directory Servers page, configure these settings:
   - **Display Contacts** Specify whether to display your contacts on the contact list home screen and in the directory.
   - **Show My Offline Contacts** Specify whether to include offline contacts on the contact list home screen or in the directory.
4. Click **Update**.

Configuring AES Encryption

Polycom endpoint systems support AES media encryption. You need to set your system encryption settings to be compatible with your Lync Server settings.

Polycom recommends that you use automatic discovery, which requires you to ensure that each Polycom endpoint has compatible encryption settings and requires you to correctly configure Lync SRV records. If Microsoft Lync Server is not configured for automatic discovery, you need to select Specify.

Each codec within Polycom systems must have the same settings.

- If both Microsoft Lync and Polycom endpoints have encryption turned off, calls connect without encryption.
- If Microsoft Lync or a Polycom endpoint is set to require encryption and the other is not, calls fail to connect.

To configure AES encryption:

1. Open a browser window and in the Address field enter the Polycom system IP address or host name.
2. Go to **Admin Settings > General Settings > Security**.
3. In the AES Encryption drop-down menu, select **When Available** or **Required**.

Supporting Lync-hosted Video Conferencing and Lync Server 2013

Lync-hosted conferencing is supported only when Polycom endpoints are registered to Lync Server. To participate in Lync-hosted video conferences using a Polycom HDX system or to register the system to Lync Server 2013, you must install the RTV option key on the Polycom HDX system. If you want to use the call management features, you will need to pair your HDX system with a Polycom Touch Control.

When using Lync-hosted video conferencing, keep in mind the following points:

- When in a Lync-hosted call, the Polycom HDX system displays a Busy presence state. It rejects any inbound calls.
- When in a Lync-hosted call, other multipoint calling methods, such as internal multipoint hosting, RMX/DMA hosted conferencing, and Conference on Demand, are disabled.
- You need to install the RTV option key on your HDX system to support Lync-hosted conference calls and 720p high-definition video between an HDX system and a Lync client.
- You will need the RTV option key to enable support for Lync Server 2013

A Polycom Touch Control is required for the following HDX system functionality:

- View the participants in a Lync-hosted conference.
- Add participants to the Lync-hosted conference.
- Organize and initiate Lync-hosted conferences with Polycom HDX and Microsoft Lync clients and groups.

Using the Polycom Touch Control with Lync Conferencing

A Polycom HDX system must be paired with a Polycom Touch Control to initiate, view, add, and organize participants in a Lync-hosted video conference call.

To initiate a Lync-hosted call:

1. From the Call screen on the Polycom Touch Control, touch **Conference.**
2. Set up the call with the participants you want. You can add participants using any one of the following methods.
   a. Touch **Keypad** and enter the participant SIP addresses. Each time you enter a SIP address, touch **Add** to add it to the list of conference participants.
   b. Touch **Directory**, then touch the names you want to include in the list of participants. If you touch a group, the group opens and you can touch individual names to add them.
   c. Touch **Favorites**, then touch the names you want to include in the list of participants.
3. Touch **Join** when your list of participants is complete.

   The conference call is initiated.

   If you want to add another participant during a conference call, touch **Add Participant** and repeat any one of the methods in step 2. You do not need to put other participants on hold though there may be a brief audio or video pause.
4. To view all participants in a call, touch **Participants** from the call screen.

Understanding Roles in Lync-hosted Calls

Participants in a Lync-hosted call can have one of three roles depending on the level of user rights granted within the call. The privileges associated with each role are shown in Table 4-1 and 4-2. You set up these roles on Microsoft Lync Server, but if you are the conference organizer, you can change the roles of other participants using the Lync client.

The organizer of a Lync-hosted conference can choose to leave the conference by touching **Hang Up**. The other participants can continue with the call.

Table 5: Managing Participants in a Lync-hosted Call

Role	*Add a Participant*	*View Participants*
Organizer	Y	Y
Presenter	Y	Y
Attendee	N	Y

Table 6: Managing a Lync-hosted Call

Role	*Remove a Participant*	*End a Conference*	*Leave a Conference*	*Mute a Participant*	*Mute a Conference*	*Mute Self*
Organizer	Y	Y	Y	Y	Y	Y
Presenter	N	N	Y	Y	Y	Y
Attendee	N	N	Y	N	N	Y

Supporting Microsoft Real-Time Video (RTV)

Microsoft clients use the RTV protocol by default, which provides VGA and HD 720p video. Polycom supports high-quality RTV video among Microsoft components, Polycom ITP, Polycom HDX endpoints, and the Polycom RMX system. RTV video is only supported when Polycom endpoints are registered to Lync Server.

If you do not use RTV, Lync Server 2010 can provide H.263, CIF resolution, and does not support multi-party conference calls that are hosted on the Lync Server. The RTV protocol is mandatory on HDX to register with Lync Server 2013.

The following Polycom systems support the RTV protocol:

- Polycom HDX systems with the RTV option key.
- Polycom ITP systems.
- Polycom RMX system with the MPMx card

Call Quality Scenarios for RTV Video

The quality of video used depends on the capabilities of the endpoint you are using.

- RTV video requires a minimum call rate of 112 kbps. Calls below this rate connect with audio only.
- Multipoint calls initiated by a Microsoft Lync client are hosted on the Microsoft AVMCU. Polycom HDX systems must have the RTV key installed in order to connect. Multipoint calls initiated by an HDX system with the RTV key installed are also hosted on the Microsoft AVMCU.
- Multipoint calls initiated by a Group Series system that does not have the RTV key are hosted on the Group Series system's internal multipoint control unit (MCU) and do not use RTV. If a Lync 2010 client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Microsoft clients, the Polycom Group Series system uses RTV when the RTV option key is installed. If the Polycom Group Series system does not have the RTV option, the Lync 2010 client can use H.263/CIF. Point-to-point calls with a Lync 2013 require that the RTV option key be installed.
- When a Polycom HDX or Polycom ITP calls into an RMX conference that includes participants, the Polycom system can use H.264, while Lync uses RTV.

- Polycom ITP systems use RTV only on point-to-point calls with a Lync client and connect with only the primary codec.

5: Deploying Polycom® Immersive Telepresence (ITP) Systems

When deploying a Polycom® ITP system for use in a Microsoft® environment, you must complete tasks in Lync™ Server and the Polycom ITP system.

This section contains the following major topics:

Configuring Lync Server for use with a Polycom ITP System

When configuring your Microsoft environment, complete the following tasks:

Configuring Authentication in Lync Server

If you want to include an HDX system or ITP system in your Microsoft environment, NTLM must be enabled on your Microsoft Lync. By default, NTLM is enabled in Lync Server. If NTLM has been disabled for any reason, you need to enable it.

The Polycom HDX systems, Polycom ITP systems, and RMX systems support only NTLM authentication, and do not support Kerberos.

Configuring Microsoft Call Admission Control

Microsoft Call Admission Control policies are supported and enforced when your HDX system or ITP system is registered to a Microsoft Lync edge server.

When a Microsoft Call Admission Control policy is enforced in a Microsoft Lync Server environment, the following limitations apply:

- SIP calls between HDX systems or ITP systems are unable to support dual-stream people stream and content stream.
- The maximum available bandwidth for SIP calls is 2 Mbps.

Enabling High-Definition (HD) Video on the Lync Server

If your deployment includes support for high-quality RTV, you need to change the default video settings of your Lync Server. For example, Polycom HDX systems and RMX systems support video conferencing with high-definition video (720p RTV).

You must restart the Lync Server in order for these changes to take effect.

To change the default video settings for your Lync Server:

1. Access Lync PowerShell.
2. Change the video settings for your Lync Server. For example,
   `Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M`
3. Restart your Lync Server.

Creating and Enabling Conference Room User Accounts

You must create a conference room user account in Active Directory for each HDX codec in the ITP room. Once you have added the conference room user accounts to Active Directory, you must enable and configure them for use with the Lync Server. If needed, enable HDX users for remote access and federation.

Task 1: Add a Conference Room User for each Codec within your ITP System

You will need to use Active Directory to configure each ITP system in your deployment with a set of conference room user accounts. The names used for the user accounts must follow the ITP naming convention shown in Table 7.

When using the ITP naming convention, the Primary codec must have a name that indicates that it is an ITP system and how many codecs it has. The corresponding Secondary and any subsequent codecs' names must be derived from the Primary codec's name and indicate the codec number.

The examples in the following table show the names you would enter in the User logon name field of the New User wizard if the name of the Primary codec was `vineyard`.

Table 7: ITP Naming Convention

Codec	*Format*	*Example*
Primary codec	`<name>itp<number_of_codecs>@<domain>`	`vineyarditp4@abc.com`
Secondary codec	`~<name>itp<codec_number>@<domain>`	`~vineyarditp2@abc.com`

Codec	*Format*	*Example*
Right codec	`~<name>itp<codec_number>@<domain>`	`~vineyarditp3@abc.com`
Left codec	`~<name>itp<codec_number>@<domain>`	`~vineyarditp4@abc.com`

Each HDX system in your deployment must have a conference room user account in Active Directory. You can use a script, the Active Directory Users and Computers management console, or custom software to do this. The following procedure shows you how to manually add a conference room user in the Active Directory Users and Computers management console.

If your deployment includes Polycom Calendaring for Outlook, additional considerations apply when creating this user account. See Configuring Mailboxes for Room-based HDX or Group Series Systems.

Note: Set Passwords to Never Expire

If these conference room users have an expiring password, you will need to keep track of the users and passwords and make sure to update the accounts as required. Polycom recommends setting the passwords to never expire.

To add a conference room user to the Active Directory:

1. Go to **Start > Run** and open the Active Directory Users and Computers console by entering: `dsa.msc`.
2. In the console tree, select **Users > New > User**.
3. In the New User wizard, enter the required conference room user information and click **Next**.
4. Set the user password. Polycom recommends that you also set the **Password never expires** option.
5. Click **Next** and then **Finish**.
6. Repeat for each codec within your system.

Task 2: Enable Conference Rooms for the Lync Server

After adding the conference room user accounts to Active Directory, you must enable and configure them for use with Lync Server.

Polycom recommends using Lync PowerShell to do this. For more information, see Windows PowerShell and Lync Server Management Tools.

To enable a conference room user for the Lync Server:

1. Access Lync PowerShell.
2. Enable a conference room user for Lync. For example,

```
Enable-CsUser -Identity Ken Myer -RegistrarPool lync.corp.local
-SipAddressType FirstNameLastName -SipDomain sipdomain.com
```

You need to enable each conference room user account you created for your ITP system.

Hiding the Secondary Codecs in the Lync Directory

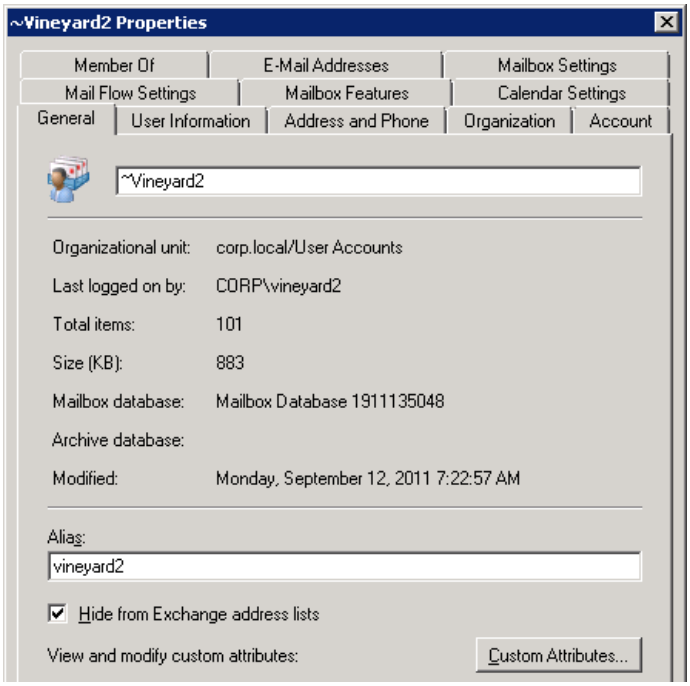
You can hide the secondary and subsequent codecs in the Lync directory based on one of the two following conditions:

- If the administrator created exchange mailboxes for all of the secondary codecs, you can hide the codecs using the Exchange Management Console.
- If the administrator did not create exchange mailboxes, you can hide the codecs using the Active Directory Service Interfaces Editor (ADSI Edit) tool on the Lync server.

Hiding the Secondary Codecs in the Directory Using the Exchange Management Console

To hide the secondary codecs in the directory using the Exchange Management Console:

1. On the Exchange server, open the **Exchange Management Console**.
2. Select **Recipient Configuration > Mailbox**.
3. Right-click the user you want to hide and select **Properties**.
4. On the General tab, select the **Hide from Exchange address lists** check box, shown next.



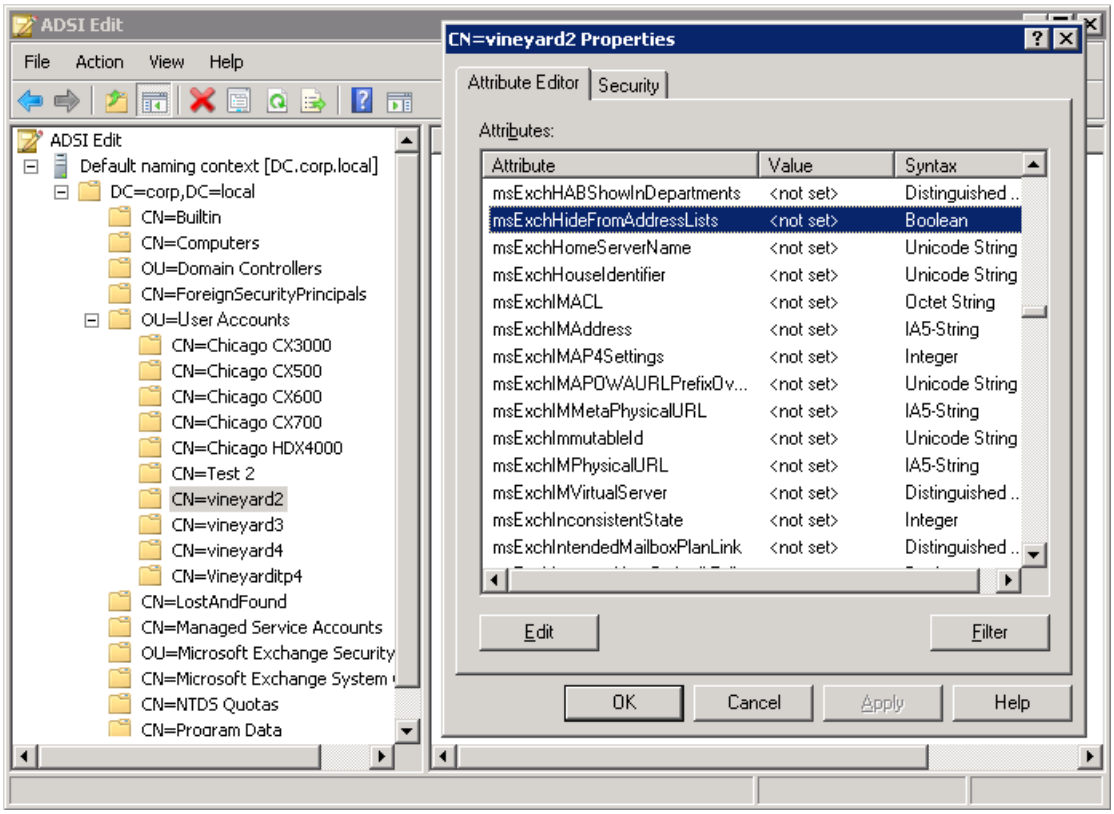
5. Click **OK**.

Hiding the Secondary Codecs in the Directory Using the ADSI Edit Tool

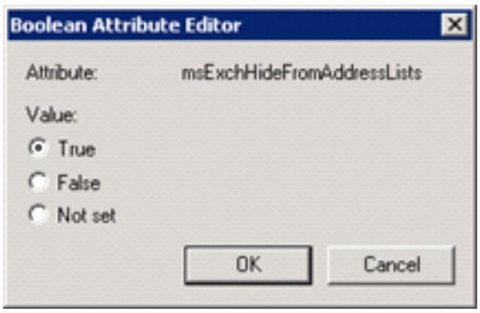
Active Directory Service Interfaces Editor (ASDI Edit) is a Lightweight Directory Access Protocol (LDAP) editor that you can use to manage objects and attributes in Active Directory. To install and obtain more information about ADSI, refer to Microsoft ADSI Edit.

To hide the secondary codecs in the directory using the ADSI Edit tool:

1. Open the ADSI Edit tool.
2. Expand the domain and navigate to the user that you want to hide.
3. Right-click the user and select **Properties.**
4. Select the attribute named **msExchHideFromAddressLists**, shown next, and click **Edit**.



5 On the Boolean Attribute Editor, select **True** in the Value field, shown next.



6 Click **OK**.

Enabling Conference Room Access for Remote and Federated Users

If you are supporting remote users and federated users, you need to configure the following on the Lync Server edge server:

- Enable support for external users for your organization
- Configure and assign one or more policies to support external user access

Once you have configured the Lync Server edge server, you can enable Lync Server to support remote and federated user access to a conference room.

To enable remote and federated user access to a conference room:

For detailed instructions on configuring support for external users in Lync Server 2010, see Microsoft Configuring Support for External User Access.

Configuring Your Polycom ITP System for Lync Server

After you have created and enabled the conference room user accounts and hidden the Secondary codecs in Active Directory, you must configure each Polycom HDX codec in the ITP room for the Microsoft environment.

Your Polycom ITP system should be installed according to standard installation procedures. See the ITP installation guide for your model of Polycom ITP system for information on how to install your system.

Then perform the following tasks:

- Registering All Codecs with the Lync Server
- Configuring the LAN Properties for each Codec
- Configuring Display Options for the ITP System Contact List
- Configuring AES Encryption

Registering All Codecs with the Lync Server

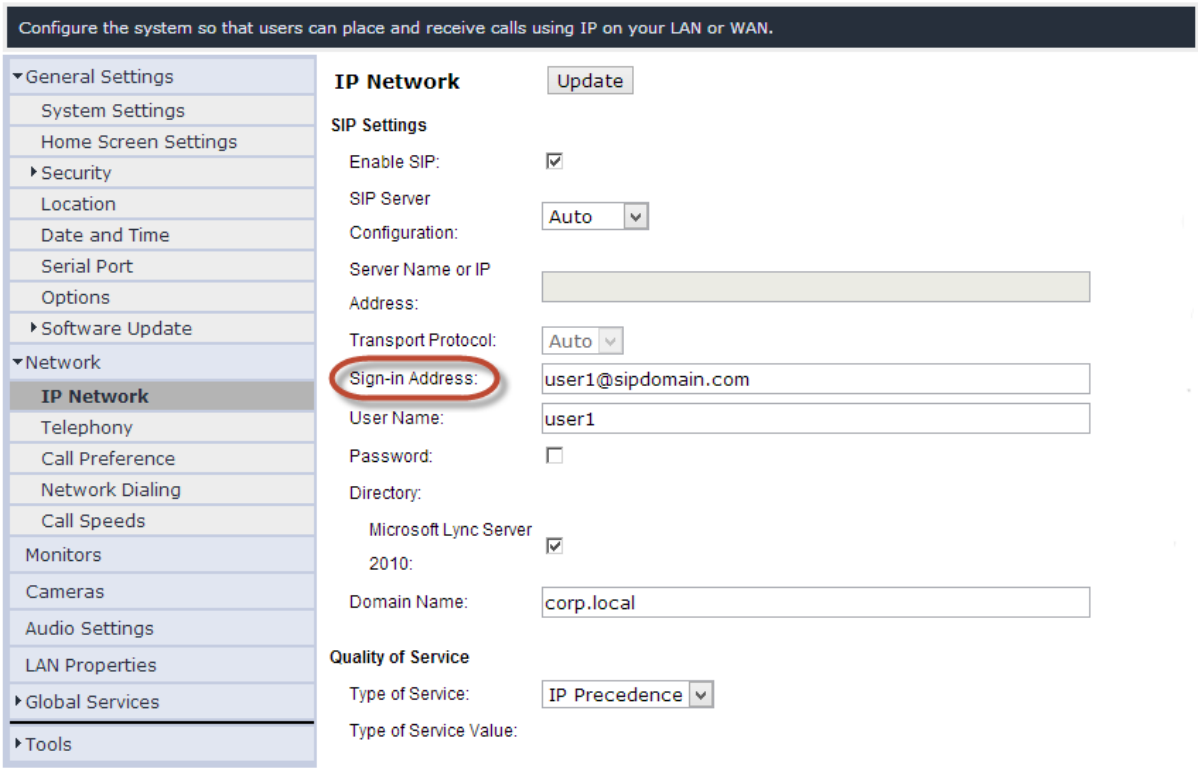
When an ITP system is registered with a Lync Server, the Polycom ITP system user can see a list of Lync 2010 contacts, see if the contacts are online, and call them without needing to know their addresses. Contacts appear in the directory.

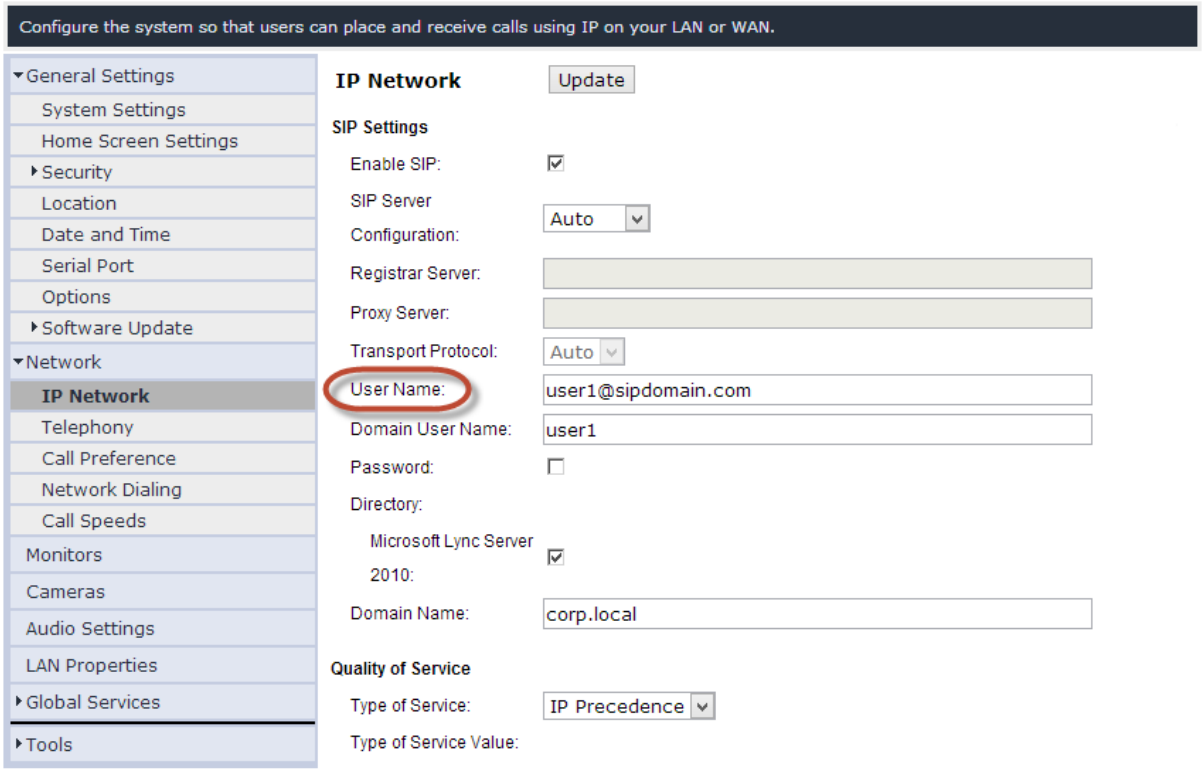
Note: Use the FQDN of the Access Edge Server Role

If registering a remote ITP system with a Lync Server edge server, use the fully qualified domain name of the access edge server role.

To configure an HDX system or ITP system codec to register with Lync Server:

1. Open a browser window and in the **Address** field enter the Polycom system IP address or host name.
2. Go to **Admin Settings > Network > IP Network** and select **SIP**.
3. Configure the settings in the **SIP Settings** section of the **IP Network** screen, as shown next with and without the RTV option key installed.





- **Enable SIP** Mark this check box to enable the HDX system to receive and make SIP calls.
- **SIP Server Configuration** Select Auto if your Microsoft Lync Server configuration is set up for automatic discovery. If Microsoft Lync Server is not configured for automatic discover, you need to select Specify.
- **Server Name or IP Address** If you selected **Specify** in the **SIP Server Configuration** field, you need to specify the IP address or DNS name of the SIP Registrar Server.
  - In a Lync Server environment, specify the DNS name of the Lync Server. The default port is `5061`.
  - If registering a remote HDX system with a Lync Server edge server, use the fully qualified domain name of the access edge server role. The port for the edge server role is usually 443 and must be entered explicitly.
  - You can also enter the name of a Lync Director Server.

    Polycom recommends using the DNS name. The format for entering the address and port is the following: `<DNS_NAME>:<TCP_Port>:<TLS_Port>`

    Syntax Examples:

    - To use the default port for the protocol you have selected: `lyncserver.corp.local`
    - To specify a different TLS port (and use the default TCP port): `lyncserver.corp.local::443`

    Note: If you have not installed the RTV option key, this setting is named **Registrar Server**.

- **Proxy Server** Specify the DNS name or IP address of the SIP Proxy Server. If you leave this field blank, the Registrar Server is used. If you selected Auto for your SIP Server Configuration and leave the Proxy Server field blank, no Proxy Server is used.

  By default for TCP, the SIP signaling is sent to port 5060 on the proxy server. By default for TLS, the SIP signaling is sent to port 5061 on the proxy server.

  The syntax used for this field is the same as for the Registrar Server field.

  Note: If you have installed the RTV option key, this setting is hidden. In Microsoft networks, the Proxy server and the Registrar server are always the same server, so only one server address field is required.

- **Transport Protocol** The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required.
  - **Auto** enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for Microsoft environments.
  - **TCP** provides reliable transport via TCP for SIP signaling.
  - **UDP** provides best-effort transport via UDP for SIP signaling.
  - **TLS** provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060. TLS is required when connecting to a Microsoft Lync server.

- **Domain Name** Specifies the domain name for authentication with the LDAP server. You can leave this field blank when you use a UPN (username@domainname.com) in the User Name field (recommended).

- **Sign-in Address** Specify the system's SIP name. This is the SIP URI. Specify the user name for the conference room or user account created for the Polycom system. Note: If you have not installed the RTV option key, this setting is named User Address.

- **User Name** Specifies the name to use for authentication when registering with a SIP Registrar Server—for example, jsmith@company.com.

  Polycom supports the User Principal Name format (username@domain.com) as well as the legacy Microsoft DOMAIN\username format.

  If the SIP server requires authentication, this field and the password cannot be blank.

  Note: If you have not installed the RTV option key, this setting is named Domain User Name.

- **Password** When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP Server.

- **Directory: Microsoft Lync Server** Specifies whether the SIP Registrar Server is a Lync Server. Enabling this setting activates integration features such as the Microsoft global directory and Lync 2010 contact sharing with presence.

4. Click **Update**.

5. Repeat these steps for each codec within your ITP room.

After you have registered each codec within your ITP room with Lync Server 2010, you can continue to Configuring the LAN Properties for each Codec.

Configuring the LAN Properties for each Codec

To register with Lync Server 2010, each codec in your ITP room must be accessible via a DNS server for Lync Server 2010 (or Lync Server 2010 edge server) and must have a valid domain name setting.

To configure the Polycom system LAN properties:

1. Open a browser window and in the Address field enter the Polycom system IP address or host name.
2. Go to **Admin Settings > LAN Properties**.
3. If needed, enter the Domain Name for the domain to which the Polycom ITP system belongs.
4. In the DNS Servers field enter the IP address for a DNS server that the Polycom system and Lync Server have in common.

   When registering a remote Polycom system, use a DNS server that the system has in common with the Lync Server edge server.
5. Click **Update**.

Configuring Display Options for the ITP System Contact List

You can display your Microsoft contacts in your ITP system contact list. You do this only on the Primary codec of your ITP system.

To configure the display options for contact list information:

1. Open a browser window and in the Address field enter the IP address or host name of the Primary codec.
2. Go to Admin **Settings > Global Services > Directory Servers**.
3. In the **Lync Server** section of the Directory Servers page, configure these settings:
   - **Display Contacts** Specify whether to display your contacts on the contact list home screen and in the directory.
   - **Show My Offline Contacts** Specify whether to include offline contacts on the contact list home screen or in the directory.
4. Click **Update**.

Configuring AES Encryption

Polycom endpoint systems support AES media encryption. You need to set your system encryption settings to be compatible with your Lync Server settings.

The Microsoft Lync Server requires encryption by default. If you want to keep this setting, you must ensure that each of the Polycom endpoints have compatible encryption settings.

Each codec within Polycom ITP systems must have the same settings.

- If both Microsoft Lync and Polycom endpoints have encryption turned off, calls connect without encryption.

- If Microsoft Lync or a Polycom endpoint is set to require encryption and the other is not, calls fail to connect.

To configure AES encryption:

1. Open a browser window and in the Address field enter the Polycom system IP address or host name.
2. Go to Admin **Settings > General Settings > Security**.
3. In the AES Encryption drop-down menu, select **When Available** or **Required**.

Lync-hosted Video Conferencing Not Supported

Polycom ITP systems cannot participate in multipoint calls hosted by a Lync AVMCU.

Supporting Real-Time Video (RTV)

Lync clients use the RTV protocol by default, which provides VGA and HD 720p video. Polycom supports high-quality RTV video among Microsoft components, Polycom ITP, Polycom HDX endpoints, and the Polycom RMX system. RTV video is only supported when Polycom endpoints are registered to Lync Server.

Without RTV support, Microsoft clients receive lesser quality video. If you do not use RTV with Lync 2010, Microsoft clients can use H.263 and CIF resolution, and do not support multi-party conference calls. You must enable RTV to integrate Polycom prodcuts with Lync Server 2013.

The following Polycom support the RTV protocol:

- Polycom HDX systems with the RTV option key.
- Polycom ITP systems.
- Polycom RMX system with the MPMx card

Call Quality Scenarios for RTV Video

The quality of video used depends on the capabilities of the endpoint you are using.

- RTV video requires a minimum call rate of 112 kbps. Calls below this rate connect with audio only.
- Multipoint calls initiated by a Microsoft Lync client are hosted on the Microsoft AVMCU. Polycom HDX systems must have the RTV key installed in order to connect. Multipoint calls initiated by an HDX system with the RTV key installed are also hosted on the Microsoft AVMCU.
- Multipoint calls initiated by an HDX system that does not have the RTV key are hosted on the HDX system's internal MCU and do not use RTV. If a Lync 2010 client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Lync 2010 clients, the Polycom HDX system uses RTV when the RTV option key is installed. If the Polycom HDX system does not have the RTV option, the call uses H.263/CIF.

- When a Polycom HDX or Polycom ITP calls into an RMX conference that includes Lync or Communicator participants, the Polycom system can use H.264, while Lync uses RTV.
- Polycom ITP systems use RTV only on point-to-point calls with a Lync client and connect with only the primary codec.

6: Deploying Polycom® RMX Systems

Integrating your Polycom® RMX system with Lync™ Server 2010 and 2013 includes adding a DNS entry, as well as creating and installing a security certificate. You also need to add a static route on the Lync Server for the RMX system to use. You should also enable Lync presence for the RMX system's virtual meeting rooms that you will use.

Note: Use a Lync Server Edge Server to Support Remote and Federated Users

If you need to support remote or federated users, your deployment must include a Lync Server 2010 or 2013 edge server, see Supporting Remote and Federated Users in Lync Server Environments.

This section outline the following tasks required to configure Polycom RMX system with Lync Server 2010.

You need to do the following:

1. Configuring Your Polycom RMX System for Lync Server
2. Configuring Lync Server for use with a Polycom RMX System
3. Enabling Microsoft Presence
4. Enabling Edge Server Integration with Your Polycom RMX System

Configuring Your Polycom RMX System for Lync Server

To begin, you need to configure your RMX system for use in a Lync Server environment. This includes setting up your RMX system for SIP, creating security certificates, and ensuring encryption settings.

Do the following:

- Set up the RMX System for Security and SIP
- Creating a Security Certificate for the Polycom RMX System
- Configuring Encryption for your Deployment
- Configuring Lync Server for use with a Polycom RMX System

Set up the RMX System for Security and SIP

Your RMX system must be accessible via DNS as well as be configured for SIP calls.

In this section, complete the following two tasks:

- Task 1: Configure the RMX IP Network Service
- Task 2: Add the RMX FQDN (SIP signaling IP address) in DNS

Task 1: Configure the RMX IP Network Service

You need to configure the IP network services to include SIP.

To configure the RMX IP Network Service:

1. Using the Web browser, connect to the RMX.
2. In the RMX Management pane, expand the **Rarely Used** list and click **IP Network Services**.
3. In the IP Network Services pane, double-click the **Default IP Service** entry.

   The Default IP Service - Networking IP dialog opens.
4. Make sure the IP Network Type is set to **H.323 & SIP** even though SIP will be the only call setup you use with the Lync Server.
5. Make sure that the correct parameters are defined for the Signaling Host IP Address, Media Card 1 IP Address, Media Card 2 IP Address (RMX 2000/4000 if necessary), Media Card 3 IP Address (RMX 4000 if necessary), Media Card 4 IP Address (RMX 4000 if necessary) and Subnet Mask.
6. Click **SIP Servers**.
7. In the SIP Server field, select **Specify**.
8. In the SIP Server Type field, select **Microsoft**.
9. Enter the IP address of the Lync Server 2010 and the Server Domain Name.
10. If not selected by default, change the Transport Type to **TLS**.

Task 2: Add the RMX FQDN (SIP signaling IP address) in DNS

To register with Lync Server 2010 or 2013, the Polycom RMX SIP signaling domain must be accessible via the DNS server used by the Lync Server. You need to configure a DNS A record for the FQDN of the RMX SIP signaling domain.

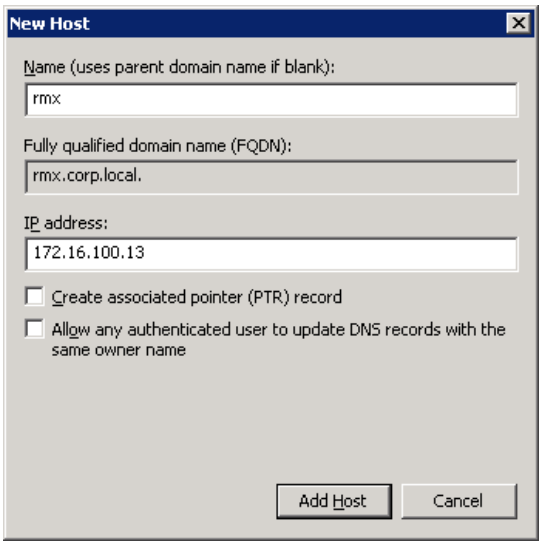
The RMX system and the Lync Server both need to resolve the RMX host record identically, regardless of the domain you select to store the DNS Host record.

To create a DNS record:

1. On the computer where the DNS manager is installed, open the **DNS Manager** and expand the **Forward Lookup Zone**.
2. Right-click the appropriate domain zone and select **New Host (A or AAAA).**

   The New Host dialog opens.

3 Define the new record. The following example defines a record using `rmx.corp.local` for the FQDN for the RMX SIP signaling domain and 172.16.100.13 as the IP address of the RMX signaling host.



4 Click **Add Host**.

5 Click **OK** to confirm and then click **Done**.

Creating a Security Certificate for the Polycom RMX System

You must install a security certificate on the RMX system so that Lync Server trusts it.

You can install a security certificate using one of the following two ways:

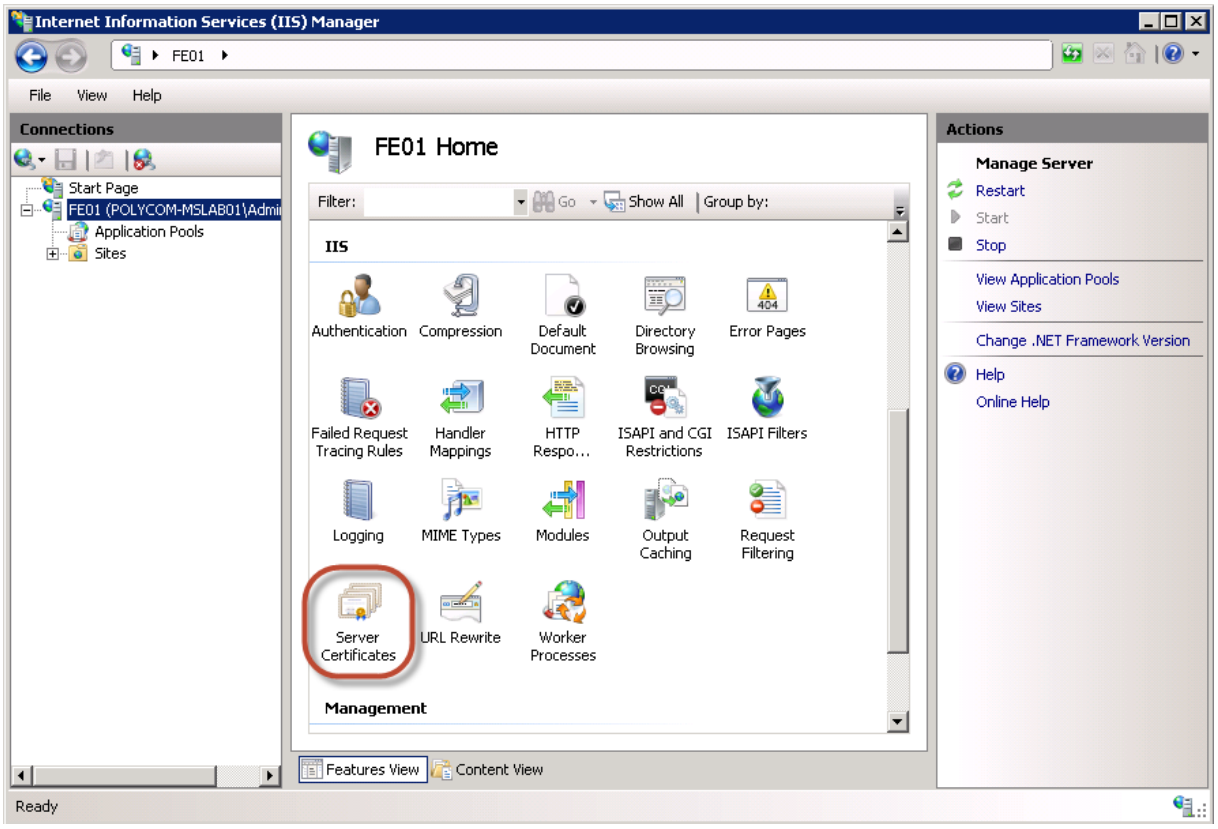
- Purchase and install a certificate from a commercial Trusted Root Certificate Authority (CA) such as VeriSign or Thawte. Use the procedures in the Polycom RMX system's documentation for Certificate Management to create a Certificate Signing Request and to install the certificate(s) received from the CA.
- Request and obtain a certificate from your enterprise CA. You can do this in two ways:
  - If you must submit certificate requests through the enterprise's CA team or group, use the procedures in the Polycom RMX System Administrator's Guide to create a Certificate Signing Request and to install the certificate(s) received from the CA team or group.
  - If your organization permits the submission of certificate requests directly to the enterprise's CA server, you can use the Internet Information Services (IIS) Manager on the Lync Server to download an export file of the certificate to your PC for later installation on the Polycom RMX system. This procedure is described next.

To request a security certificate for the Polycom RMX system using IIS Manager 7:

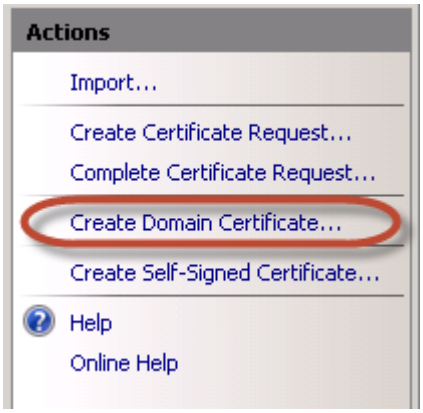
1 On the Lync Server, select **Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager (7.0)** to open IIS 7.

2 Under Connections, double-click the server name.

3 In the Features View, double-click **Server Certificates** under IIS, shown next.



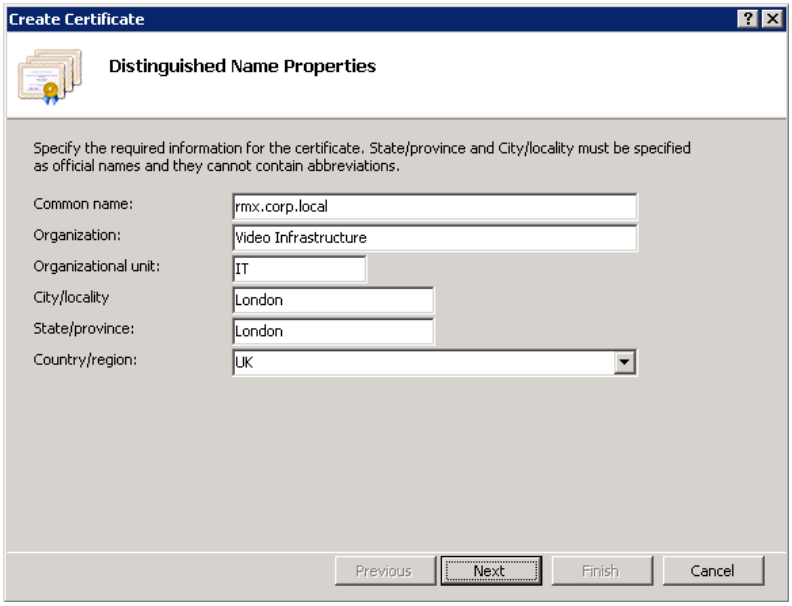
4 In the Actions pane on the far right, select the **Create Domain Certificate** action.



The Create Certificate wizard displays.

5 In the Distinguished Name Properties panel, shown next, complete all fields. Do not leave any fields blank.

- In the Common Name field, enter the FQDN of RMX SIP signaling interface.



6 Click **Next**.

7 In the Online Certification Authority panel, select a Certificate Authority from the list and enter a friendly name.

8 Click **Finish**.

Your certificate is created.

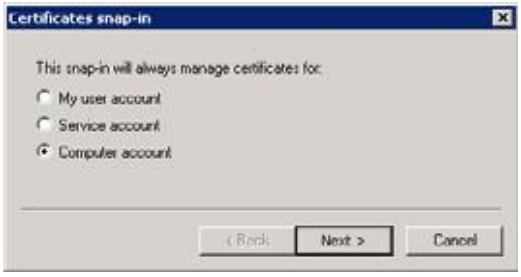
To use the Microsoft Management Console to export the created certificate:

1 Open Microsoft Management Console and add the Certificates snap-in.

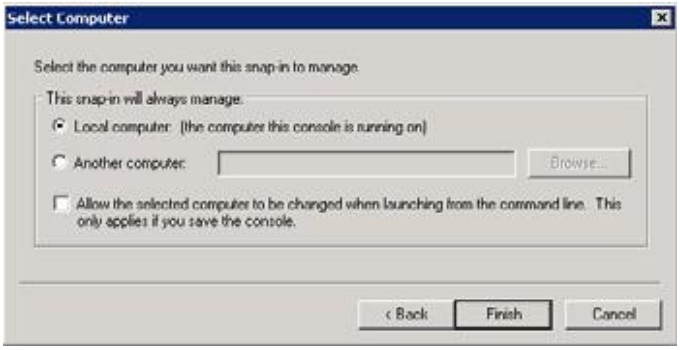
a Choose **File > Add/Remove Snap-in**.

b Select **Certificates** from the Available Snap-ins area and click **Add**.

c On the Certificates snap-in page, select **Computer Account** and click **Next**, as shown next.



d On the Select Computer page, select **Local Computer** and click **Finish**.



2 Click **OK**.

3 Browse to **Certificates (Local Computer) > Personal > Certificates**.

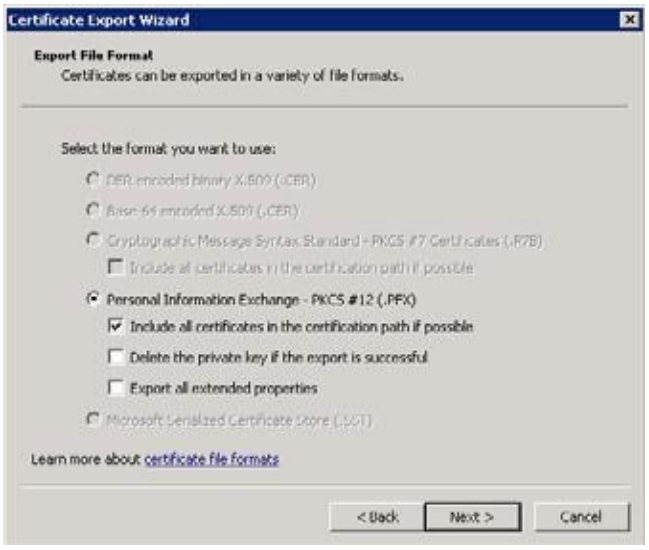
4 Right-click the created certificate and select **All Tasks** > **Export…** to view the Certificate Export wizard.

5 In the Certificate Export wizard, do the following:

a In the Export Private Key panel, select **Yes**, export the private key.

b Click **Next**.

c In the Export File Format panel, select **Include all certificates in the certification path if possible**.



d Click **Next**.

e In the Password panel, enter a password. This password cannot include special characters or numbers.

f Click **Next**.

6 In the File to Export panel, enter a path where you want to save the new file, for example, `c:\temp\rmxcert.pfx`.

Installing the certificate on your RMX system

Once the `*.pfx` file is on your PC, you can upload it to the Polycom RMX system and install it, using the procedures in the Polycom RMX system's documentation.

Configuring Encryption for your Deployment

The Microsoft Lync Server requires encryption by default. If you want to keep this setting, you must ensure that each of the Polycom endpoints have compatible encryption settings.

For example, legacy H.323 endpoints do not support encryption. If these endpoints need to participate in conferences with Lync clients, consider changing your Lync Server encryption settings to support encryption rather than require encryption.

For more information about configuring RMX system encryption for Microsoft Lync, see the section *Configuring Encryption Settings for Integration with Microsoft Lync Server 2010* in Chapter 8 of the Polycom RMX System Administrator's Guide.

As a best practice, Polycom recommends using Lync PowerShell commands to update the Lync Server encryption settings. For more details on using Lync PowerShell, see Microsoft Lync Server Management Shell.

To change the Lync Server encryption setting:

1 Use the following Lync PowerShell command to determine the current encryption setting for Lync Server 2010 or 2013:

```
Get-CsMediaConfiguration
Identity : Global
EnableQoS : False
EncryptionLevel : RequireEncryption
EnableSiren : False
MaxVideoRateAllowed : VGA600K
```

2 If you are deploying endpoints that don't support encryption, use the following Lync PowerShell command to change your encryption setting to support encryption:

```
set-CsMediaConfiguration -EncryptionLevel supportencryption
```

3 Verify your encryption settings:

```
Get-CsMediaConfiguration
Identity: Global
EnableQoS : False
EncryptionLevel: SupportEncryption
EnableSiren: False
MaxVideoRateAllowed: VGA600K
```

Configuring Lync Server for use with a Polycom RMX System

The Polycom® RealPresence® Collaboration Server 800s and RMX 1500/2000/4000 systems can host multiple video endpoints in a single conference and host multiple conferences simultaneously. To accommodate these features, you need to configure your RMX 800s/1500/2000/4000 system as a trusted application and not as a single user in Lync Server 2010.

Polycom recommends using Lync PowerShell commands to perform the following tasks. For detailed documentation for Lync PowerShell, see Microsoft Lync Server Management Shell.

Note: Using Domain Names

Within Microsoft environments, SIP domains often match the email domain.
As an alternative, you can use a separate SIP domain for your Lync Server. Be sure you use the correct domain names when configuring your SIP integration, especially if your primary SIP domain is different from the Active Directory domain for your Polycom devices. For information on , see Using Multiple Computer Application Pools.

Complete the following tasks to set the Lync routing for the Polycom RMX system:

- Task 1: Use Lync Topology Builder to Define Your Trusted Application Pool
- Task 2: Use Lync PowerShell to Create the Trusted Application
- Task 3: Use Lync PowerShell to Update the Topology
- Task 4: Use Lync PowerShell to Define a Static Route for the Polycom RMX System

Task 1: Use Lync Topology Builder to Define Your Trusted Application Pool

Creating a Trusted Application Pool simplifies the management of multiple Polycom devices. In this task, you'll create a trusted application pool and add one or more RMX systems as nodes under that pool name.

To define your trusted application pool:

1. Navigate to **Start > All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Topology Builder** to open the Lync Server Topology Builder.
2. When prompted, save a copy of the topology.
3. Expand the appropriate site container, right-click the **Trusted Application Servers** folder, and select **New Trusted Application Pool**.
4. In the Define the Trusted Application Pool FQDN, enter the name of the FQDN of the application pool you want to create, for example, `sipdomain.com`.

   As a best practice, Polycom recommends configuring this pool to be a multiple computer pool. See Using Multiple Computer Application Pools for more information.

5 Click **Next** to add computers to this pool.

6 In the Define the computers in this pool step, enter the FQDN for the RMX SIP signaling domain and click **Add**.

7 When finished adding computers, click **Next**.

8 Select the appropriate Next hop pool and click **Finish**.

9 Select **Action > Topology > Publish** to verify and publish your topology changes.

Task 2: Use Lync PowerShell to Create the Trusted Application

This step creates the trusted application using the Lync PowerShell.

To create the trusted application:

1 Navigate to **Start > All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Management Shell** to open the Lync PowerShell terminal.

2 Use the `New-CsTrustedApplication` command to set up a trusted application for the RMX system.

```
New-CsTrustedApplication -applicationId VideoProxy
-TrustedApplicationPoolFqdn sipdomain.com -port 5061
```

The parameters are defined as follows:

-ApplicationId A descriptive name for the application. Must be unique within your Lync deployment.

-trustedApplicationPoolFQDN The FQDN of the application pool. In our example, `sipdomain.com`.

-port The SIP port. The default port number for SIP is 5061.

For more information about the `New-CsTrustedApplication` command see Microsoft New-CsTrustedApplication.

Task 3: Use Lync PowerShell to Update the Topology

This step shows you how to use Lync PowerShell to update the topology.

To update the topology:

1 Navigate to **Start > All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Management Shell** to open the Lync PowerShell terminal.

2 Use the `Enable-CsTopology` command to update the Lync topology.

```
Enable-CsTopology
```

Task 4: Use Lync PowerShell to Define a Static Route for the Polycom RMX System

This step explains how to define a static route for your Polycom RMX system using Lync PowerShell. Route changes you make take effect immediately.

To define a static route:

1. Navigate to **Start > All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Management Shell** to open the Lync PowerShell terminal.
2. Use the `New-CsStaticRoute` command to set up a static route for the RMX system.

   ```
   $route = New-CsStaticRoute -TLSRoute -destination rmx.corp.local
   -port 5061 -matchuri sipdomain.com -usedefaultcertificate $true
   ```

   where `rmx.corp.local` is the FQDN of the RMX SIP signaling domain and `sipdomain.com` is the name of the Trusted Application Pool you created.

   For more information about the `New-CsStaticRoute` command see Microsoft New-CsStaticRoute.
3. Set the routing configuration. By configuring the static route, matched URI dialing is enabled.

   The following example sets the route to be global:

   ```
   Set-CsStaticRoutingConfiguration -identity global -route@{Add=$route}
   ```
4. **Optional**. To check that the commands were entered correctly in the PowerShell, enter:

   ```
   Get-CsStaticRoutingConfiguration
   ```

The Polycom RMX system is now set as a trusted host, and calls from a Lync client to a SIP address in the Polycom RMX system's domain will be routed through that system.

Enabling Microsoft Presence

You can register RMX system meeting rooms, entry queues, and SIP factories with your Lync Server so their presence is displayed in Lync clients. To do this you need to complete steps in both your Microsoft environment and in your RMX system.

You can register up to 100 RMX system meeting rooms with Lync.

Use the following steps to configure your RMX conferencing entities for Microsoft presence:

- Configuring your Microsoft Environment to Support RMX Room Presence
- Configure your RMX System for Microsoft Presence

Configuring your Microsoft Environment to Support RMX Room Presence

To register RMX conferencing entities, complete the following three tasks:

- Task 1: Create an Active Directory Account for the Conferencing Entity
- Task 2: Enable the Active Directory Account for Lync Server

Task 1: Create an Active Directory Account for the Conferencing Entity

The RMX system registers the conference room using a Lync-enabled Active Directory account.

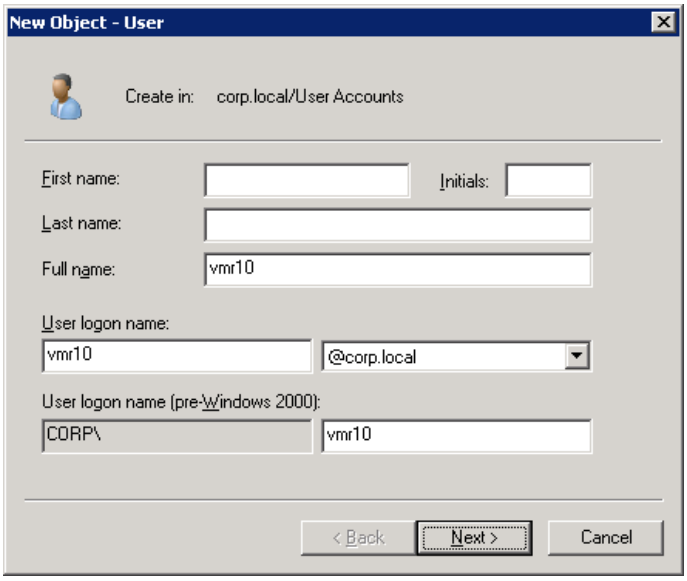
The SIP URI on the Lync-enabled account needs to be in the same SIP domain you defined as the Server Domain Name entry in the RMX SIP Servers configuration.

Note: Each RMX Conference Entity Must Have a Unique Active Directory account.

Each RMX conferencing entity must have a unique Active Directory account. You cannot, for example, re-use an Active Directory account that you create for federation.

To create an Active Directory account for the conferencing entity user:

1. Go to **Start > Run** and open the Active Directory Users and Computers console by entering: `dsa.msc`
2. In the console tree, select **Users > New > User**.
3. In the New User wizard, shown next, enter the required user information. Use lower case and/or numbers for all user values.



4. Click **Next**.
5. Set the user password. Polycom recommends that you set the **Password never expires** option.
6. Click **Next** and then **Finish**.
7. Repeat for each RMX conferencing entity.

After creating this account, you'll need to use the following account properties to register the room in the RMX system.

- The Active Directory account display name is used as the meeting room Display Name in the RMX system. This display name you see here is used as the room name in the contact list.
- The user portion of the Lync account's SIP URI is used as the Routing Name in the RMX system.

Task 2: Enable the Active Directory Account for Lync Server

You need to enable the Active Directory user for Lync Server. The new user must be enabled for the Lync Server and given a SIP URI.

To enable the Conferencing Entity User Account for Lync Server:

1. On the computer running the Lync Server, go to **Start >All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Control Panel**.

   The Windows Security dialog opens.

2. Enter the user name and password as configured in the Lync Server and click **OK**.

   The Microsoft Lync Server Control Panel dialog opens.

3. Click the **Users** tab.
4. In the User Search dialog, click **Enable Users**.

   The New Lync Server User dialog opens.

5. Click the **Add** button.

   The Select from Active Directory dialog opens.

6. Enter the conferencing entity user name you defined in the Active Directory, and then click the **Find** button.

   The user is listed in the Select From Active Directory dialog.

7. Select the listed user (conferencing entity user) and click **OK**.

   The selected user displays in the New Lync Server User dialog.

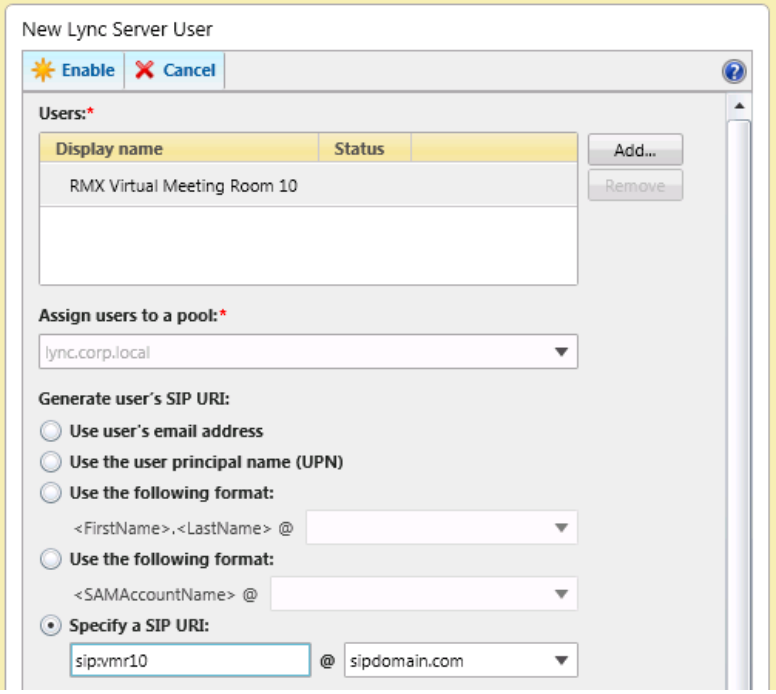
8. Assign the user to a pool and define a SIP URI using all lowercase or numbers.

   The user portion of SIP URI needs to match the Routing Name when you configure RMX meeting room. For example, for the address `sip:vmr10@sipdomain.com` use only the `vmr10` portion of the address.

Define the following parameters:

- In Assign users to a pool field, select the required pool.

- Under Generate user SIP URI, select the **Specify a SIP URI** option, as shown next.



9 Click **Enable**. The selected user appears as enabled in the User Search pane.

Task 3: Enable the RMX Account for Remote Access and Federation

Next, enable remote access if you are configuring users for remote or federated conference calls.

For detailed instructions on configuring support for external users in Lync Server, see Microsoft Configuring Support for External User Access.

For detailed information on setting up a federated environment, see Enabling Edge Server Integration with Your Polycom RMX System.

Configure your RMX System for Microsoft Presence

After you have completed the three tasks in Configuring your Microsoft Environment to Support RMX Room Presence, ensure that the conference entity has been enabled for SIP in the RMX system.

Complete the following two tasks:

- Task 1: Enabling SIP Registration in the Conference Profile
- Task 2: Create or Modify the RMX Conferencing Entity

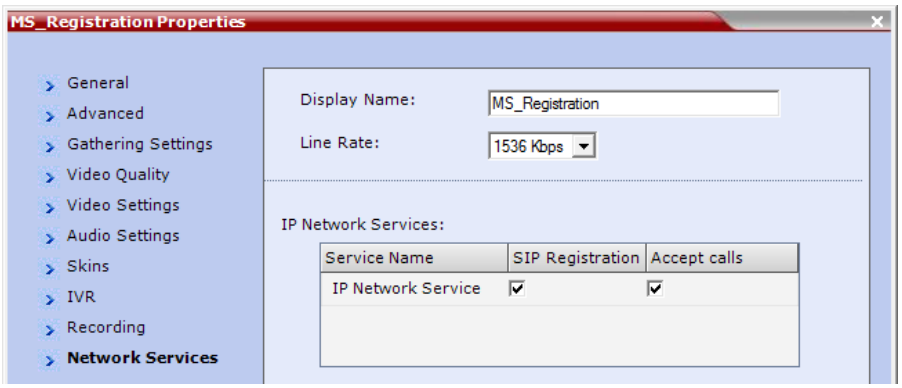
Task 1: Enabling SIP Registration in the Conference Profile

For each conference entity that requires a SIP registration, you must assign a conference profile and enable SIP in that conference profile. By default, SIP registration is disabled in conference profiles. A

meeting room cannot register until you assign it a conference profile and enable SIP in that conference profile.

To enable SIP registration for a conference profile:

1. Using the RMX management console, create a new profile or edit an existing profile.
2. In IP Network Services, check **SIP Registration**, shown next.



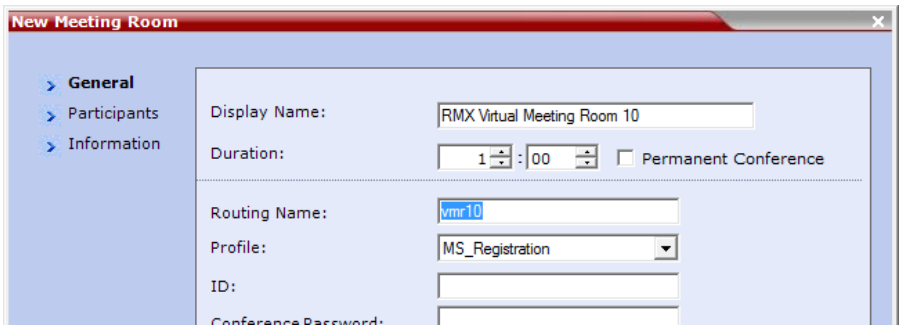
3. Click **OK**.

Task 2: Create or Modify the RMX Conferencing Entity

Next, create an RMX conferencing entity that matches the Active Directory account you created or modify an existing conference entity to match the Active Directory account.

To create an RMX conferencing entity:

1. Within the RMX management, got to **Frequently Used** > **Meeting Rooms** > **New Meeting Room**.
2. Use the Active Directory account display name as the meeting room **Display Name**.
   - Use the Lync account SIP URI as the **Routing Name**. For example, if the SIP URI is `sip:vmr10@sipdomain.com`, you will use only the `vmr10` portion of this address for the RMX configuration.



3. In the Profile drop-down menu, select the conference profile that you enabled for SIP registration.

For detailed instructions on working with RMX system meeting rooms and conferencing entities, see the Polycom RealPresence Collaboration Server (RMX) 800s/1500/2000/4000 Administrator's Guide.

Enabling Edge Server Integration with Your Polycom RMX System

Before enabling edge server integration with your RMX system, you must configure the RMX SIP signaling domain as a trusted application.

When your RMX system is configured with a Microsoft Edge Server, the following Microsoft features are available for your RMX system:

- ICE media support
- Federation
- External User Access
- Call Admission Control (Call Admission Control policies are managed on your Microsoft Lync Server.)

Note: Federation and CAC Require Lync Server or Edge Server Support

Federation and Call Admission Control are only supported for Polycom endpoints and devices registered to a Microsoft Lync Server.

Setting Up a Microsoft Edge Server for the Polycom RMX System

The Microsoft Edge Server enables you to set up remote and federated users. Before setting up an Edge Server, you must:

- Enable the firewall for UDP
- Provide the RMX system with a unique account in Active Directory and register it with the Lync Server edge server
- Set up a TLS connection
- Ensure that the RMX system SIP signaling domain has been allowed on the Lync Server edge server to which you are federating (if your deployment does not include a DMA system).

To set up a Microsoft Edge server with the Polycom RMX system and support Microsoft Call Admission Control policies, complete the following tasks:

- Task 1: Create an Active Directory Account for the RMX System
- Task 2: Enable the RMX User Account for Lync Server Edge Server
- Task 3: Enable the RMX Account for Remote Access and Federation
- Task 4: Configure the RMX System for Federated Dialing
- Task 5: Configure RMX System Flags for Federation and Microsoft Call Admission Control

Task 1: Create an Active Directory Account for the RMX System

You need to create an Active Directory account to register the RMX system with the Lync Server and to automatically synchronize with the Lync Server edge server.

You need to create a dedicated account and enable the account for the Lync Server. Because you are adding the RMX system as a trusted application, the password you enter is not important; however, you do need to enter a value for the password field, as shown in step 5. The RMX system is able to use its trusted application configuration to register with the Lync Server. Polycom recommends setting this password to never expire.

After creating this account, you'll need to use the user portion of the Active Directory account's SIP URI as the Server User Name when configuring the RMX system to register with the edge server.

To add the RMX user to the Active Directory:

1. Go to **Start > Run** and open the **Active Directory Users and Computers** console by entering: `dsa.msc`
2. In the console tree, select **Users > New > User**.
3. In the New User wizard, shown next, enter the user information.

4. Click **Next**.
5. Set the user password. Polycom recommends that you set the **Password never expires** option.
6. Click **Next** and **Finish**.

   The new User is added to the Active Directory Users list.

Task 2: Enable the RMX User Account for Lync Server Edge Server

After adding the RMX user account to Active Directory, you must enable it and configure it for use with Lync Server. This includes defining a SIP URI for the RMX user account. Enter the SIP URI in the Server User Name when you configure the RMX system for use with the edge server.

To enable the RMX User Account for Lync Server:

1. On the computer running the Lync Server, go to **Start >All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Control Panel**.

   The Windows Security window opens.

2. Enter your user name and password as configured in the Lync Server and click **OK**.

   The Microsoft Lync Server Control Panel window opens.

3. Click the **Users** tab.

4. In the User Search pane, click **Enable Users**.

   The New Lync Server User pane opens.

5. Click the **Add** button.

   The Select from Active Directory dialog opens.

6. Enter the conferencing entity user name you defined in the Active Directory, and click the **Find** button.

   The user you requested is listed in the Select From Active Directory dialog.

7. Select the user and click **OK**.

   The user displays in the New Lync Server User pane.

8. Assign the user to a pool and define a SIP URI using all lowercase or numbers. This SIP URI is used as the Server User Name for the RMX system when you configure it for use with the Lync Server edge server.

   Define the following parameters:

   - In Assign users to a pool field, select the required pool.
   - In the Generate user SIP URI field, select the **Specify a SIP URI** option and enter a SIP URI. For example, `rmx1edge`.

9. Click **Enable**.

   The user displays as enabled in the User Search pane.

Task 3: Enable the RMX Account for Remote Access and Federation

Before you configure the RMX system account for remote access and federation, ensure that you have configured a Lync Server edge server.

To enable the RMX account for external users, you need to do both the following:

- Enable support for external users for your organization.
- Configure and assign one or more policies to support external user access.

To configure the RMX account for federation and remote user access in Lync Server, see Microsoft Configuring Support for External User Access.

Task 4: Configure the RMX System for Federated Dialing

You need to configure the default IP Network Service for the RMX system to work with the Lync Server edge server as the SIP Server. In addition, you must define in the RMX ICE environment parameters the same RMX user you defined in the Active Directory.

Before completing Task 4, ensure that you have configured the RMX to work in a Microsoft environment. In particular, ensure that the `MS_ENVIRONMENT` flag is set to `YES`, the IP Network Service is set to work with Microsoft as the SIP Server, and the TLS certificate is installed. For a detailed description of these settings, see *Configuring the MCU for Federated (ICE) Dialing* in Appendix H of the Polycom RealPresence Collaboration Server (RMX) 800s/1500/2000/4000 Administrator's Guide.

To configure the RMX for Federated Dialing:

1. In the RMX Web browser, in the RMX Management pane, expand the **Rarely Used** list and click **IP Network Services**.
2. In the IP Network Services pane, double-click the **Default IP Network Service** entry.

   The Default IP Service - Networking IP dialog opens.
3. Click the **SIP Servers** tab.
4. In the SIP Server Type field, select **Microsoft**.
5. Make sure that the IP address of the Lync Server edge server is specified and the Server Domain Name is the same as defined in the Lync Server edge server and in the Management Network for the DNS.
6. Click the **SIP Advanced** tab, shown next.

7. In the Server User Name field, enter the SIP URI that you defined for the user you created in Active Directory, for example, `rmx1edge`.
8. In the ICE Environment field, select **MS** for Microsoft ICE implementation.
9. Click **OK**.

   The RMX system will register with the Lync Server edge server and enable automatic retrieval of the STUN server and Relay server parameters for ICE dialing.

Task 5: Configure RMX System Flags for Federation and Microsoft Call Admission Control

Enable the following system flags on the RMX system:

```
MS_ENVIRONMENT=YES
CAC_ENABLE=YES
PRESERVE_ICE_CHANNEL_IN_CASE_OF_LOCAL_MODE=YES
```

For more information about configuring RMX system flags, see the Polycom RealPresence Collaboration Server (RMX) 800s/1500/2000/4000 Administrator's Guide.

Monitoring the connection to the STUN and Relay Servers in the ICE environment

You can view ICE parameters in the Signaling Monitor - ICE Servers dialog.

To monitor the ICE connection:

1. In the RMX web browser, in the RMX Management pane, click **Signaling Monitor**.
2. In the Signaling Monitor pane, click the **IP Network Service** entry.
3. Click the **ICE Servers** tab.

   The system lists the ICE servers it is connected to, the connection status, and the status of the firewall detection in the RMX system.

7: Deploying Polycom® DMA Systems

When you incorporate a Polycom® DMA system in a Microsoft® Lync™ environment, you can do the following:

- Use the Polycom DMA system to manage conferences on your Polycom RMX systems
- Route outgoing calls from the DMA system to the Lync Server
- Route incoming calls from your Lync Server to endpoints and systems registered to the DMA system
- In a Lync Server 2013 environment, DMA systems only support meet on the bridge calling scenarios, this is achieved by SIP peering DMA with Lync 2013. This configuration, whilst supported in Lync 2010, is no longer supported with Lync Server 2013.

To deploy a Polycom DMA system in a Microsoft Lync environment, you need to configure Lync Server settings and your Polycom DMA system. This section contains two major steps that show you how to do both.

- Configuring Lync Server for Use with a DMA System
- Configuring Your Polycom DMA System for Lync Server

Configuring Lync Server for Use with a DMA System

Configuring Lync Server for use with a Polycom DMA system requires you to complete two tasks:

- Set the Routing for the Polycom DMA System
- Enable Federation in your Lync Environment

Set the Routing for the Polycom DMA System

This section shows you how to use Lync Server Management Shell commands to set routing for the Polycom DMA system, which enables the DMA system to receive Lync Server calls.

Complete the following four tasks to set the Lync routing for the Polycom DMA system:

- Task 1: Use Lync Topology Builder to Define Your Trusted Application Pool
- Task 2: Use Lync PowerShell to Set the Polycom DMA System as a Trusted Host with a Static Route
- Task 3: Use Lync PowerShell to Create the Trusted Application
- Task 4: Use Lync PowerShell to Update the Topology

Task 1: Use Lync Topology Builder to Define Your Trusted Application Pool

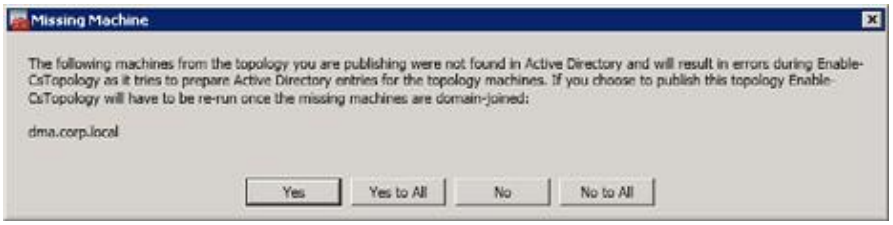
Creating a Trusted Application Pool simplifies the management of multiple Polycom devices. In this step, you'll create a trusted application pool and add one or more RMX systems as nodes under that pool name.

To define your trusted application pool:

1. Navigate to **Start > All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Topology Builder** to open the Lync Server Topology Builder.
2. When prompted, save a copy of the topology.
3. Expand the appropriate site container, right-click the **Trusted Application Servers** folder and select **New Trusted Application Pool...**
4. In the Define the Trusted Application Pool FQDN, enter the name of the FQDN of the application pool you want to create. For example, `sipdomain.com`.

   As a best practice, Polycom recommends configuring this pool to be a multiple computer pool. See Using Multiple Computer Application Pools for more information for more information.
5. Click **Next** to add computers to this pool.
6. In the Define the computers in this pool step, enter the FQDN for the DMA virtual host. For example, `dma.corp.local`.
7. Select the appropriate Next hop pool and click **Finish**.
8. Select **Action > Topology > Publish...** to verify and publish your topology changes.
9. Click **Yes** on the **Missing Machine** warning message.

   When it publishes the topology, the Lync Server attempts to match the FQDN of the Trusted Application Computer to an existing Computer object in Active Directory and typically displays a **Machine Missing** warning, as shown next.



10. Click **Yes** to accept the warning and complete the topology publishing wizard. Because the DMA system is not a Windows domain-joined host, it does not need to exist in Active Directory. There is no need to either domain-join the host or re-run this step as described in the warning message.

Task 2: Use Lync PowerShell to Set the Polycom DMA System as a Trusted Host with a Static Route

To set the DMA system as a trusted host with a static route:

1. Navigate to **Start > All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Management Shell** to open the Lync PowerShell terminal.
2. Use the `New-CsStaticRoute` command to set up a static route for the DMA system.

   ```
   $route = New-CsStaticRoute -TLSRoute -destination dma.corp.local-port 5061 -matchuri sipdomain.com -usedefaultcertificate $true
   ```

   where `dma.corp.local` is the FQDN of the DMA virtual host and `sipdomain.com` is the SIP routing domain (matched URI).

   For more information about the `New-CsStaticRoute` command see Microsoft New-CsStaticRoute.
3. Set the routing configuration. By configuring the static route, matched URI dialing is enabled.

The following example sets the route to be global:

```
Set-CsStaticRoutingConfiguration -identity global -route@{Add=$route}
```

4. **Optional.** To check that the commands were entered correctly in the PowerShell, enter:

   ```
   Get-CsStaticRoutingConfiguration
   ```

Task 3: Use Lync PowerShell to Create the Trusted Application

To create the trusted application:

1. Navigate to **Start > All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Management Shell** to open the Lync PowerShell terminal.
2. Use the `New-CsTrustedApplication` command to set up a trusted application for the DMA system.

   ```
   New-CsTrustedApplication -applicationId VideoProxy-trustedApplicationPoolFqdn sipdomain.com -port 5061
   ```

   The parameters are defined as follows:

   - **-ApplicationId** A descriptive name for the application. Must be unique within your Lync deployment.
   - **-trustedApplicationPoolFQDN** The FQDN of the application pool. In our example, `sipdomain.com`.
   - **-port** The SIP port. The default port number for SIP is 5061.

For more information about the `New-CsTrustedApplication` command see Microsoft New CsTrustedApplication.

Task 4: Use Lync PowerShell to Update the Topology

To update the topology:

1. Navigate to **Start > All Programs > Microsoft Lync Server (2010 or 2013) > Lync Server Management Shell** to open the Lync PowerShell terminal.
2. Use the `Enable-CsTopology` command to update the Lync topology.

   ```
   Enable-CsTopology
   ```

   The Polycom DMA system is now set as a trusted host, and calls from a Lync client to a SIP address in the Polycom DMA system's domain will be routed through that system.

Enable Federation in your Lync Environment

The second step in configuring Lync Server for Use with a DMA System is to enable federation. Note that federation is supported only for Polycom endpoints and devices registered to a Microsoft Lync Server or Microsoft Office Communications Edge Server.

Complete the following two tasks to enable federation in your Lync environment:

- Task 1: Configure the Microsoft Lync Edge Server
- Task 2: Ensure the Primary SIP Signaling Domain is Allowed

Task 1: Configure the Microsoft Lync Edge Server

You will need to include a Lync Server 2010 or 2013 edge server in your environment. Instructions on how to configure a Lync Server 2010 or 2013 edge server are available at Microsoft Deploying Edge Servers.

Microsoft provides a Lync Server Microsoft Lync Server 2010, Plannng Tool, and Microsoft Lync Server 2013, Planning Tool you can use to start planning your topology.

Microsoft Lync Edge Server Requirements

- TLS is required for both federated environments and for remote users.
- Polycom devices use the Access Edge Server IP address to register to a Lync Server edge server.

Task 2: Ensure the Primary SIP Signaling Domain is Allowed

When federating with another Lync Server environment, you need to ensure that the domain in the matchURI is allowed on the federated Lync Server edge server.

If you did not use the primary SIP domain as the matchURI, you must add both the primary SIP domain and any DMA and RMX SIP signalling domains to the allowed domain list on the federated Lync Server edge server.

Example Primary SIP Domain Scenarios

- Primary SIP domain was used as the matchURI when configuring the RMX/DMA static route.

  - If companyB wants to connect to calls managed by a DMA system or RMX system on companyA, companyB must add the following domains to its list of allowed SIP domains in the Lync Server edge server.
    - companyA's primary SIP domain
  - If companyA wants to connect to calls managed by a DMA system or RMX system on companyB, companyA must add the following domains to its list of allowed SIP domains on companyA's edge server.
    - companyB's primary SIP domain

- A domain other than the primary SIP domain was used as the matchURI when configuring the RMX/DMA static route.
  - If companyB wants to connect to calls managed by a DMA system or RMX system on companyA, companyB must add the following domains to its list of allowed SIP domains in the Lync Server edge server.
    - companyA's primary SIP domain
    - Each RMX/DMA SIP signaling domain
  - If companyA wants to connect to calls managed by a DMA system or RMX system on companyB, companyA must add the following domains to its list of allowed SIP domains on companyA's edge server.
    - companyB's primary SIP domain
    - Each RMX/DMA SIP signalling domain

You have successfully configured Lync Server for Use with a Polycom DMA System. The second major section of this chapter shows you how to configure your Polycom DMA system for Lync Server.

Configuring Your Polycom DMA System for Lync Server

This section outlines the following three major steps that configure a Polycom DMA system with Lync Server:

- Ensure DNS is Configured Properly
- Create a Security Certificate for the Polycom DMA 7000 System
- Configure a DMA System SIP Peer for Lync Server

Ensure DNS is Configured Properly

To configure DNS properly, ensure that:

- You have all the fully qualified domain names (FQDNs) of the system you are creating a certificate for. A two-node system has three domain names: one virtual and two physical; a single-node system has two domain names: one virtual and one physical.
- All of the FQDNs are in the primary DNS server of the environment and resolve correctly to the Polycom DMA system.

If the host information in DNS is wrong, the certificates will not work.

Create a Security Certificate for the Polycom DMA 7000 System

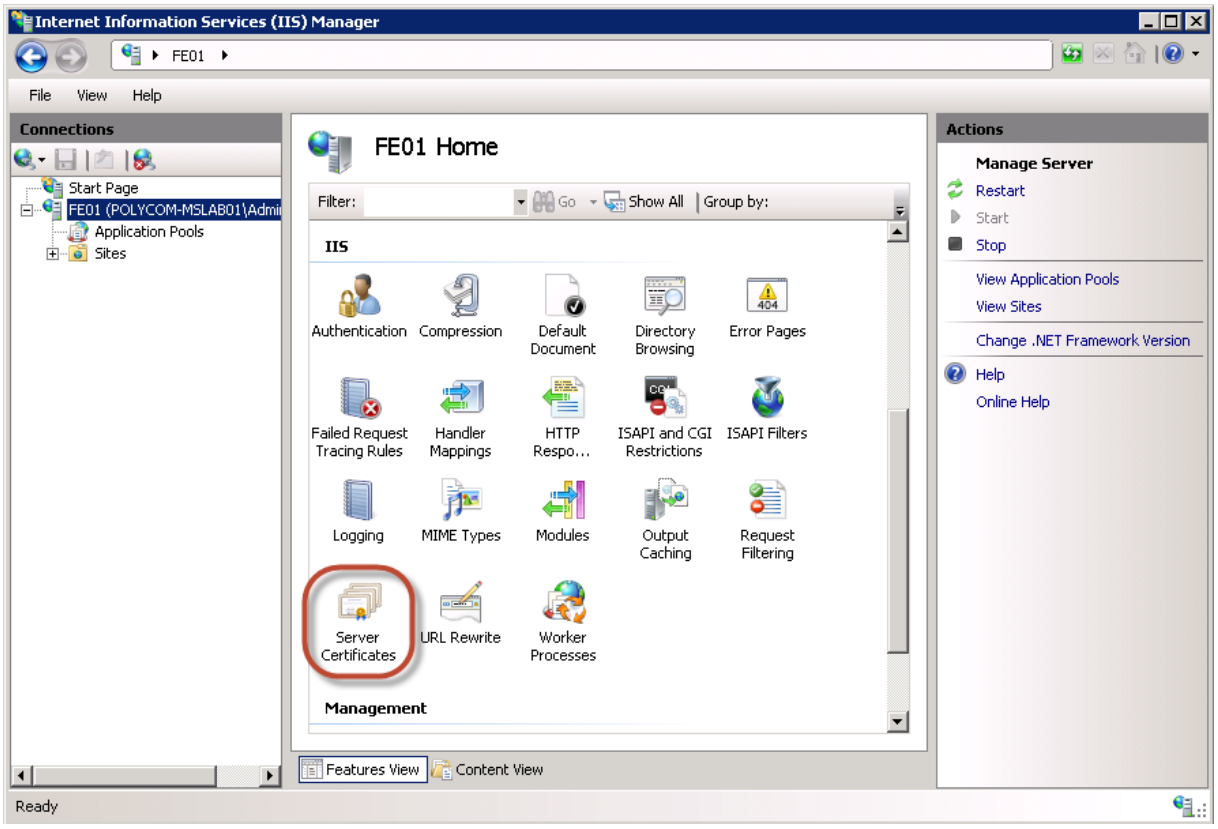
The second step in configuring a Polycom DMA system with Lync Server is to install a security certificate on the DMA system so that Lync Server trusts it. You can purchase or install a certificate or request and obtain a certificate from your enterprise CA, as explained next:

- You can purchase and install a certificate from a commercial Trusted Root Certificate Authority (CA) such as VeriSign or Thawte. Use the procedures in the Polycom DMA system's documentation for Certificate Management to create a Certificate Signing Request and to install the certificate(s) you receive from the CA.
- If you want to request and obtain a certificate from your enterprise CA, there are two ways you can do this:
  - If certificate requests must be submitted through the enterprise's CA team or group, use the procedures in the Polycom DMA system's online help for Certificate Management to create a Certificate Signing Request and to install the certificate(s) received from the CA team or group.
  - If your organization permits, you can use the Internet Information Services (IIS) Manager on the Lync Server to request certificates directly to the enterprise CA server. You can then use the IIS Manager to export the certificate to your PC and install it on the Polycom DMA system. The following procedures show you how to request, export, and install a certificate with the IIS Manager.

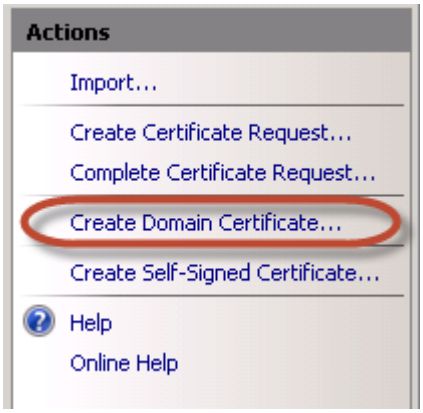
To request a security certificate for the Polycom DMA system using IIS Manager 7:

1. On the Lync Server, select **Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager (7.0)** to open IIS 7.
2. Under Connections, double-click the server name.

3 In the Features View, double-click **Server Certificates** under **IIS**, shown next.



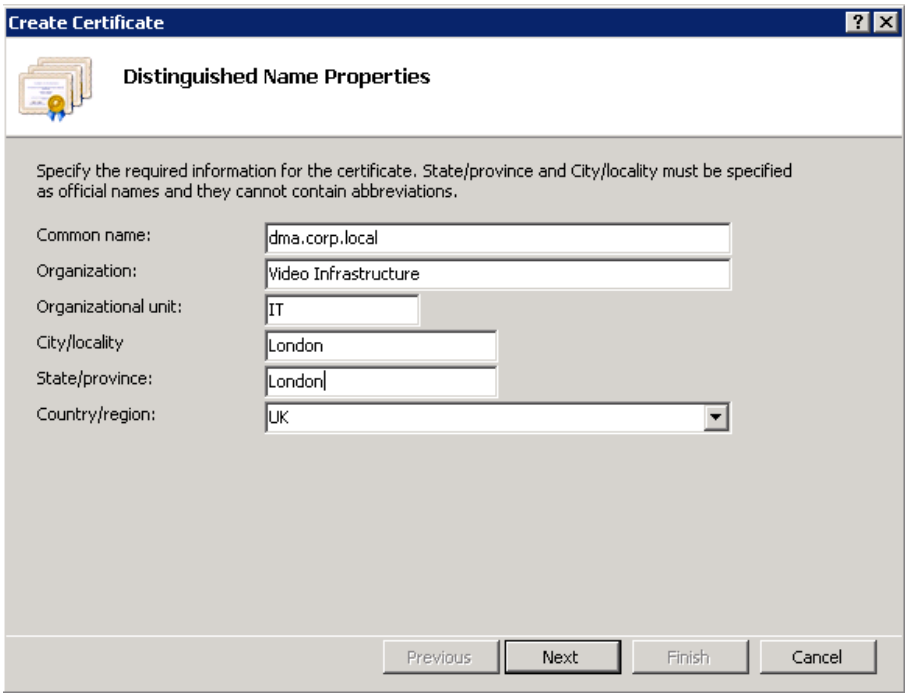
4 In the Actions pane (far right), select the **Create Domain Certificate**, shown next.



The **Create Certificate** wizard displays.

5 In the Distinguished Name Properties panel, shown next, complete all fields. Do not leave any fields blank. Do not leave any fields blank.

- In the **Common Name** field, enter the FQDN of DMA virtual host name. This name must match what is in the DNS.



6 Click **Next**.

7 In the Online Certification Authority panel, select a Certificate Authority from the list and enter a name that you can easily identify, for example, DMA certificate.

8 Click **Finish**.

You have created the certificate.

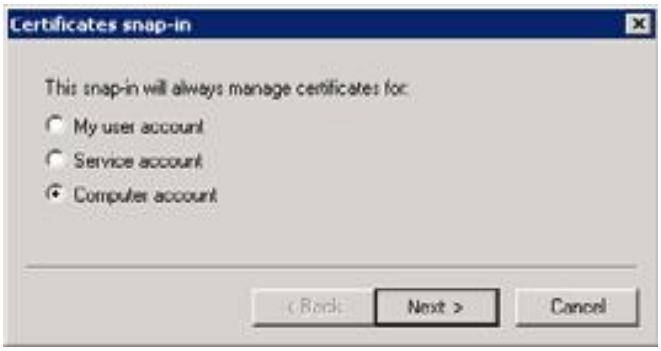
To use the Microsoft Management Console to export the created certificate:

1 Open Microsoft Management Console and add the Certificates snap-in, if it has not been added already.

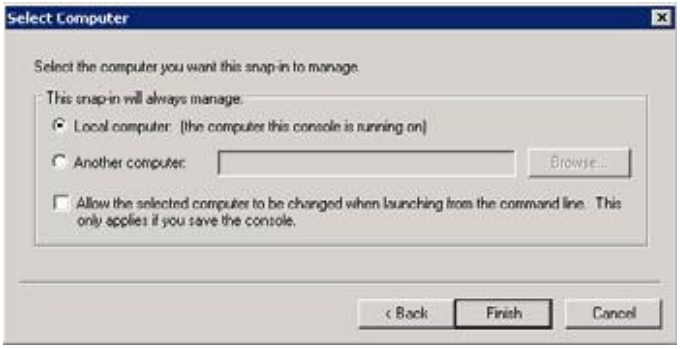
a Choose **File > Add/Remove Snap-in**.

b Select **Certificates** from the Available Snap-ins area and click **Add**.

c On the Certificates snap-in dialog, select **Computer Account** and click **Next**.



d On the Select Computer dialog, select **Local Computer**.



e Click **Finish**.

2 Click **OK**.

3 Browse to **Certificates (Local Computer) > Personal > Certificates**.

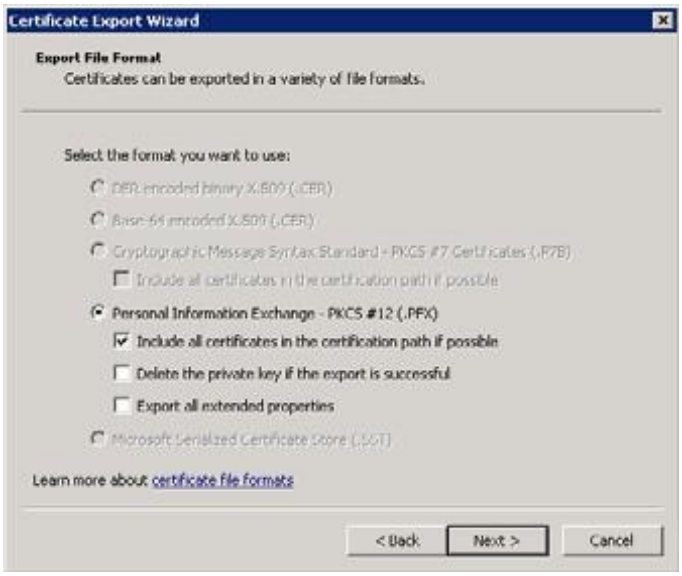
4 Right-click the created certificate and select **All Tasks > Export…** to view the Certificate Export wizard.

5 In **the Certificate Export** wizard, do the following:

a In the Export Private Key panel, select **Yes**, export the private key.

b Click **Next**.

c In the Export File Format panel, shown next, select the option **Include all certificates in the certification path if possible**.



d Click **Next**.

e In the Password panel, enter a simple password.

f Click **Next**.

6 In the File to Export panel, enter a path where you want to save the new file, for example, `c:\temp\dmacert.pfx`.

7 Once the `*.pfx` file is on your PC, you can upload it to the Polycom DMA system and install it, using the procedures in the Polycom DMA system's online help for Certificate Management.

Configure a DMA System SIP Peer for Lync Server

The third step in configuring a Polycom DMA system with Lync Server is to configure the Polycom DMA system as a SIP proxy and registrar.

When you use the DMA system as a SIP peer, you are able to host video calls between Polycom SIP endpoints that are registered with the DMA system and both Microsoft and Polycom SIP endpoints registered with the Lync Server.

Perform the following three tasks to configure a DMA system SIP peer for Lync Server:

- Task 1: Configure a SIP Peer in the DMA System
- Task 2: (Optional) Configure your DMA System to Route to Specific SIP Domains
- Task 3: Set up a Dial Rule for the Lync Server

Note: Microsoft Features Require Registration with a Microsoft Server

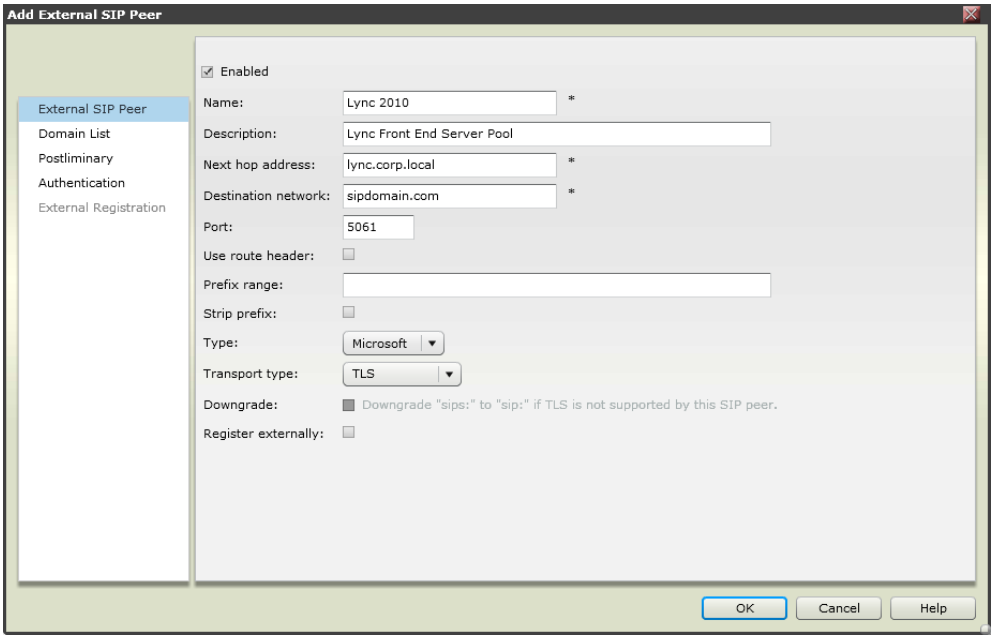
When Polycom endpoints are registered to the DMA system, Microsoft features such as federation, RTV video, Call Admission Control, and Lync-hosted conferences are not supported. These features are only supported when the Polycom endpoint is registered to a Lync Server.

Task 1: Configure a SIP Peer in the DMA System

In the DMA system, configure an external SIP peer for the Microsoft Lync Server. This allows SIP calls routed from the DMA system to reach devices registered to the Lync Server. Note that Lync 2013 does not support SIP peering.

To configure the DMA System as a SIP Peer for Lync Server calls:

1. Log into the DMA System.
2. Navigate to **Network > External SIP Peer**.
3. Select **External SIP Peer**.
4. In the Actions menu, click **Add**.
5. The Add External SIP Peer dialog displays, shown next.



6. Ensure that the **Enabled** is checked.
7. Type a name and description for the SIP Peer.
8. In the Next hop address field, type the FQDN address of the Microsoft Lync Server Front End Pool.
9. Enter the primary SIP domain for destination network.
10. In the Port field, enter the SIP port to use. Typically Lync is configured to use the SIP port of 5061.

11 Use route header should be left unchecked

12 Leave the Prefix range field blank.

You can use prefixes if your environment includes heterogeneous SIP domains that you need to differentiate between, for example, if your DMA system also routes calls to a BroadSoft environment. See the DMA system documentation for more information about using prefixes.

13 In the Type drop-down list, select **Microsoft**.

14 In the Transport Type drop-down list, select **TLS**.

15 Ensure **Register Externally** is not checked. Though some external SIP peers (Acme SBC, for example) require peer proxies to register with them, Microsoft Lync Server does not.

16 Click **OK**.

Outgoing SIP calls are now routed to endpoints registered to the Microsoft server.

Note: Using Dial Strings

Depending on your environment, you may need to ensure that the dial string sent to the Lync Server can be understood. Optionally, you can include a Postliminary Script that will ensure the string is compatible with Microsoft call extensions. For example, you can include a Postliminary script that strips the dial string of any prefix that isn't compatible with Lync. For more information, consult the Polycom DMA 7000 System Operations Guide.

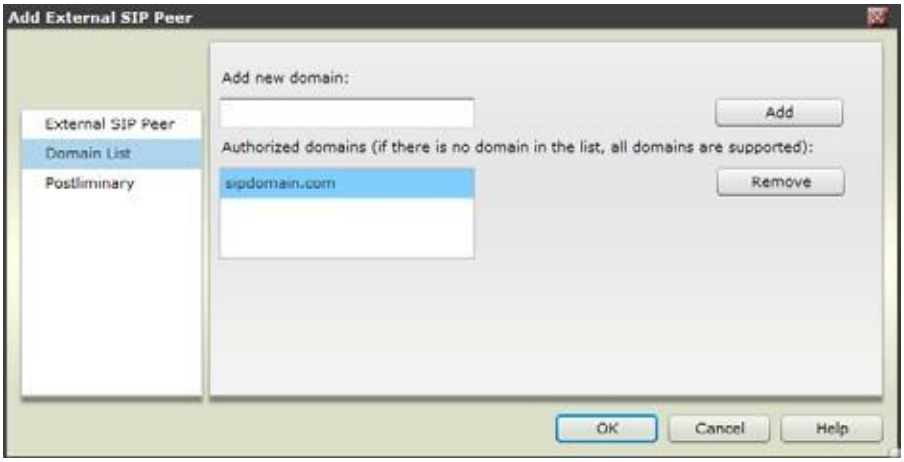
Task 2: (Optional) Configure your DMA System to Route to Specific SIP Domains

You have the option of configuring your DMA system to route to specific SIP domains that are associated with the SIP peer you created. When you configure specific SIP domains, DMA restricts call routing to the SIP domains you configure. If you do not configure specific SIP domains, the DMA system will route calls to any SIP domain.

To configure the DMA system to use a specific SIP Domain:

1 Navigate to **Network > External SIP Peer**.

2 Select **Domain List**, shown next.



3 Enter the name of the SIP domain and click **Add**. For example, `sipdomain.com`.

Task 3: Set up a Dial Rule for the Lync Server

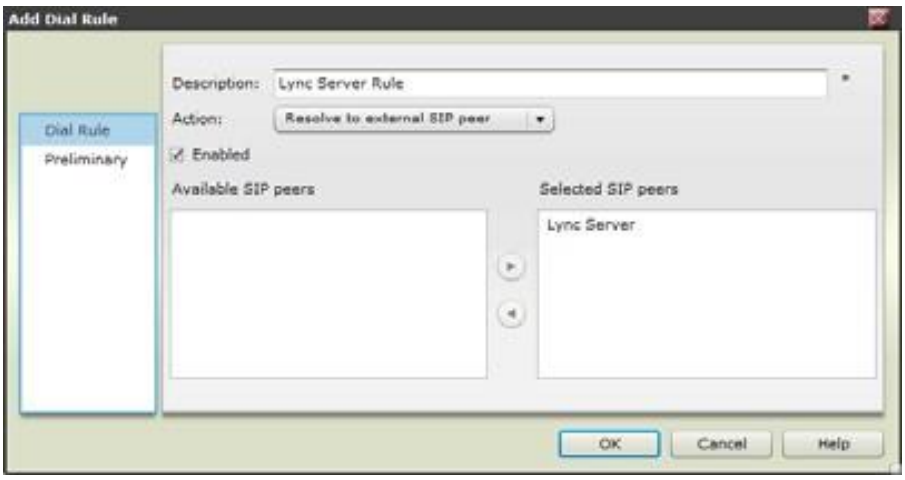
The third task in configuring a DMA system SIP peer is to set up a dial rule. As a best practice, the dial rule you use for the Lync Server should be last in your logical list of dial rules.

To set up a dial rule for Lync Server calls:

1 Select **Admin > Call Server > Dial Rules**.

2 Click **Add**.

3 The Add Dial Rule dialog displays, shown next.



4 In the Add Dial Rule dialog, enter a description for your dial rule.

5 In the Action drop-down menu, select **Resolve to external SIP peer**.

6 Check **Enabled**.

7 In the Available SIP Peers area, select **Lync Server** and move it to the Selected Peers area using the arrow.

8 Click **OK**.

8: Polycom® Calendaring for Outlook (PCO)

Polycom Calendaring for Outlook offers an integrated and enhanced calendaring experience for your video conferencing. This chapter details Polycom and Microsoft products that you can use with the Polycom Calendaring for Outlook feature, and shows you how to deploy Polycom® Calendaring for Outlook.

Polycom Solution Support Services

Polycom Implementation and Maintenance services provide support only for Polycom solution components. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services, and its certified Partners, to help customers successfully design, deploy, optimize and manage Polycom visual communication within their third-party UC environments. UC Professional Services for Microsoft Integration is mandatory for Polycom Calendaring for Outlook and Microsoft Lync Server integrations.

See Polycom Services or contact your local Polycom representative for more information.

This chapter includes the following sections:

- Polycom Products for Use with Calendaring for Outlook
- Microsoft Products for Use with Polycom Calendaring for Outlook
- Deploying Polycom Calendaring for Outlook

Polycom Products for Use with Calendaring for Outlook

Use the following table to identify Polycom products and versions you can use with the Calendaring for Outlook feature.

Table 8: Polycom Products for Use with Polycom Calendaring for Outlook

System	*Version*	*Description*
Polycom Calendaring for Outlook	1.4.0	Allows Outlook users to schedule meetings that include video, audio, and recording. Allows invitees to join a video-enabled meeting by clicking a link.

System	*Version*	*Description*
Polycom HDX systems	3.1.2	Monitor the Microsoft Exchange calendar of the configured account and display on-screen notifications of meetings. Users can join meetings via these notifications.
Polycom Group Series systems	4.1.1	Monitor the Microsoft Exchange calendar of the configured account and display on-screen notifications of meetings. Users can join meetings via these notifications.
Polycom RMX 1500 / 2000 / 4000 systems	8.1.7 MPMx card is required to support RTV. 1 GB controller board required for Edge Server support. Edge server support is not supported on MPMx cards prior	Monitors the Exchange mailbox for the Polycom Calendaring service and hosts Polycom Calendaring for Outlook conferences. Displays meeting information at the start of a meeting, called the Gathering Phase.
Polycom RMX 800s	8.1.7	Monitors the Exchange mailbox for the Polycom Calendaring service and hosts Polycom Calendaring for Outlook conferences. Displays meeting information at the start of a meeting, called the Gathering Phase.
Polycom CMA 4000 or 5000 system	6.2.0	Provisions Polycom HDX and Group Series systems for Polycom Calendaring for Outlook functionality and routes H.323 calls to the appropriate Polycom RMX or DMA system.
Polycom RealPresence Resource Manager	8.0	Provisions Polycom HDX and Group Series systems for Polycom Calendaring for Outlook functionality and routes H.323 calls to the appropriate Polycom RMX or DMA system.
Polycom CMA Desktop (PC and Mac)	5.2.4.29384	Allows users to join video-enabled meetings by clicking a link in a meeting invitation.

System	*Version*	*Description*
Polycom RealPresence Desktop	3.0.38914	Allows users to join video-enabled meetings by clicking a link in a meeting invitation.
Polycom DMA 7000 system	6.0.2	Monitors the Exchange mailbox for the Polycom Calendaring service and determines the appropriate Polycom RMX system to host a given Polycom Calendaring for Outlook conference.
Polycom RSS 4000 system	8.5	Via a connection from the Polycom RMX system, records Polycom Calendaring for Outlook conferences in H.323 format when selected in the Polycom Calendaring for Outlook add-in.

Microsoft Products for Use with Polycom Calendaring for Outlook

You can use the following table to identify the Microsoft products and versions that support Calendaring for Outlook.

Table 9: Microsoft Products for Use with Polycom Calendaring for Outlook

System	*Version*	*Description*
Microsoft Active Directory	2003, 2008, or 2012	Enables account logins and integrates with Microsoft Exchange. Note that Polycom products currently support only a single-forest Active Directory deployment.
Microsoft Exchange	2007 with SP2 2010, 2013	Hosts mailboxes and calendars. SP1 is required for the ‘Manage Full Access Permissions’ function. Exchange Web Services must be enabled.
Microsoft Outlook	2007 with SP2 2010, and 2013 (32 and 64bit)	
Microsoft Lync Server	2010 and 2013	Provides presence-based real-time instant messaging (IM), voice, video, and data communications.

System	*Version*	*Description*
Microsoft Lync Client	2010 and 2013	Can join video-enabled meetings by clicking a link in a meeting invitation.
DNS	N/A	Permits call routing to Polycom RMX and DMA systems and DMA subscription to Exchange for mail notifications.
Microsoft Office	2007, 2010 (32 bit only) and 2013 (32 and 64 bit)	Microsoft Outlook and Microsoft Word® are required for sending Polycom Calendaring for Outlook invitations. Users of older versions of Microsoft Office can receive invitations.

Deploying Polycom Calendaring for Outlook

This section shows you how to deploy the Polycom Calendaring for Outlook feature. You need to complete steps in each of the following sections to deploy Polycom Calendaring for Outlook:

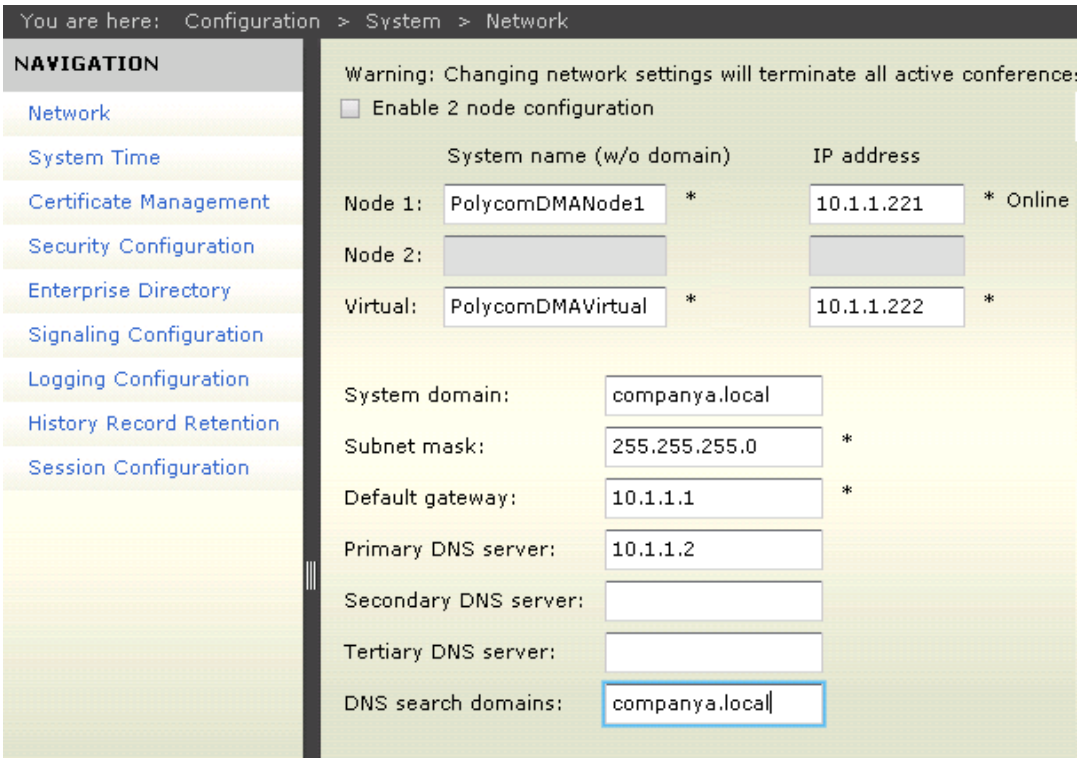
- Configuring DNS Entries for Polycom Devices
- Considerations for Remote Users
- Configuring the Polycom Infrastructure Mailbox and Devices
- Configuring Calendaring Settings for Polycom Video Media Center (VMC)
- Configuring Mailboxes for Room-based HDX or Group Series Systems
- Configure Mailboxes for Polycom HDX or Group Series Desktop Systems
- Configuring Polycom Group Series System Calendaring Settings
- Configuring Polycom HDX System Calendaring Settings
- (Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX or Group Series systems
- Configuring and Installing the Polycom Calendaring for Outlook add-In
- Testing Polycom Calendaring for Outlook Deployment

Configuring DNS Entries for Polycom Devices

To enable Polycom devices to work correctly with Calendaring for Outlook, you must set the devices to register to the exchange server for notifications. This registration will succeed only if the DNS server used by the exchange server has an A record that resolves the FQDN of the Polycom system's virtual IP address. The DNS server is usually the nearest Active Directory Domain Controller providing DNS services for an Exchange Server.

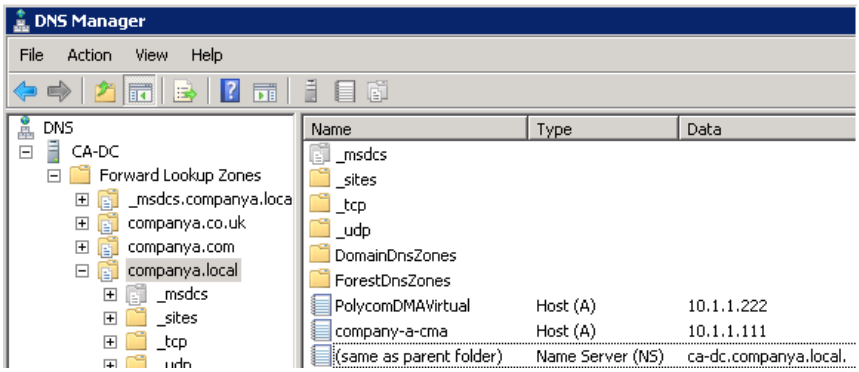
The following figure illustrates an example subscription. In this example, Company A's DMA has a virtual IP address `10.1.1.222` and virtual system name `PolycomDMAVirtual.companya.local`.

Figure 4: Example Subscription



In the following figure, the DNS server used by Company A's Exchange Server has an A record resolving `10.1.1.222` to `PolycomDMAVirtual.companya.local`.

Figure 5: A Record Resolving



If the Polycom DMA system does not receive confirmation of its subscription attempt from the exchange server, the Polycom DMA dashboard displays Subscription Pending as its exchange integration status. This is a normal status for up to two minutes while the first-time registration process occurs. If the Exchange Server is able to resolve the DMA system's virtual IP address as an FQDN but the DMA

system still displays the Subscription Pending status, there may be a firewall between DMA and the Exchange Server preventing connectivity.

Troubleshooting: DMA Displays Subscription Pending

If the Exchange Server is able to resolve the DMA system's virtual IP address as an FQDN but the DMA system still displays the Subscription Pending status, there may be a firewall between DMA and the Exchange Server preventing connectivity.

Considerations for Remote Users

Polycom Calendaring for Outlook supports H.323 clients, including Polycom HDX and Group Series systems, and Microsoft Lync clients.

You can support remote users under the following conditions:

- Polycom HDX or Group Series system H.323 calls are supported only if a remote Polycom HDX or Group Series user is registered to a Polycom VBP-S or VBP-S/T device that proxies the Polycom HDX or Group system's registration to a Polycom CMA system gatekeeper inside the enterprise network.
- Polycom HDX or Group Series system SIP calls are supported only if the Polycom HDX or Group Series is registered to Lync Server via a Lync Edge server.
- Polycom supports calendar access for remote users through the Outlook Anywhere feature. If you are using the Outlook Anywhere feature with a Polycom HDX or Group Series system, you will need to set up your HDX or Group Series with access to Exchange Web Services and in particular, to the `/ews/*` paths provided by the Exchange Client Access Server role. To enable access to the `/ews/*` paths see Microsoft Deploying Outlook Anywhere.
- For security purposes, only users on an organization's Exchange infrastructure can create video meetings requests. You can include federated and remote users in meeting invitations but federated and remote users cannot create meeting invitations.

Configuring the Polycom Infrastructure Mailbox and Devices

Polycom infrastructure devices including the Polycom RMX system, Polycom DMA system, and Polycom RSS can monitor a single exchange mailbox that is automatically scheduled into Polycom Calendaring for Outlook meetings.

Polycom infrastructure devices respond to meeting invitations sent to the exchange mailbox address and provide the meeting organizer with the option to ask recipients to accept or decline the meeting.

The Polycom infrastructure account will always receive meeting invitations except where there arises a conflict in Virtual Meeting Room (VMRs) numbers. However, VMR numbers are randomly generated by the Polycom Calendaring for Outlook add-in and are unlikely to conflict. If a conflict does occur, the meeting organizer must cancel the meeting and send a new invitation. For details on other scenarios that may cause the Polycom DMA system or Polycom RMX system to reject meeting invitations, see the administrator guide for your product on Polycom Support.

Note: VMR IDs are Randomly Generated

The Polycom Calendaring for Outlook add-in generates random Virtual Meeting Room (VMR) identification numbers for calendared conferences. You cannot set VMR meeting room IDs.

Complete the following four tasks to set up your Polycom Infrastructure Mailbox and Devices:

- Task 1: Create the Polycom Infrastructure Account and Mailbox
- Task 2: Configure Microsoft Exchange Integration with Polycom RMX Systems
- Task 3: Configure Calendaring Settings for Polycom DMA System
- Task 4: Configure Calendaring Settings for Polycom RSS System

Task 1: Create the Polycom Infrastructure Account and Mailbox

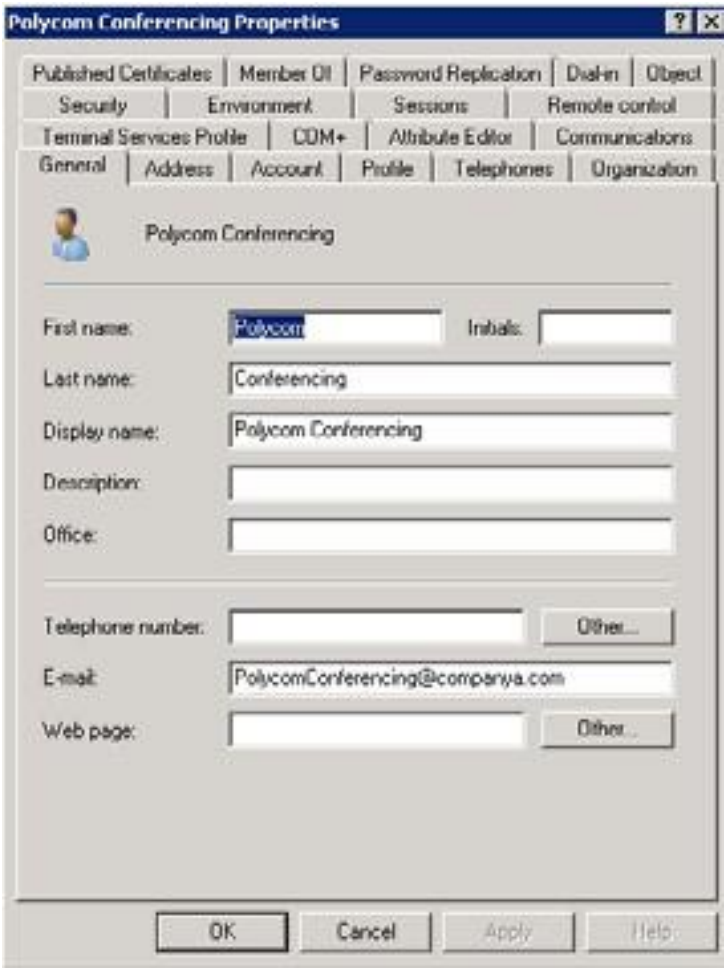
In Microsoft Exchange, create a standard user mailbox and account, using an email address such as `PolycomCalendaring@companya.com`. The Polycom infrastructure device will monitor this account.

Requirements:

- You must create a standard user mailbox dedicated for Polycom use and you cannot use a room mailbox for the Polycom infrastructure mailbox. A dedicated mailbox is also important because the Polycom DMA or RMX system deletes all messages from the Inbox when it checks this mailbox for meeting invitations.
- You must a password that is set to never expire. If you cannot use a permanent password at your organization, you will need to re-enter a temporary password for the account in each device when the temporary password expires or when the Active Directory administrator changes it.

The email account you create is automatically included in meetings created in Polycom Calendaring for Outlook. Figure 6 shows the General tab of the Polycom Calendaring Properties dialog. for an example of configuring a Polycom infrastructure mailbox.

Figure 6: Example Polycom Infrastructure Account



Task 2: Configure Microsoft Exchange Integration with Polycom RMX Systems

The Polycom RMX system's Gathering Phase feature is dependent on the Polycom RMX system's ability to directly access the Exchange server mailbox to determine information such as the name of a given meeting, and what attendees are participating.

To configure exchange integration with a Polycom RMX system:

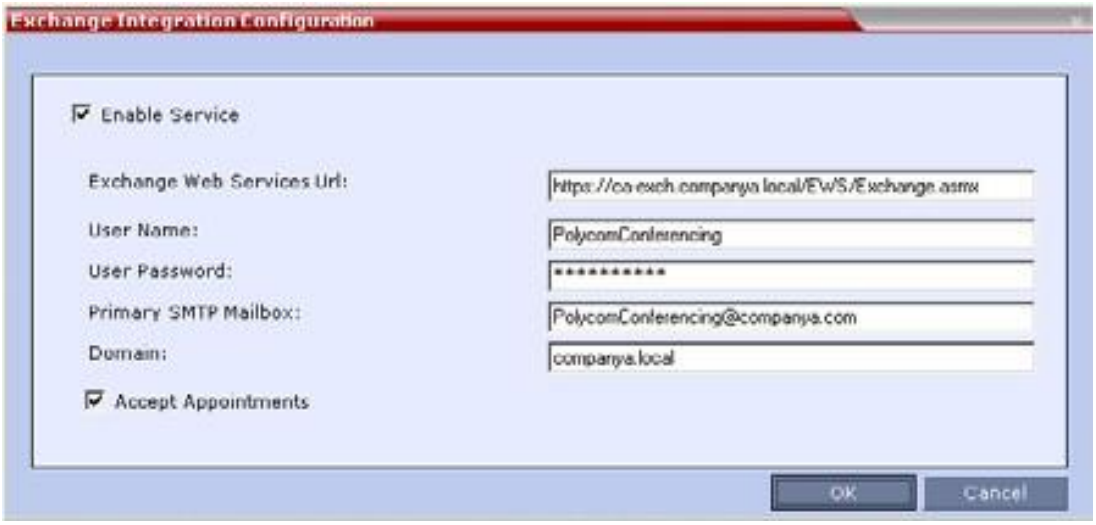
1. Using a web browser, connect to the RMX system.
2. Select **Setup > Exchange Integration Configuration**.

   The Exchange Integration Configuration dialog displays.
3. Mark the **Enable Service** check box.

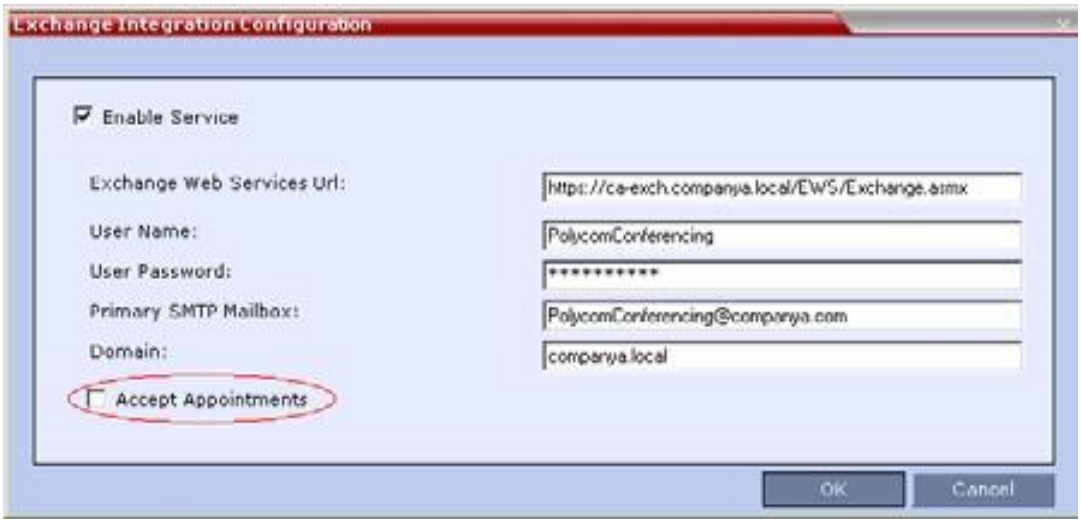
4 Complete the following fields:

- **Exchange Web Services URL** Specify the full URL path to the Exchange Web Service, including the `Exchange.asmx` service on the Exchange server.
- **Domain** This is the logon domain of the user in either NETBIOS or DNS name notation. For example, in an Active Directory domain named `COMPANYA.local` with a NETBIOS name of COMPANYA, enter either `COMPANYA.local` or `COMPANYA`.
- **User Name** This is the Active Directory account's user name. Do not include domain information.
- **Password** The password for the user account.
- **Primary SMTP Mailbox** This must match the **Primary SMTP Address** for the account in exchange and displays in the Mail field in Active Directory.

5 Check **Accept Appointments** if your deployment does not include a DMA system.



If your deployment includes a DMA system, do not check Accept Appointments. When a DMA system is present, it accepts appointments on behalf of the RMX.



User Tip: Using the MS Exchange Management Shell

You can use the Microsoft Exchange Management shell to list the full Exchange Web Services URL. Use a command prompt to navigate to the installation directory of the Microsoft Exchange Management shell, and enter:

```
get-WebServicesVirtualDirectory |fl
```

The Exchange Web Services URL is included in the returned list.

Task 3: Configure Calendaring Settings for Polycom DMA System

You need to subscribe the DMA system to the exchange server to receive notifications of meeting invitations. Be sure you have properly configured DNS before continuing, as shown in Configuring DNS Entries for Polycom Devices.

To configure calendar settings for the DMA system:

1. In a web browser, connect to the DMA system.

2 Go to **Configuration > Conference Setup > Calendaring Service**.

A dialog displays.

3 Check Enable Calendaring Service.

4 On the exchange server, specify the login credentials for the system. Use the Polycom infrastructure account you configured in the section Configuring the Polycom Infrastructure Mailbox and Devices.

5 If you have multiple exchange servers behind a load balancer, under **Accept Exchange notifications from these additional IP addresses**, add the IP address of each exchange server.

6 Click **Update**.

A dialog informs you that the configuration has been updated.

7 Click **OK**.

Task 4: Configure Calendaring Settings for Polycom RSS System

You need to set the Polycom RSS system to subscribe to the exchange server to receive notifications of meeting invitations for meetings that will be recorded.

To configure calendar settings for a Polycom RSS system:

1 In a web browser, connect to the RSS system.

2 Go to **System Config > Service Setting > Calendar Configuration**.

A dialog displays.

3 Check Enable Calendar Integration.

4 Complete all available fields.

Configuring Calendaring Settings for Polycom Video Media Center (VMC)

The Polycom VMC 1000 manages live and video-on-demand (VOD) content created by Polycom RSS devices and manages video streams created by other devices. The Polycom VMC 1000 provides scalable and reliable content access by means of streaming protocols to end users across the entire enterprise.

To configure calendaring settings for a Polycom VMC, you will need to:

- Configure each Polycom RSS device for use with the VMC.
- Set up the VMC for Exchange Discovery.

For complete instructions, see the Polycom Video Media Center (VMC) 1000 Administrator Guide.

Configuring Mailboxes for Room-based HDX or Group Series Systems

Configure an exchange room mailbox and an Active Directory account for each room-based HDX or Group Series within your deployment.

Note: Configure Additional Settings for HDX or Group Series

In many environments, user and room accounts are likely to be fully configured. If you are configuring room mailboxes and accounts for a room-based HDX or Group Series, you will need to configure additional settings.

You can use the same workflows to schedule a video-enabled Polycom Calendaring for Outlook conference as you do when reserving a conference room for a meeting without video. You schedule the room mailbox, also referred to as the resource mailbox, in the Outlook client when users wish to hold a meeting in the room. Once you have configured the mailbox, the Polycom HDX or Group Series system monitors the exchange calendar for scheduled meetings.

You can configure a mailbox for an HDX or Group Series room systems in three ways:

- Enable the mailbox with a user account

  The enabled Active Directory account can be used to authenticate with Polycom CMA system for automatic provisioning if you use the same credentials for the Provisioning Service and Calendaring Service configurations in the Polycom HDX or Group Series system.
- Associate a single mailbox with a service account. You will need to enable the account for full manage permissions.
- Associate multiple mailboxes with a service account and enable the account for full manage permissions.

  By default, room mailboxes are linked to disabled Active Directory accounts.

Each of these configuration options has an associated set of available features. The features associated with each configuration option are shown in the following table.

Table 10: Features Available with the HDX or Group Series Room Mailbox

	An Exchange mailbox with enabled user account	*An Exchange mailbox with a disabled user account managed by a service account*	*Multiple Exchange mailboxes with disabled user accounts managed by a single service account*
Polycom Calendaring for Outlook	✓	✓	✓
Presence	✓ (either with CMA or Lync Server)	✓ (only with Lync Server)	✘
CMA Automatic Provisioning	✓	✘	✘
CMA Softupdate	✓	✘	✘

Note: HDX and Group Series Supports a Single Directory

Polycom HDX or Group Series systems can have a single directory. If your environment includes a Polycom CMA system and Lync Server, presence and directory are provided by Lync Server.

Option 1: Enable the mailbox with a user account

This section details two tasks you need to complete to enable a mailbox with a user account.

Task 1: Enable the user account associated with the room mailbox

To enable the user account for a room mailbox:

1. In Active Directory, enable the account associated with the room mailbox.
2. Set the user account password to never expire.

   For organizations where a permanent password is not possible, the password for the account will need to be re-entered in each infrastructure device whenever it expires or is changed by the Active Directory administrator.

Task 2: Modify the Room Mailbox Settings

You can use either the Microsoft Exchange PowerShell or the Outlook Web Access to modify room mailbox settings. You will need to include the subject and description information in the meeting invitation. Be aware that some default Exchange configurations hide these fields. The Polycom HDX or Group Series system uses this data to display call information and complete calls.

Optionally, you can add the organizer's name to the meeting invitation. You can modify these settings using Microsoft Exchange PowerShell or Microsoft Office Outlook Web Access.

To use Microsoft Exchange PowerShell to modify the mailbox settings:

1. View the settings for the room mailbox.

   `Get-MailboxCalendarSettings <ExchangeMailbox> | fl`

   For example: `Get-MailboxCalendarSettings zeusroom | fl`

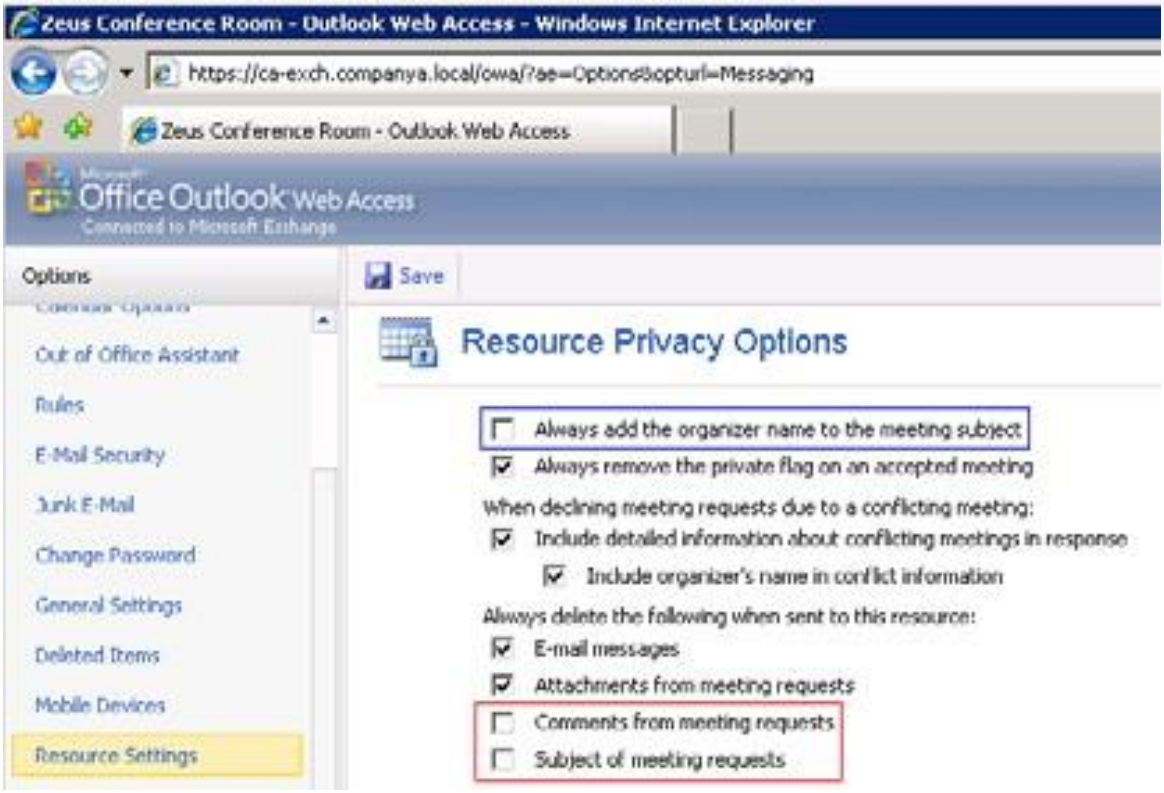
   - Set the `DeleteSubject` value to `False`. The default is `True`.
   - Set the `DeleteComments` value to `False`. The default is `True`.
   - If you want to add the organizer's name to the subject line, set `AddOrganizerToSubject` to `True`.
2. Set the room mailbox properties:

   ```
   Set-MailboxCalendarSettings -id <ExchangeMailbox> -DeleteComments$false -
   DeleteSubject$false -AddOrganizerToSubject$false
   ```

To use Outlook Web Access to enable and modify the mailbox settings:

1. Log in to Outlook Web Access using the room mailbox's credentials.
2. Click **Options**.

3 Select **Resource Settings** from the Options bar and scroll to **Resource Privacy Options**, shown next.



4 Check the following options:

- Check **Always add the organizer name to the meeting subject** if you want to include the organizer's name in the subject line.
- Check **Comments from meeting requests**
- Check **Subject of meeting requests**

Option 2: Use a Service Account to Manage a Room Mailbox

A second configuration option is to have a service account manage the mailbox. You must create a mailbox before you can associate it with a service account.

If your organization requires you to keep room accounts disabled, you can set up an Active Directory user account with rights to manage the room mailbox in Exchange.

Using a service account to manage a mailbox results in two accounts:

- A disabled primary account in Active Directory that has an associated Exchange Mailbox.
- An enabled service account in Active Directory that does not have an Exchange Mailbox directly assigned to it.

Task 1: Create the Service Account

You can name the Active Directory account starting with SRV-, or use another naming scheme in line with your organization's deployment.

To create the service account for your room mailbox:

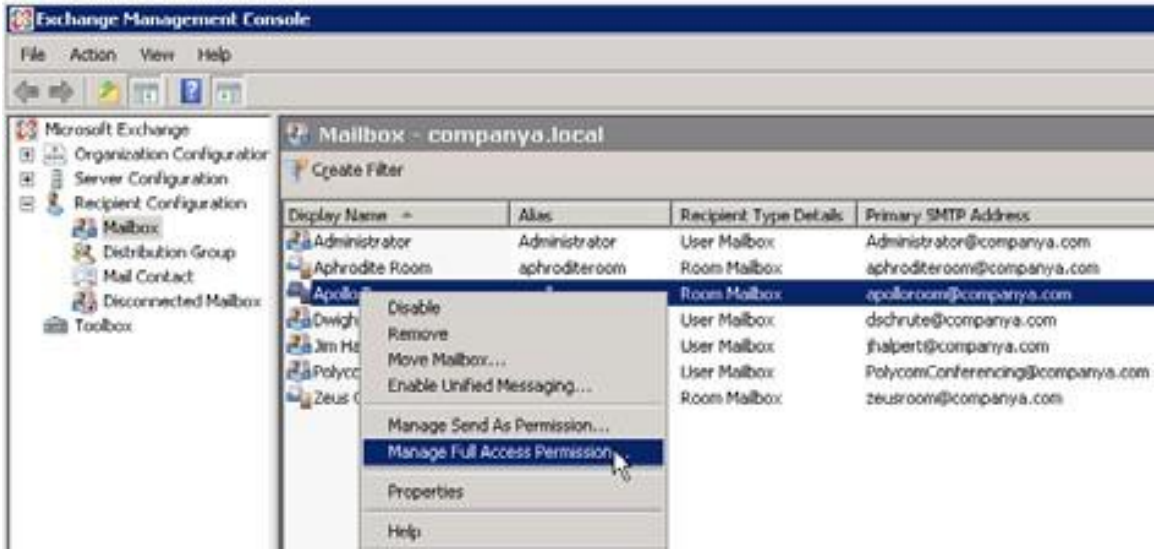
- » Use Active Directory to create the service account you will use to manage the room mailbox.

Task 2: Enable the Service Account Permission to Manage the Room Mailbox

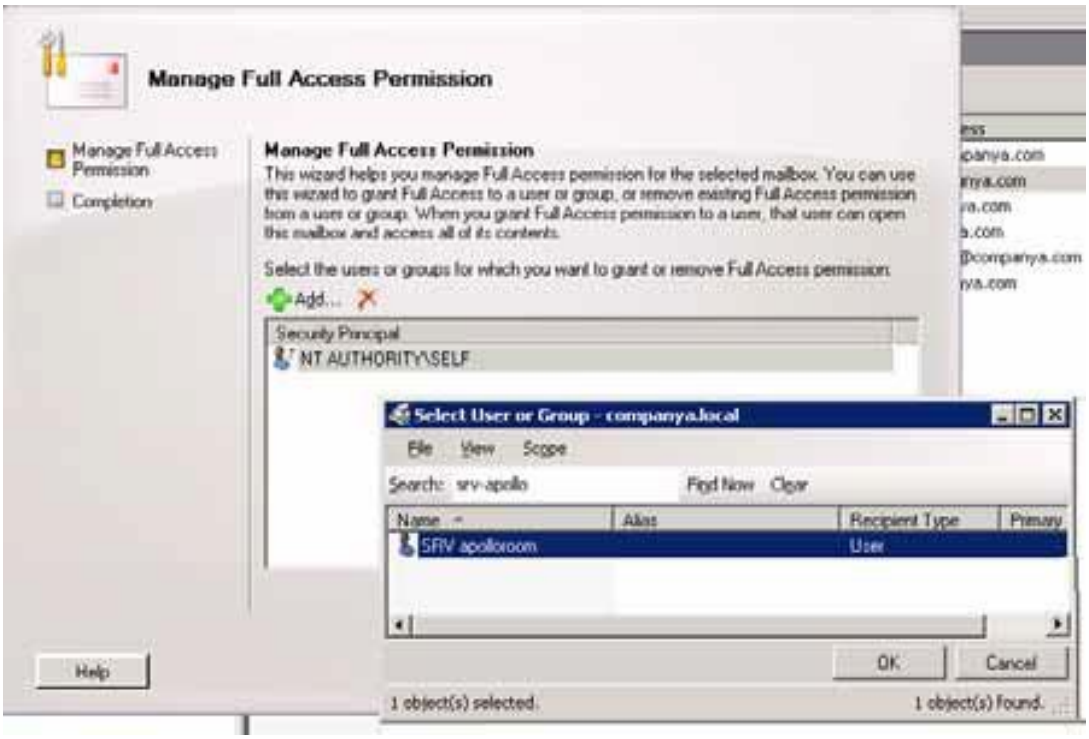
You can use the either the Exchange Management Console or the Exchange Management Shell.

To enable permissions using the Exchange Management Console:

1. Navigate to the resource mailbox you want to grant permissions for.
2. Right-click the mailbox and select **Manage Full Access Permission**, as shown next.



3 In the **Manage Full Access Permission** dialog, click **Add** and add the Active Directory service account to the list. In the Select User or Group dialog shown next, the `SRV-apolloroom` is a service account that has no directly assigned Exchange mailbox but is given permission to manage the room mailbox assigned to the `apolloroom` user.



4 Click **OK** to complete the procedure.

To enable permissions using the Exchange Management Shell:

Run the following Exchange Management Shell command to grant the service account full access permissions for the room mailbox:

```
Add-MailboxPermission -Identity '<conference room primary
SMTP address>' -User
'<domain>\<EPActiveDirectoryAccountUserName>' -AccessRights
'FullAccess' -InheritanceType ‘All’
```

Option 3: Associate Multiple Mailboxes with a Service Account

You can use one service account for all Polycom HDX or Group Series systems in the Polycom Calendaring for Outlook deployment.

Note: Presence Feature is Not Available

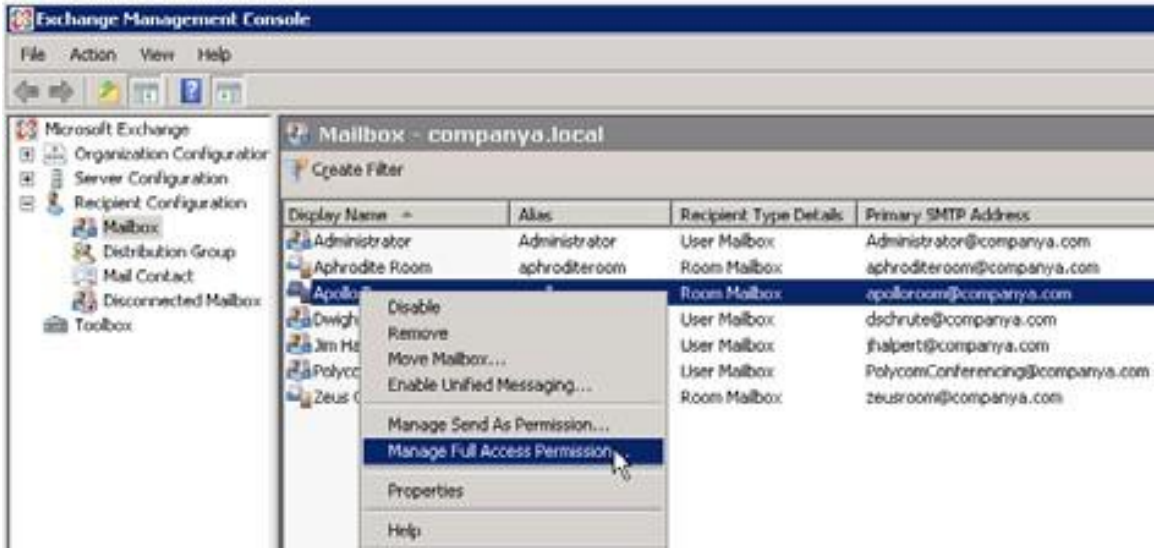
If you create one service account for multiple room mailboxes, you will not be able to take advantage of the presence feature.

The steps for associating multiple mailboxes with a service account are the same as those for single mailboxes, with the exception that you can enable the same service account permission to manage multiple mailboxes.

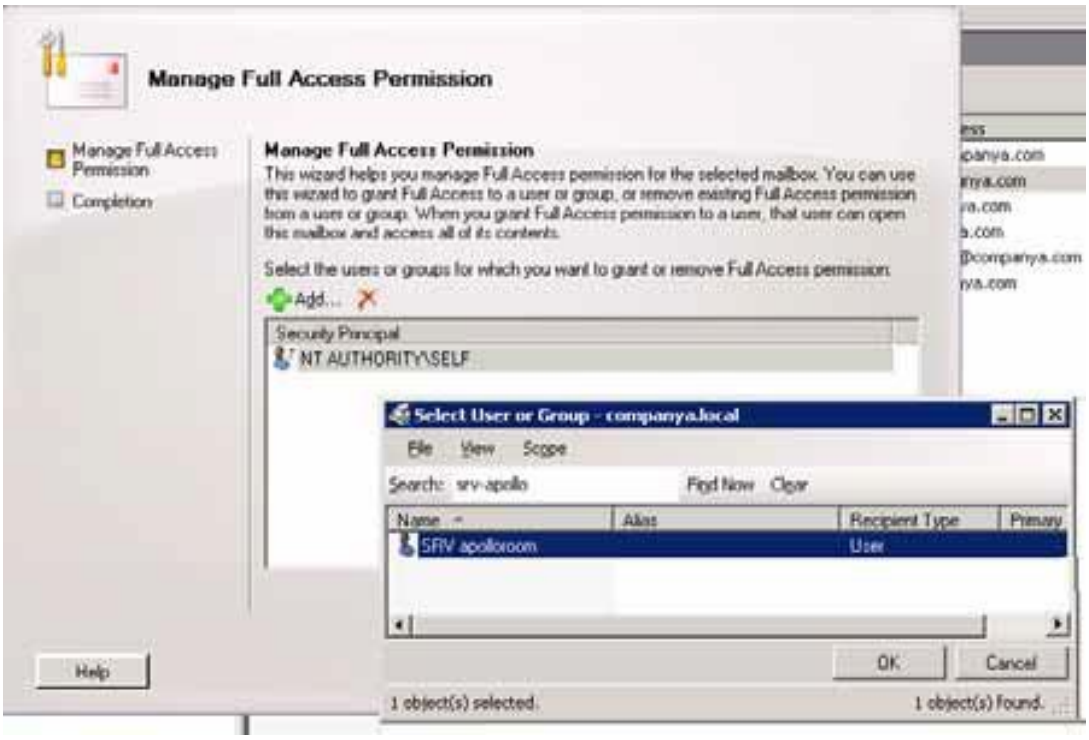
You can use the either the Exchange Management Console or the Exchange Management Shell.

To enable permissions using the Exchange Management Console:

1. Navigate to the resource mailbox you want to grant permissions for.
2. Right-click the mailbox and select **Manage Full Access Permission**, as shown next.



3 In the **Manage Full Access Permission** dialog, click **Add** and add the Active Directory service account to the list. In the Select User or Group dialog shown next, the `SRV-apolloroom` is a service account that has no directly assigned Exchange mailbox but is given permission to manage the room mailbox assigned to the `apolloroom` user.



4 Click **OK** to complete the procedure.

To enable permissions using the Exchange Management Shell:

Run the following Exchange Management Shell command to grant the service account full access permissions for the room mailbox:

```
Add-MailboxPermission -Identity '<conference room primary
SMTP address>' -User
'<domain>\<EPActiveDirectoryAccountUserName>' -AccessRights
'FullAccess' –InheritanceType ‘All’
```

Figure 7, shown next, provides an example configuration. You can replicate this example association between `Aphrodite` and `SRV-AllEP-CompanyA` for multiple rooms.

Figure 7: Using a service account for all HDX or Group Series conference rooms.

Configure Mailboxes for Polycom HDX or Group Series Desktop Systems

You need to configure HDX or Group Series desktop systems in your deployment to use an individual user's Active Directory account and Exchange Mailbox for authentication with Exchange.

Optionally, you can use the Active Directory account to authenticate with Polycom CMA system for automatic provisioning.

There is no additional Exchange configuration necessary to integrate user accounts with HDX or Group Series system.

Configuring HDX or Group Series Mailboxes to Prevent Meeting Conflicts

By default, Microsoft Outlook will allow users and mailboxes to schedule conflicting meetings and you will need to disable this default behavior. You can use either Microsoft Outlook or Microsoft Outlook Web Access to disable this feature for mailboxes that service HDX or Group Series systems.

To configure Microsoft Outlook to decline conflicting meeting requests:

1. In Microsoft Outlook, select **Tools > Options** to view the **Options** dialog.

2 Click **Calendar Options** to view the Calendar Options dialog.

3 In the Advanced Options section, click **Resource Scheduling**.

4 In Resource Scheduling, check both:

- **Automatically accept meeting requests and process cancellations**
- **Automatically decline conflicting meeting requests**

To configure Microsoft Outlook Web Access to decline conflicting meeting requests:

1 In Outlook Web Access, select **Options**.

2 Choose **Resource Settings**.

3 In the Resource Scheduling, check both:

- **Automatically process meeting requests and cancellations**
- **Allow conflicts check boxes are both marked**

Configuring Polycom Group Series System Calendaring Settings

You must configure calendar settings for each Group Series system in your deployment. When configuring calendar settings for a Polycom Group Series, you need to specify the room mailbox and the Active Directory user name for the service account that manages the mailbox.

Note that you have the option of using the Polycom CMA system to dynamically manage the calendaring settings as shown in the section (Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX or Group Series systems.

To configure the calendaring service on a Group Series system:

1 In a web browser, connect to the Group Series system.

2 Go to Admin **Settings > Servers > Calendaring Service**.

3 Check **Enable Calendaring Service**.

4 Complete the following fields.

For complete documentation on configuring calendaring settings for a Group Series system, see the Administrator's Guide for Polycom Group Series Systems.

- **Microsoft Exchange Server Address** This is the fully qualified domain name (FQDN) of the Microsoft Exchange Client Access Server. If your organization has multiple Client Access Servers behind a network load balancer, then the Exchange Server Address is the FQDN of the Client Access Servers' Virtual IP Address. You can use an IP address in place of an FQDN but Polycom recommends using the same FQDN that you use for Outlook clients.
- **Domain** This is the logon domain of the user in either NETBIOS or DNS name notation. For example, in an Active Directory domain named `companya.local` with a NETBIOS name of `COMPANYA` you can enter either `companya.local` or `COMPANYA`.
- **User Name** This is the Active Directory account's user name and no domain information included.

- **Password** The password for the user account.
- **Mailbox (Primary SMTP)** This must match the **Primary SMTP Address** for the account in Exchange. This address displays as the **Mail** field in Active Directory.

5 Click **Update**.

Example Calendar Settings

This section provides several calendaring example settings.

Figure 8 shows an example of Option 1: Enable the user account for the room mailbox. The `zeusroom` Active Directory account is enabled and no service accounts are required. The User Name `zeusroom` Active Directory account is enabled as well.

Figure 8: Assigning a User Account for a Room Mailbox.

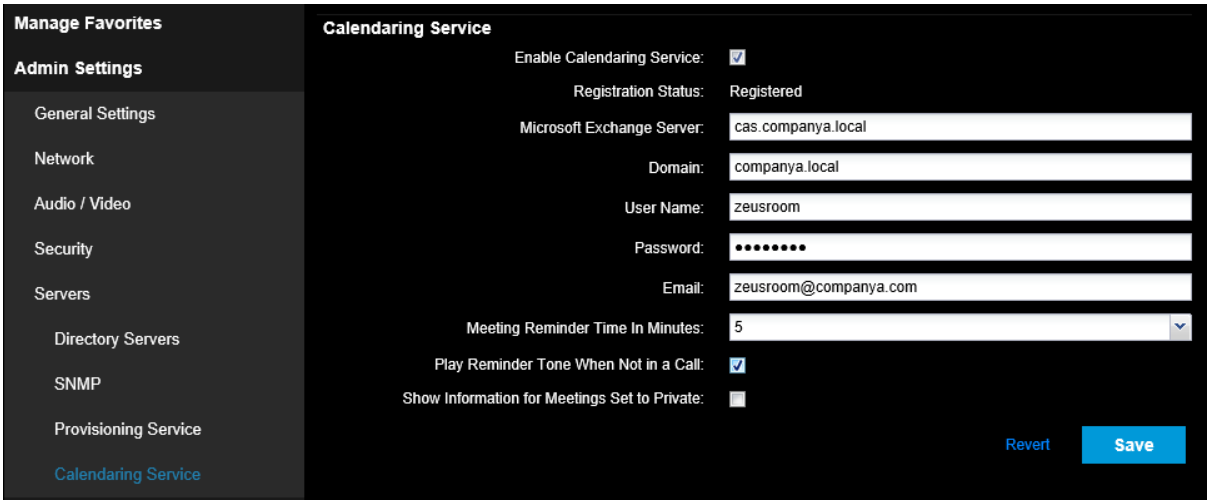


Figure 9 shows an example of Option 2: Use a Service Account with a Room Mailbox. In this example, the `apolloroom` mailbox and the `SRV-apolloroom` service account is integrated in a Group Series system.

Figure 9: Using a service account to manage a mailbox

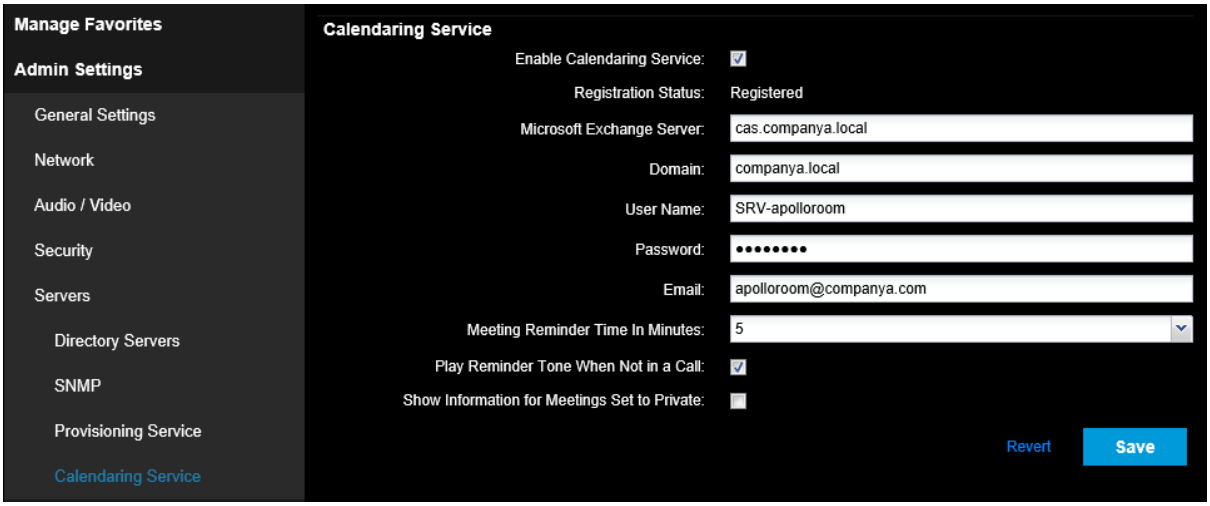


Figure 10 shows Option 3: Associate Multiple Mailboxes with a Single Account. In this example, the `aphroditeroom` is associated with the `SRV-AllGS-CompanyA` service account. Note that this account may be associated with other Group Series room system mailboxes.

Figure 10: Associate Multiple Mailboxes with a Single Account

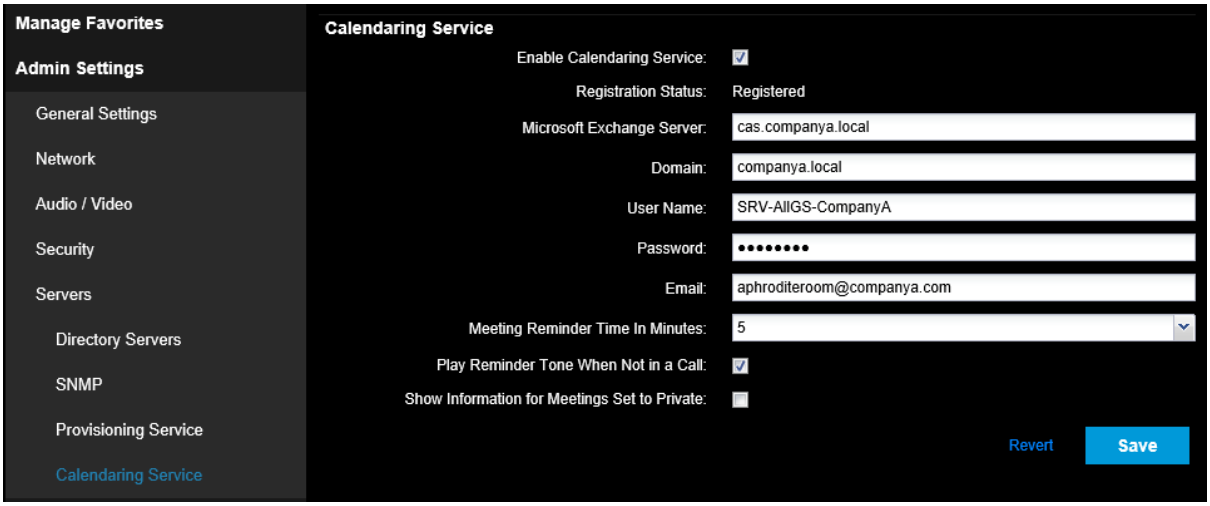


Figure 11 shows the calendar settings of the Polycom Group Series system assigned to user Dwight Schrute, which reside on the LAN inside Company A's corporate network.

Figure 11: User-based Calendar Settings in the Polycom Group Series System

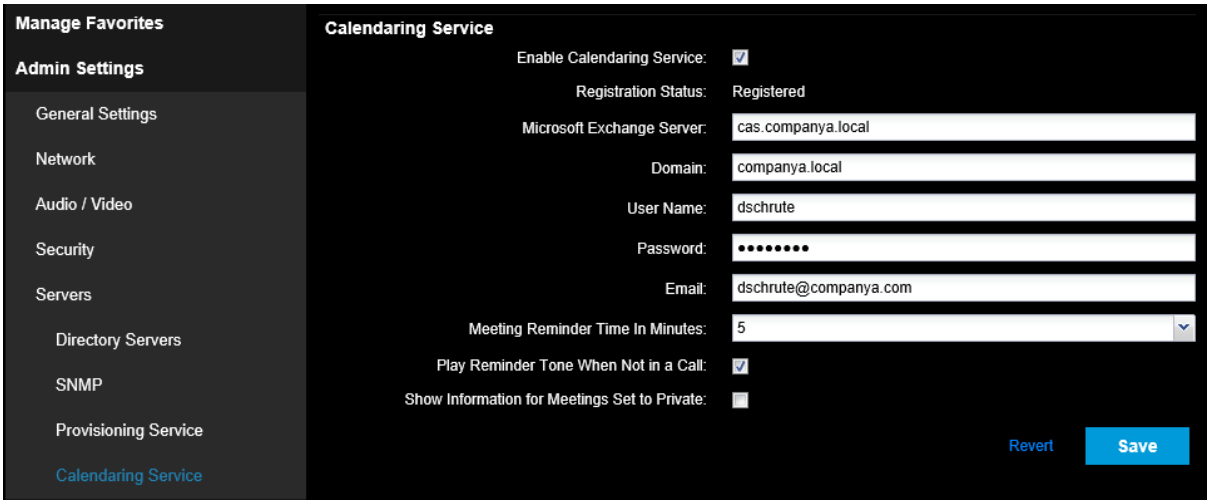
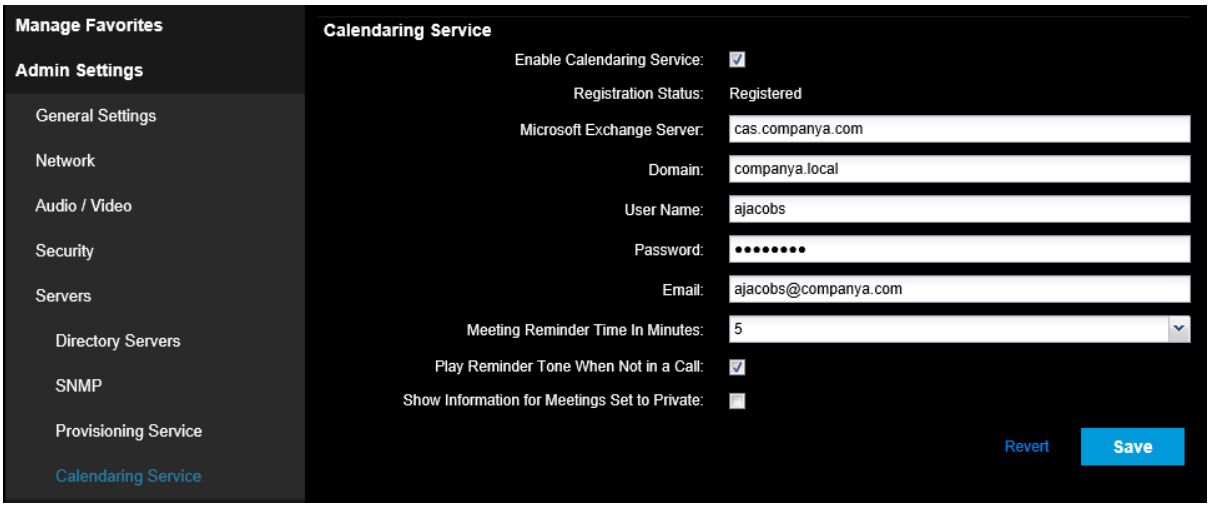


Figure 12 shows the configuration for a Small Office Home Office (SOHO) user. The Group Series relies on Exchange Web Services for remote access. For this reason, when configuring a remote Group Series user, you need to use a publicly-routable Exchange server address and enable Microsoft Outlook Anywhere.

Figure 12: Calendar Configuration for a SOHO User.



Configuring Polycom HDX System Calendaring Settings

You must configure calendar settings for each HDX system in your deployment. When configuring calendar settings for a Polycom HDX, you need to specify the room mailbox and the Active Directory user name for the service account that manages the mailbox.

Note that you have the option of using the Polycom CMA system to dynamically manage the calendaring settings as shown in the section (Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX or Group Series systems.

To configure the calendaring service on an HDX system:

1. In a web browser, connect to the HDX system.
2. Go to **Admin Settings > Global Services > Calendaring Service**.
3. Check **Enable Calendaring Service**.
4. Complete the following fields.

   For complete documentation on configuring calendaring settings for an HDX system, see the Administrator's Guide for Polycom HDX Systems.

   - **Server Address** This is the fully qualified domain name (FQDN) of the Microsoft Exchange Client Access Server. If your organization has multiple Client Access Servers behind a network load balancer, then the Exchange Server Address is the FQDN of the Client Access Servers' Virtual IP Address. You can use an IP address in place of an FQDN but Polycom recommends using the same FQDN that you use for Outlook clients.
   - **Domain** This is the logon domain of the user in either NETBIOS or DNS name notation. For example, in an Active Directory domain named `companya.local` with a NETBIOS name of `COMPANYA` you can enter either `companya.local` or `COMPANYA`.
   - **User Name** This is the Active Directory account's user name and no domain information included.
   - **Password** The password for the user account.
   - **Mailbox (Primary SMTP)** This must match the **Primary SMTP Address** for the account in Exchange. This address displays as the **Mail** field in Active Directory.
5. Click **Update**.

Example Calendar Settings

This section provides several calendaring example settings.

Figure 13 shows an example of Option 1: Enable the user account for the room mailbox. The `zeusroom` Active Directory account is enabled and no service accounts are required. The User Name `zeusroom` Active Directory account is enabled as well.

Figure 13: Assigning a User Account for a Room Mailbox.

Figure 14 shows an example of Option 2: Use a Service Account with a Room Mailbox. In this example, the `apolloroom` mailbox and the `SRV-apolloroom` service account is integrated in an HDX system.

Figure 14: Using a service account to manage a mailbox

Figure 15 shows Option 3: Associate Multiple Mailboxes with a Single Account. In this example, the `aphroditeroom` is associated with the `SRV-AllHDX-CompanyA` service account. Note that this account may be associated with other HDX room system mailboxes.

Figure 15: Associate Multiple Mailboxes with a Single Account

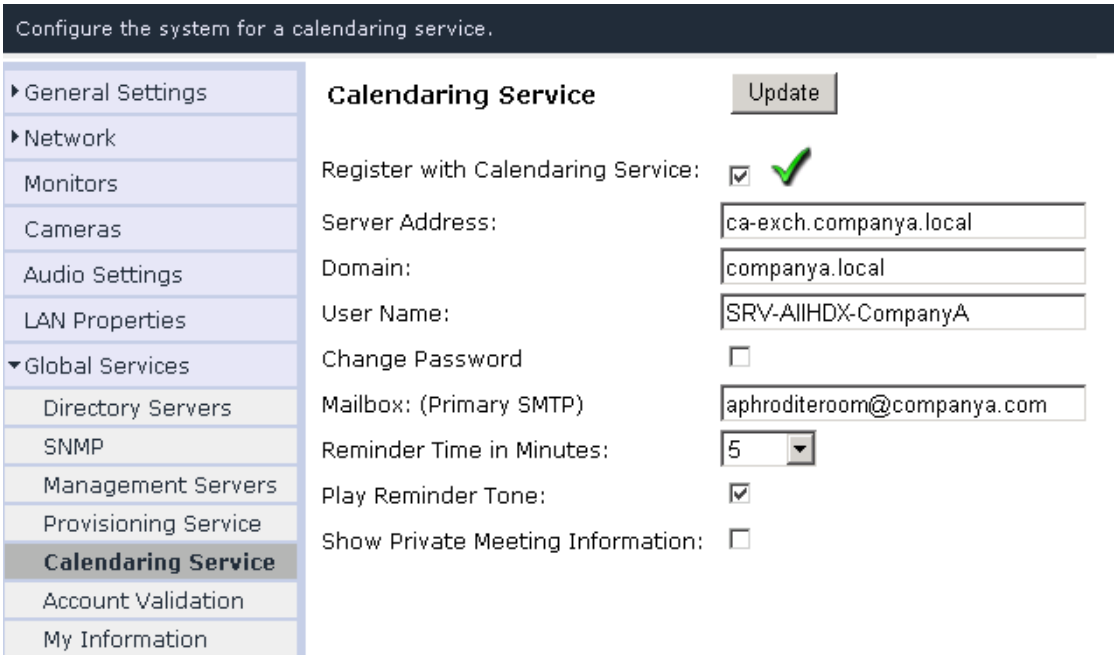


Figure 16 shows the calendar settings of the Polycom HDX system assigned to user Dwight Schrute, which reside on the LAN inside Company A's corporate network.

Figure 16: User-based Calendar Settings in the Polycom HDX System

Figure 17 shows the configuration for a Small Office Home Office (SOHO) user. The HDX relies on Exchange Web Services for remote access. For this reason, when configuring a remote HDX user, you need to use a publicly-routable Exchange server address and enable Microsoft Outlook Anywhere.

Figure 17: Calendar Configuration for a SOHO User.

(Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX or Group Series systems

If you want to use the Polycom CMA system to automatically provision a Polycom endpoint system, the endpoint system must use the same user name and password to access both the Exchange server and the Polycom CMA system, as shown in the Polycom CMA System Operations Guide.

Note: Use an enabled resource account room mailbox with CMA

You must use an enabled resource account room mailbox to take advantage of CMA Automatic Provisioning.

Configuring and Installing the Polycom Calendaring for Outlook add-In

The Polycom Calendaring for Outlook add-In software and its templates must be installed on each Microsoft Outlook client.

For complete instructions, see *Configure and Install the Polycom Calendaring for Outlook add-In* in the Polycom Unified Communications Deployment Guide for Microsoft Environments.

Configuring and Installing the Polycom Calendaring for Outlook add-in requires you to complete the following three tasks:

- Task 1: Configure Polycom Calendaring for Outlook add-in Preferences for Installation to Client PCs
- Task 2: Install Polycom Calendaring for Outlook add-in to Client PCs
- Task 3: Deploy Customization Files

Task 1: Configure Polycom Calendaring for Outlook add-in Preferences for Installation to Client PCs

You can configure the client experience of the Polycom Calendaring for Outlook add-in before deploying the client to users. For details on how to configure preferences as an administrator, refer to *Configure and Install the Polycom Calendaring for Outlook add-In* in the Polycom Unified Communications Deployment Guide for Microsoft Environments.

Task 2: Install Polycom Calendaring for Outlook add-in to Client PCs

You can install the Calendaring for Outlook add-in in a number of ways. After customizing preferences in Task 1:, you can provide the installation file to users via existing software deployment processes. You can provide user a link to a network location the file resides on by using a software installation program like

Microsoft SMS or using a Group Policy Object. For information about preferred software delivery methods, consult the documentation for your software delivery product.

For an example deployment method using Microsoft Active Directory and Global Policy, refer to *Configure and Install the Polycom Calendaring for Outlook add-In* in the Polycom Unified Communications Deployment Guide for Microsoft Environments.

Task 3: Deploy Customization Files

After installing the conference add-ins, you can deploy the customization files you created in Task 1 to the folder locations on client PCs. The add-in must already be installed on the client PC to ensure these file paths have been created. For an example of a deployment method using Microsoft Active Directory and Global Policy, refer to *Configure and Install the Polycom Calendaring for Outlook add-in* in the Polycom Unified Communications Deployment Guide for Microsoft Environments.

Testing Polycom Calendaring for Outlook Deployment

- Walk through scheduling and joining a meeting.
- For more details on the on-screen experience with a Polycom HDX system, see the Administrator's Guide for Polycom HDX Systems.
- For more details on the on-screen experience with a Polycom Group Series system, see the Administrator's Guide for Polycom Group Series Systems.

Appendix A: Polycom® HDX System Configuration Files

The following table lists all of the `.dat` files that the Polycom® HDX system can read from the USB boot device.

You can put these files in a `/usb_oob/general` directory or in a `/usb_oob/<serial_number>` directory on a USB storage device.

- Provisionable configuration files in `the /usb_oob/general` directory are copied to the Polycom HDX system unconditionally.
- Provisionable configuration files in the `/usb_oob/<serial_number>` directory are copied to Polycom HDX system only when the `<serial_number>` matches the serial number of the endpoint.
- If the same file exists in both the `/usb_oob/general` and `/usb_oob/<serial_number>` directories, the copy in the `/usb_oob/<serial_number>` directory takes priority.

Table 11: Polycom HDX .dat Files

`.dat` File Name	*Description*	*Value Range*	*Content Example*
langwithcntry	Language and country	Text string	English/en
connecttomylan	Enable or disable LAN interface	False, True	
lanportspeed	LAN speed	Auto, 10_Mbps, 100_Mbps, 1000_Mbps	
landuplexmode	LAN duplex	Auto, Full, Half	
dot1xenabled	Enable or disable 802.1X authentication	False, True	
dot1xid	802.1X authentication user id	Text string	johnsmith
dot1xpwd	802.1X authentication password	Text string	johnsmithpassword
vlanmode	Enable or disable VLAN	False, True	
vlanid	VLAN ID	Integer in [2,4094]	100

.dat File Name	*Description*	*Value Range*	*Content Example*
.dat File Name	Description	Value Range	Content Example
dhcp_flg	Enable or disable DHCP client	Client, Off	
hostname	Host name of the Polycom HDX system	Text string	hdx334
userdomain	Domain of the user account used to log into the provisioning server	Text string	polycom.com
domainname	Domain of the Polycom HDX system, which will be set by the network itself if DCHP is provisioned	Text string	
ipaddress	IP address of the Polycom HDX system	IP address	172.18.1.222
subnetmask	Subnet mask of the Polycom HDX system		255.255.255.192
defaultgateway	IP address of the default router	IP address	172.18.1.65
dnsserver	DNS server	IP address	172.18.1.15
dnsserver1	Alternate DNS server	IP address	
dnsserver2	Alternate DNS server	IP address	
dnsserver3	Alternate DNS server	IP address	
provisionserveraddress	IP address of the Polycom CMA server	IP address or host name	polycomCMA.polycom.com
ldapuserid	LDAP user id	Text string	johnsmith
ldappassword	LDAP password	Text string	johnsmithpassword

Appendix B: Exchange Calendar Polling Information

This appendix provides information on Exchange Calendar Polling.

Polycom HDX and Group Series System

When actively viewing the endpoint's calendar onscreen, the Polycom HDX and Group Series system polls the Exchange server for updates every 20 seconds. When viewing any other screen, or when the Polycom HDX or Group Series system is in standby, polling occurs every five minutes.

Polycom DMA System

Polycom DMA system uses the Push Notification feature of Exchange Web Services to receive notifications of new or updated calendar events in the Polycom Calendaring Mailbox as they are created. Upon receiving a push notification, Polycom DMA system connects to Exchange to download the meeting details. When doing this, Polycom DMA system processes the new event and also requests a refreshed view of all calendar events occurring in the next 24 hours.

In the absence of these notifications, Polycom DMA system connects to the Exchange server every five minutes to retrieve the number of events scheduled to occur on the current calendar day, which it reports on the Dashboard under Calendaring Service as Meetings scheduled today.

Polycom RMX System

The Polycom RMX system polls the Exchange server for updates every 15 seconds. When polling, the RMX considers events two hours in the past and 24 hours into the future.

Polycom RSS System

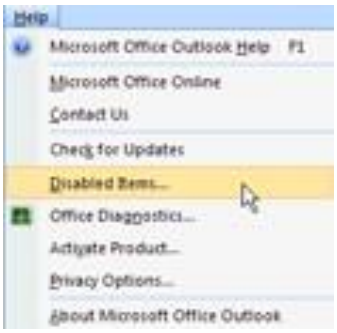
The Polycom RSS system polls the Exchange server every 30 seconds.

Troubleshooting

Use the following list as a guide to resolving the following issues, problems, or common difficulties you may encounter while deploying this solution.

I am no longer able to access the Polycom Calendaring for Outlook add-in

The Polycom Calendaring for Outlook add-in can become disabled. If this occurs, navigate to **Help** > **Disabled Items** in Microsoft Outlook and enable the Polycom Calendaring for Outlook add-in again.



Polycom HDX or Group Series systems display conference times but no details

The Exchange PowerShell commands that delete meeting information after a meeting has been accepted have not been correctly completed. Review the Exchange PowerShell commands in Task 2: Modify the Room Mailbox Settings and verify that they have been performed correctly.

I am unable to complete a call to a federated or remote HDX or Group Series system

In a Lync Server deployment, you must enable HDX or Group Series system users for remote access and federation as shown in Task 3: Enable the RMX Account for Remote Access and Federation.

I cannot import a PFX file into the RMX system

Because the content of container PFX files can vary, the RMX system sometimes fails to import it. The workaround is to use OpenSSL to extract the files you need from the PFX file. Once the *.pfx file is on your PC, you can upload it to the Polycom RMX system and install it.

Follow these instructions:

1. Download and install OpenSSL if necessary on the RMX workstation. You can download OpenSSL from Shining Light Productions.
2. Use OpenSSL to extract the root CA certificate. For example,

   ```
   C:\Program Files\OpenSSL-Win64\bin\openssl pkcs12 -in rmxcert.pfx -cacerts -nokeys -out rootCA.pem
   ```

3. Use OpenSSL to extract the certificate. For example,

   ```
   C:\Program Files\OpenSSL-Win64\bin\openssl pkcs12 -in rmxcert.pfx -clcerts -out cert.pem -nodes
   ```

4. Use OpenSSL to extract the private key. For example,

```
C:\Program Files\OpenSSL-Win64\bin\openssl pkcs12 -in rmxcert.pfx -clcerts -out
pkey.pem -nodes
```

5. Manually create your password file.
   - Create a new text file called `certPassword.txt` containing the pfx password on single line with no carriage return.

Once the `*.pfx` file is on your PC, you can upload it to the Polycom RMX system and install it, using the procedures in the Polycom RMX system's documentation.

Getting Help

For more information about installing, configuring, and administering Polycom products, refer to Documents and Downloads at Polycom Support.

To find all Polycom partner solutions, see Polycom Global Strategic Partner Solutions.

For more information on solutions with this Polycom partner, see the following resources:

- Polycom Unified Communications Solution for Microsoft Environments on Polycom Strategic Global Partner Solutions site.
- Lync Server 2010 PowerShell.
- Microsoft's Lync Server 2010 Planning Guide and Microsoft Lync Server 2010 on the Microsoft TechNet Library.

The Polycom Community

The Polycom Community gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, simply create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.