Polycom® Unified Communications Deployment Guide for Microsoft® Environments
Contents

About This Guide ............................................................................................................................................. 1

Conventions Used in this Guide ..................................................................................................................... 1
  Information Elements ................................................................................................................................. 1
  Typographic Conventions .......................................................................................................................... 2
  What's in This Guide? ................................................................................................................................. 2

Chapter 1: Getting Started ............................................................................................................................. 5

Before You Begin ........................................................................................................................................... 5
What's New? .................................................................................................................................................. 5
Required Solution Hardware ......................................................................................................................... 5
Hardware and Software Dependencies ......................................................................................................... 6
Getting Help and Support Resources .......................................................................................................... 6

Chapter 2: Polycom® Unified Communications for Microsoft® ................................................................. 7

Polycom-Enabled Unified Communications ................................................................................................. 7
  End User Advantages ................................................................................................................................. 7
  System Administrator Advantages ............................................................................................................. 8
Polycom Conferencing for Microsoft Outlook............................................................................................... 8
  End User Advantages ................................................................................................................................. 8
  System Administrator Advantages ............................................................................................................. 8

Chapter 3: Using Polycom®-Enabled Unified Communications with Microsoft® Lync™ Server 2010 ................................................................................................................................. 11

Features of the Polycom-Enabled Lync Server 2010 Solution ....................................................................... 11
Supported Lync Server Versions .................................................................................................................. 12
Before You Begin .......................................................................................................................................... 12
  General Knowledge ................................................................................................................................. 12
  Encryption and Security ............................................................................................................................ 12
  Remote and Federated Users ...................................................................................................................... 13
  Microsoft Call Admission Control ........................................................................................................... 13
  Microsoft Real-Time Video (RTV) ............................................................................................................. 13
Getting Help from Polycom Solution Support Services .................................................................................. 13
Polycom Products Tested for use with this Solution .................................................................................... 14
Setting up Dial Plans for a Lync Server Environment ................................................................................... 16
  Matched URI Dialing ............................................................................................................................... 16
  Registered RMX User Name Dialing ........................................................................................................ 16
Supporting Remote and Federated Users in Lync Server Environments ....................................................... 17
# Polycom® Unified Communications Deployment Guide for Microsoft® Environments

## Chapter 4: Deploying Polycom® HDX Systems

### Configuring Lync Server 2010 for use with an HDX System
- Configuring Authentication in Lync Server .................................................. 21
- Using Microsoft Call Admission Control ...................................................... 22
- Enabling RTV on the Lync Server ................................................................. 22
- Adding Calendar and Scheduling Features to Polycom HDX Systems ............. 22
- Enabling Conference Rooms for the Lync Server ......................................... 23
- Enabling Conference Room Access for Remote and Federated Users .......... 23
- Adding Lync Contacts to Conference Room Local Address Book .................. 24

### Configuring Your Polycom HDX System for Lync Server
- Installing the RTV Option Key on your HDX System .................................... 24
- Register Polycom HDX System with the Lync Server .................................... 25
- Understanding SIP Settings ........................................................................... 26
- Configuring the Polycom HDX System LAN Properties .................................. 28
- Configuring Display Options for the HDX System Contact List ..................... 28
- Configuring AES Encryption .......................................................................... 28
- Supporting Lync-hosted Video Conferencing ............................................... 29
  - Using the Polycom Touch Control with Lync Conferencing ....................... 29
  - Understanding Roles in Lync-hosted Calls ................................................. 30

### Supporting Microsoft Real-Time Video (RTV)
- Call Quality Scenarios for RTV Video ......................................................... 31

## Chapter 5: Deploying Polycom® Immersive Telepresence (ITP) Systems

### Configuring Lync Server 2010 for use with a Polycom ITP System
- Configuring Authentication in Lync Server .................................................. 33
- Configuring Microsoft Call Admission Control ............................................. 33
- Enabling High-Definition (HD) Video on the Lync Server ............................ 34
- Creating and Enabling Conference Room User Accounts ............................ 34
  - Task 1: Add a Conference Room User for each Codec within your ITP System .......... 34
  - Task 2: Enable Conference Rooms for the Lync Server ............................ 35
- Hiding the Secondary Codecs in the Lync Directory ....................................... 36
  - Hiding the Secondary Codecs in the Directory Using the Exchange Management Console 36
  - Hiding the Secondary Codecs in the Directory Using the ADSI Edit Tool .......... 37
- Enabling Conference Room Access for Remote and Federated Users .......... 38

### Configuring Your Polycom ITP System for Lync Server
- Registering All Codecs with the Lync Server ............................................... 39
- Configuring the LAN Properties for each Codec ......................................... 42
- Configuring Display Options for the ITP System Contact List ..................... 43
Contents

Chapter 6: Deploying Polycom® RMX Systems ................................................. 45

Configuring Your Polycom RMX System for Lync Server .......................... 45
Set up the RMX System for Security and SIP ........................................... 46
  Task 1: Configure the RMX IP Network Service .................................. 46
  Task 2: Add the RMX FQDN (SIP signaling IP address) in DNS .............. 46
  Task 3: Installing the certificate on your RMX system ......................... 47
Configuring Encryption for your Deployment ......................................... 51
Configuring Lync Server for use with a Polycom RMX System .................. 52
  Task 1: Use Lync Topology Builder to Define Your Trusted Application Pool 52
  Task 2: Use Lync PowerShell to Create the Trusted Application .......... 53
  Task 3: Use Lync PowerShell to Update the Topology ......................... 53
  Task 4: Use Lync PowerShell to Define a Static Route for the Polycom RMX System 54
Enabling Microsoft Presence ..................................................................... 54
  Configuring your Microsoft Environment to Support RMX Room Presence 54
    Task 1: Create an Active Directory Account for the Conferencing Entity 55
    Task 2: Enable the Active Directory Account for Lync Server .......... 56
    Task 3: Enable the RMX Account for Remote Access and Federation .... 57
  Configuring your RMX System for Microsoft Presence .......................... 57
    Task 1: Enabling SIP Registration in the Conference Profile .............. 57
    Task 2: Create or Modify the RMX Conferencing Entity .................. 58
Enabling Edge Server Integration with your Polycom RMX System .............. 59
Setting Up a Microsoft Edge Server for the Polycom RMX System ............ 59
  Task 1: Create an Active Directory Account for the RMX System .......... 60
  Task 2: Enable the RMX User Account for Lync Server Edge Server ...... 61
  Task 3: Enable the RMX Account for Remote Access and Federation ..... 61
  Task 4: Configure the RMX System for Federated Dialing .................. 62
  Task 5: Configure RMX System Flags for Federation and Microsoft Call Admission Control 63
Monitoring the connection to the STUN and Relay Servers in the ICE environment .......... 63

Chapter 7: Deploying Polycom® DMA Systems ............................................. 65

Configuring Lync Server for Use with a DMA System .............................. 65
Set the Routing for the Polycom DMA System ......................................... 65
  Task 1: Use Lync Topology Builder to Define Your Trusted Application Pool 65
  Task 2: Use Lync PowerShell to Set the Polycom DMA System as a Trusted Host with a Static Route ................................................................. 66
  Task 3: Use Lync PowerShell to Create the Trusted Application .......... 67
  Task 4: Use Lync PowerShell to Update the Topology ......................... 67
Communications Server
Chapter 8: Polycom

Polycom® Unified Communications
Deploying Polycom Immersive Telepresence

Deploying Polycom HDX Systems with Office Communications Server

Deploying Polycom Immersive Telepresence (ITP) Systems with Office Communications Server

Enable Federation in your Lync Environment .................................................. 68
Task 1: Configure the Microsoft Lync Edge Server ........................................ 68
Task 2: Ensure the Primary SIP Signaling Domain is Allowed ...................... 68
Configuring Your Polycom DMA System for Lync Server ......................... 69
Ensure DNS is Configured Properly ................................................................. 69
Create a Security Certificate for the Polycom DMA 7000 System ............... 69
Configure a DMA System SIP Peer for Lync Server .................................. 74
    Task 1: Configure a SIP Peer in the DMA System .................................. 74
    Task 2: (Optional) Configure your DMA System to Route to Specific SIP Domains ............ 76
    Task 3: Set up a Dial Rule for the Lync Server ....................................... 76
Chapter 8: Polycom®-Enabled Unified Communications for Microsoft® Office Communications Server ................................................................. 79
Understanding Microsoft Office Communications Server Environments ........ 79
    Features Available with Office Communications Server .......................... 80
    Key Concepts .......................................................................................... 80
        Microsoft Domain Accounts ............................................................... 80
        Encryption and Security .................................................................... 80
        Remote and Federated Users ............................................................ 80
Polycom Products you can Integrate with Office Communications Server ... 80
Deploying Office Communications Server ...................................................... 82
    Task 1: Implementing Requirements for Office Communications Server .... 82
    Task 2: Configure Authentication in Office Communications Server .......... 83
    Task 3: Add Conference Rooms with Polycom HDX Systems to Active Directory ............................ 83
    Task 4: Enable Conference Rooms for the Office Communications Server .......... 84
    Task 5: Enable Conference Rooms for Remote Access and Federation .... 84
    Task 6: Add Contacts to the Conference Room Local Address Book ........... 85
    Task 7: Configure the Office Communications Server Pool Encryption Setting ...................... 86
Deploying Polycom HDX Systems with Office Communications Server ........ 87
    Task 1: Register Polycom HDX Systems with the Office Communications Server .......... 87
        Understanding SIP Settings ............................................................. 89
    Task 2: Configure the Polycom HDX System LAN Properties .................... 90
    Task 3: Configure Display Options for Contact List ................................ 91
    Task 4: Configure AES Encryption ...................................................... 91
Deploying Polycom Immersive Telepresence (ITP) Systems with Office Communications Server ................................................................. 92
    Configuring Office Communications Server for Use with an ITP System .... 92
        Task 1: Configure Authentication on the Office Communications Server ............ 92
        Task 2: Configure Microsoft Call Admission Control .......................... 92
        Task 3: Enable HD Video on the Office Communications Server .............. 92
        Task 4: Add a Conference Room User for each Codec within your ITP System ... 93
        Task 5: Enable Conference Rooms for the Office Communications Server ....... 94
        Task 6: Hiding the Secondary Codecs in the Directory .......................... 95
Communications Server

Chapter 9: Supporting Remote and Federated Users for Microsoft® Office Communications Server

Deploying Microsoft Office Communications Edge Server for Federation

Deploying Microsoft Office Communications Edge Server

Task 1: Configure the RMX/DMA as a Routable Gateway

Task 2: Ensure SIP Signaling Domains are Allowed

Deploying RMX Systems with Office Communications Server Edge Server

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

Task 2: Create the RMX User Account for Office Communications Server Edge Server

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

Task 4: Configure the RMX for ICE Dialing

Task 5: Add the SIP Signaling Domain to the Federated Office Communications Server Edge Server

Monitor the connection to the STUN and Relay Servers in the ICE environment
Appendix A: Polycom® HDX System Configuration Files .............................. 153

Appendix B: Exchange Calendar Polling Information ............................. 155

Polycom HDX System ............................................................................. 155
Polycom DMA System .......................................................................... 155
Polycom RMX System ........................................................................... 155
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RSS System</td>
<td>155</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>157</td>
</tr>
<tr>
<td>Getting Help</td>
<td>159</td>
</tr>
<tr>
<td>The Polycom Community</td>
<td>159</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td><img src="image" alt="Note Icon" /></td>
<td>The Note icon highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.</td>
</tr>
<tr>
<td>Administrator Tip</td>
<td><img src="image" alt="Administrator Tip Icon" /></td>
<td>The Administrator Tip icon highlights techniques, shortcuts, or productivity related tips.</td>
</tr>
<tr>
<td>Caution</td>
<td><img src="image" alt="Caution Icon" /></td>
<td>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.</td>
</tr>
<tr>
<td>Warning</td>
<td><img src="image" alt="Warning Icon" /></td>
<td>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.</td>
</tr>
<tr>
<td>Web Info</td>
<td><img src="image" alt="Web Info Icon" /></td>
<td>The Web Info icon highlights supplementary information available online such as documents or downloads on support.polycom.com or other locations.</td>
</tr>
<tr>
<td>Timesaver</td>
<td><img src="image" alt="Timesaver Icon" /></td>
<td>The Timesaver icon highlights a faster or alternative method for accomplishing a method or operation.</td>
</tr>
<tr>
<td>Power Tip</td>
<td><img src="image" alt="Power Tip Icon" /></td>
<td>The Power Tip icon highlights faster, alternative procedures for advanced administrators already familiar with the techniques being discussed.</td>
</tr>
</tbody>
</table>
Typographic Conventions

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

### Typographic Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Highlights interface items such as menus, soft keys, file names, and directories. Also used to represent menu selections and text entry to the phone.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Underlined Blue</strong></td>
<td>Used for URL links to external Web pages or documents. If you click on text in this style, you will be linked to an external document or Web page.</td>
</tr>
<tr>
<td><strong>Blue Text</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Fixed-width-font</strong></td>
<td>Used for code fragments and parameter names.</td>
</tr>
</tbody>
</table>

What's in This Guide?

The first chapter *Getting Started* introduces Polycom and X Unified Communication solutions. The chapters following show you how to configure and deploy specific Polycom products and systems in Microsoft Environments. The Troubleshooting section shows you solutions to common troubleshooting problems with this solution and the Getting Help section shows you where to obtain further information and how to access the Polycom community.
Chapter 1: Getting Started  Use this chapter to get an introduction and an overview of the solution, including required hardware and software.

Chapter 2: Polycom Unified Communications for Microsoft  Use this brief chapter to get an understanding of Polycom Unified Communications and an overview of Polycom Conferencing for Microsoft Outlook.


Chapter 4: Deploying Polycom HDX Systems  This chapter shows you how to deploy Polycom HDX systems in a Microsoft Lync Server 2010 environment.

Chapter 5: Deploying Polycom Immersive Telepresence (ITP) Systems  This chapter shows you how to deploy Polycom ITP systems in a Microsoft Lync Server 2010 environment.

Chapter 6: Deploying Polycom RMX Systems  This chapter shows you how to deploy Polycom RMX systems in a Microsoft Lync Server 2010 environment.

Chapter 7: Deploying Polycom DMA Systems  This chapter shows you how to deploy Polycom DMA systems in a Microsoft Lync Server 2010 environment.

Chapter 8: Polycom-enabled Unified Communications for Microsoft Office Communications Server  This chapter shows you how to implement and integrate Polycom-enabled unified communications (UC) and the Microsoft Office Communications Server components.

Chapter 9: Supporting Remote and Federated Users for Office Communications Server  This chapter shows you how to support federated or remote users by including an Office Communications Server edge server in your environment.

Chapter 10: Polycom Conferencing for Microsoft Outlook  This chapter shows you how to deploy Polycom Conferencing for Microsoft Outlook.

Chapter 11: Deploying Polycom Voice Products  This chapter shows you how to deploy Polycom voice products that support Microsoft Lync Server 2010.

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.
Chapter 1: Getting Started

This Polycom solutions guide explains how to deploy Polycom® Unified Communications (UC) software and products in a Microsoft® environment. This 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.

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 Management Shell and in particular, the Windows PowerShell feature
- Microsoft Active Directory server
- Microsoft Exchange Server
- Microsoft Office Communications Manager 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 Wave 7 include the following:

- The number of RMX video meeting rooms (VMRs) supported for Microsoft presence is increased to 100
- Microsoft-qualified support for call admission control (CAC)
- Support for updated Wave 7 versions of DMA, RMX, HDX, and ITP products
- Support for NextGen endpoints (Room Series) and VVX endpoints
- Mixed POCN (Cisco and MS) currently documented in the RMX 7.7 release notes.
Using Polycom®-Enabled Unified Communications with Microsoft® Lync™ Server 2010

Required Solution Hardware

Hardware and Software Dependencies

- Lync Server 2010
- Lync Server 2010 Cumulative Update 3

Getting Help and Support Resources

This partner solution guide includes a
Using Polycom®-Enabled Unified Communications with Microsoft® Lync™ Server 2010

This chapter provides an overview of the Polycom®-enabled unified communications solution for Microsoft® Lync™ Server 2010 environments. Lync Server 2010 provides 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 discusses details of Lync Server 2010 features.

Note: Using Microsoft Lync

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

This section includes the following tasks:

- Features of the Polycom-Enabled Lync Server 2010 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 2010 Solution

Integrating Polycom products with Microsoft Lync Server 2010 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 3

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.
- Administrators also require specific knowledge of the following components of Microsoft Lync Server 2010:
  - **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 and the Polycom RMX systems 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 system.

Microsoft Real-Time Video (RTV)

Polycom HDX systems and RMX conferencing bridges include support for Microsoft’s RTV media codec and CCCP. For details on support, use, and limitations of RTV with HDX and RMX systems, and for information on the limitations of Office Communications Server 2007, see RTV Support Released for Polycom Solutions.

- 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 will need to obtain the RTV option key for the following reasons:
  - To support Lync conferencing
  - To support RTV video resolutions beyond CIF resolution using H.263 codec
  - 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 Conferencing for Outlook (PCO) or Microsoft Office Communications 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.
**Table 3-1: Polycom Products and Supported Lync Versions**

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft OCS 2007 R2</td>
<td>3.5.6907.250</td>
<td>April 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync 2010 SPO</td>
<td>4.0.7577.199</td>
<td>July 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft OC 2007 R2 Client</td>
<td>3.5.6907.261</td>
<td>October 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync 2010 Client</td>
<td>4.0.7577.4356</td>
<td>October 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync Attendee</td>
<td>4.0.7577.4109</td>
<td>October 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync Attendee Console</td>
<td>4.0.7577.4098</td>
<td>June 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync for Mac</td>
<td>14.0.2 (120223)</td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange 2007 SP3</td>
<td>8.3.264.0</td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange 2010 SP2</td>
<td>14.2.318.2</td>
<td></td>
</tr>
<tr>
<td>Microsoft Outlook 2007</td>
<td>12.0.6557.5001 SP2</td>
<td></td>
</tr>
<tr>
<td>Microsoft Outlook 2010</td>
<td>14.0.6112.5000</td>
<td></td>
</tr>
<tr>
<td>F5 BIG-IP Load Balancer 1500</td>
<td>11.2.0.2557</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 8006</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 9006</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 9004</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 7000</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 8000</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 4500</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 6000</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 4003</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom Group Series 300</td>
<td>4.0</td>
<td></td>
</tr>
<tr>
<td>Polycom Group Series 500</td>
<td>4.0 / 4.0.1</td>
<td></td>
</tr>
<tr>
<td>Polycom Group Series 700</td>
<td>4.0.1</td>
<td></td>
</tr>
<tr>
<td>Polycom RSS 4000</td>
<td>8.5.0.0</td>
<td></td>
</tr>
<tr>
<td>Polycom DMA 7000</td>
<td>5.1.0</td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Polycom RMX 4000 / 2000 MPMx</td>
<td>7.8.0</td>
<td></td>
</tr>
<tr>
<td>Polycom VBP</td>
<td>11.2.10</td>
<td></td>
</tr>
<tr>
<td>Polycom CMA 5000</td>
<td>6.2.0</td>
<td></td>
</tr>
<tr>
<td>Polycom XMA</td>
<td>7.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom CMAD (PC and Mac)</td>
<td>5.2.3</td>
<td></td>
</tr>
<tr>
<td>Polycom RealPresence Desktop</td>
<td>2.0.0</td>
<td></td>
</tr>
<tr>
<td>Polycom TPX 306</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom TPX 408</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom OTX 306</td>
<td>3.1.0</td>
<td></td>
</tr>
</tbody>
</table>
| Polycom CX100, CX200, CX500, CX600, CX700, CX5000, CX7000 | | CX100, 200 – no version number
CX500 - v4.0.7577.296
CX600 - v4.0.7577.4100
CX700 - v4.0.7577.4100 (123)
CX5000 - v1.6.5000.0
CX7000 - v1.0.2.4821 |
| Polycom Conferencing for Outlook | 1.2.0 Build 1 | |
| Polycom OCS Configurator (RMX) | 7.2.0.11 | |
| Polycom VVX 1500 | 4.1.0 | |

**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 the Polycom Conferencing for Outlook add-in.
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.

**Registered RMX User Name Dialing**

The user name dialing feature enables users in federated environments to create ad-hoc conferences. Users dial their RMX user name and use DTMF tones to enter a conference ID which can be shared by participants. RMX registered name dialing is available only in environments that include an Office Communications Server edge server and an RMX that has been registered to that edge server.

The Lync Server edge server enables remote and federated connections to the RMX system using the registered user name for dialing. The endpoint connects to the RMX system by entering the RMX registered user name in the following format:

[RMX registered user name]@[SIP domain name]

For example: vmr10@sipdomain.com

The call reaches the Transit Entry Queue of the RMX and via IVR is routed to the destination conference.

**Note: Numeric Dialing is Not Supported In Lync Server**

Numeric dialing is not supported in Lync Server environments.

**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 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 the Lync Server 2010, the Polycom video infrastructure, and Polycom HDX 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 3-1: Lync Server Environment with a Lync Server Edge Server

![Diagram of 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 edge server environment, calls are supported to the following devices:

- Polycom HDX systems
- Lync 2010 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 2010 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 3-2: 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 this 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 system and the Lync Server both need to resolve the RMX 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 3-2: Microsoft Environments with Different SIP and Active Directory Domain Namespaces**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Example</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary SIP domain for</td>
<td>sipdomain.com</td>
<td>This domain should be used as the match URI in federated environments.</td>
</tr>
<tr>
<td>Office Communications Server or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lync</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory domain</td>
<td>corp.local</td>
<td></td>
</tr>
<tr>
<td>DMA system FQDN</td>
<td>dma.corp.local</td>
<td>DMA virtual signaling IP address. FQDN must match security certificate</td>
</tr>
<tr>
<td>RMX system FQDN</td>
<td>rmx.corp.local</td>
<td>RMX SIP signaling IP address. FQDN used for DNS must match security certificate.</td>
</tr>
<tr>
<td>Additional RMX system FQDN</td>
<td>rmx2.corp.local</td>
<td>RMX SIP signaling IP address. FQDN used for DNS must match security certificate.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td><strong>Example</strong></td>
<td><strong>Usage Notes</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application Pool</td>
<td>video.corp.local</td>
<td>Make this domain a friendly name for users to use to dial into conferences. Does not need DNS representation.</td>
</tr>
</tbody>
</table>
Chapter 2: Deploying Polycom® HDX Systems

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

This section contains the following major tasks:

- Configuring Lync Server 2010 for use with an HDX System
- Register Polycom HDX System with the Lync Server
- Supporting Microsoft Real-Time Video (RTV)

Configuring Lync Server 2010 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 2010. Talk to your Microsoft Active Directory and Lync Server administrators or visit Preparing Active Directory Domain Services for Lync Server 2010.

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 or Office Communications 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 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 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. For details on support, use, and limitations of RTV with HDX and RMX systems, and for information on the limitations of Office communications server 2007, see [RTV Support Released for Polycom Solutions](#).

**To change the default video settings for your Lync Server:**

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 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 Conferencing 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 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:

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 2010, 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 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). 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 CIF resolution. If you want to support video graphics array (VGA), high-definition 720p video, or Lync multi-party calling, on your HDX system, you will need to purchase and install an RTV option key before configuring your HDX system.
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 the Office Communications Server or 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 next. Note that the field Sign-in Address is labeled User Name when you install the RTV option key.
Click Update.

Once the Polycom HDX system registers with Lync Server 2010, 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 server (Lync or Office Communications Server) configuration is set up for automatic discovery, which requires you to correctly configure Lync SRV records. If Microsoft server (Lync or Office Communications 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 or Office Communications 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.

### Configuring the Polycom HDX System LAN Properties

To register with Lync Server 2010, the Polycom HDX system 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 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 server (Lync or Office Communications 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 > General Settings > Security**.
3. In the AES Encryption drop-down menu, select **When Available** or **Required**.

**Supporting Lync-hosted Video Conferencing**

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, 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 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.

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 2010, 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 4-1: Managing Participants in a Lync-hosted Call

<table>
<thead>
<tr>
<th>Role</th>
<th>Add a Participant</th>
<th>View Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizer</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Presenter</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Attendee</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>
Table 4-2: Managing a Lync-hosted Call

<table>
<thead>
<tr>
<th>Role</th>
<th>Remove a Participant</th>
<th>End a Conference</th>
<th>Leave a Conference</th>
<th>Mute a Participant</th>
<th>Mute a Conference</th>
<th>Mute Self</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizer</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Presenter</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Attendee</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

Supporting Microsoft Real-Time Video (RTV)

Microsoft clients, including Office Communicator and Lync client, 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 or an Office Communications Server.

If you do not use RTV, Microsoft clients use H.263, CIF resolution, and do not support multi-party conference calls.

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 an HDX system that does not have the RTV key are hosted on the HDX system’s internal multipoint control unit (MCU) and do not use RTV. If a Lync client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Microsoft 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.
Chapter 3: 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 2010 and the Polycom ITP system.

This section contains the following major topics:

- Configuring Lync Server 2010 for use with a Polycom ITP System
- Configuring Your Polycom ITP System for Lync Server
- Supporting Real-Time Video (RTV)

Configuring Lync Server 2010 for use with a Polycom ITP System

When configuring your Microsoft environment, complete the following tasks:

- Configuring Authentication in Lync Server
- Configuring Microsoft Call Admission Control
- Enabling High-Definition (HD) Video on the Lync Server
- Creating and Enabling Conference Room User Accounts
- Hiding the Secondary Codecs in the Lync Directory
- Enabling Conference Room Access for Remote and Federated Users

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 or Office Communications Server. 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 1500/2000/4000 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+Content™.
- 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:**

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 6-1.

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>
<thead>
<tr>
<th>Codec</th>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary codec</td>
<td><code>&lt;name&gt;itp&lt;number_of_codecs&gt;@&lt;domain&gt;</code></td>
<td><code>vineyarditp4@abc.com</code></td>
</tr>
</tbody>
</table>
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 Conferencing for Outlook, additional considerations apply when creating this user account. See 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 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:**

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.

![Vineyard2 Properties](image)

5 Click **OK**.

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

Active Directory Service Interfaces Editor (ADSI 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:

- Configuring Your Polycom ITP System for 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 the Office Communications Server or 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 server (Lync or Office Communications Server) configuration is set up for automatic discovery. If Microsoft server (Lync or Office Communications 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 or Office Communications 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)

Microsoft clients, including Office Communicator and Lync client, 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 or an Office Communications Server.

Without RTV support, Microsoft clients receive lesser quality video.

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 client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Microsoft 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.
Chapter 4: Deploying Polycom® RMX Systems

Integrating your Polycom® RMX system with Lync™ Server 2010 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 2010 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 edge server, see Supporting Remote and Federated Users in Lync Server Environments on page 13.

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, the Polycom RMX SIP signaling domain must be accessible via a DNS server for Lync Server 2010. 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.

![New Host dialog](image)

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**.

![Select Computer screenshot](image)

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**.

![Certificate Export Wizard screenshot](image)

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, refer to Configuring Encryption Settings for Integration with Microsoft Lync Server 2010 in 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:

   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 RMX 1500/2000/4000 system can host multiple video endpoints in a single conference and host multiple conferences simultaneously. To accommodate these features, you need to configure your RMX 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 or Office Communications 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 > 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 > 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 > 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 > 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.
   ```powershell
   $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:
   ```powershell
   Set-CsStaticRoutingConfiguration -identity global -route@{Add=$route}
   
   4. Optional. To check that the commands were entered correctly in the PowerShell, enter:
   ```powershell
   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 3: Enable the RMX Account for Remote Access and Federation

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:**

2. Enter the user name and password as configured in the Lync Server and click **OK**. The Microsoft Lync Server 2010 Control Panel dialog opens.
3. Click the **Users** tab.
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.

![Image of Generate user SIP URI](image)

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 2010, 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.

![SIP Registration Properties](image)

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, go 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.

![New Meeting Room](image)

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 RMX System 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 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 > 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 2010 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 2010 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) 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.

![IP Network Service Properties](image)

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=ICE`
- `PRESERVE_ICE_CHANNEL_IN_CASE_OF_LOCAL_MODE=YES`

For more information about configuring RMX system flags, see the Polycom RealPresence Collaboration Server (RMX) 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.
Chapter 5: 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

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:

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.
   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 > 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.

```powershell
$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:

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

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

   ```powershell
   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 > 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.

   ```powershell
   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 > Lync Server Management Shell to open the Lync PowerShell terminal.

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

   ```bash
   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 edge server to your environment. Instructions on how to configure a Lync Server 2010 edge server are available at Microsoft Deploying Edge Servers.

Microsoft provides a Lync Server 2010 Planning Tool, which gets you started with 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 2010:

- 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.

![Server Certificates under IIS](image)

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

![Create Domain Certificate in Actions pane](image)

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**.

![Select Computer dialog](image)

- d 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**.

![Certificate Export Wizard](image)

   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 or Microsoft Office Communications 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.

**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 Address field, type the FQDN address of the Microsoft server (Office Communications Server or Lync Server).

9 In the Port field, enter the SIP port to use. Use the default SIP port of 5061.

10 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.

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

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

13 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.

14 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 for more information.
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**.
Chapter 6: Polycom®-Enabled Unified Communications for Microsoft® Office Communications Server

This chapter shows you how to implement Polycom®-enabled unified communications (UC), which integrates Polycom systems with the Microsoft® infrastructure for presence-based, real-time instant messaging (IM), voice, video, and data communications. In addition, this chapter shows you how to configure the Microsoft Office Communications Server components and integrate and configure the Polycom components required for this solution.

UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. Polycom Implementation and Maintenance services provide 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 its certified Partners, to help customers successfully design, deploy, optimize and manage Polycom visual communication within their third-party UC environments.

Visit Polycom Services contact your local Polycom representative for more information.

This chapter shows you how to implement Polycom UC and includes the following sections:

- Understanding Microsoft Office Communications Server Environments
- Deploying Office Communications Server
- Deploying Polycom HDX Systems with Office Communications Server
- Deploying Polycom Immersive Telepresence (ITP) Systems with Office Communications Server
- Deploying Polycom RMX Systems with Office Communications Server
- Deploying Polycom DMA System with Office Communications Server
- Setting Up Dialing Plans

Understanding Microsoft Office Communications Server Environments

This section defines the main features of and key concepts in Microsoft Office Communications Server environments, and lists Polycom products that you can integrate with Office Communications Server.
Features Available with Office Communications Server

Polycom products provide the following features when integrated with Microsoft Office Communication Server:

- Point-to-point calls between Polycom HDX systems and Microsoft communicator clients
- Real-time presence information between Polycom devices and Microsoft Communicator clients
- Support for remote and federated endpoints to participate in point-to-point calls and video conference calls
- High-quality video (720p) between Office Communicator clients and Polycom endpoints
- Enables Microsoft Communicator clients to view the presence for Polycom RMX meeting rooms and start one-click conferences
- Optionally, one-click conferencing from Office Communicator clients to an RMX system. Contact Polycom technical support for more information on this feature.

Key Concepts

Polycom products include native support for Microsoft environments. This means that Polycom components can participate in Microsoft domains, use similar security tools, and easily be enabled to participate in calls hosted by a Microsoft Office Communications Server. This section defines several of these key concepts you will need to know when operating in a Microsoft Office Communications Server environment.

Microsoft Domain Accounts

In order to participate in calls with Microsoft Communicator clients, Polycom components must have an account in a Windows domain accessible by the Office Communications Server domain. This domain can either be an Active Directory domain or an Office Communications Server domain. You will need to configure settings at the domain level with policies and some at the account level.

Encryption and Security

You need to configure TLS security certificates to operate this solution in a Microsoft environment, which means security certificates must be used.

You have the option of configuring call encryption. Encryption settings between the Office Communications Server and Polycom components need to be compatible for calls to succeed.

Remote and Federated Users

You can register Polycom components to your Microsoft Office Communications Server edge server to support remote and federated users.

Polycom Products you can Integrate with Office Communications Server

The following table lists Polycom UC products that you can successfully integrate with Office Communications Server.
### Table 8-1: Polycom Products that Support Unified Communications with Microsoft.

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Systems</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polycom RMX 1500, 2000 or 4000 system</td>
<td>v7.6</td>
<td>Provides MCU conferencing resources. MPMx cards are required to support standard definition (VGA) and high-definition (720p) calls between Microsoft clients and the RMX system. 1 GB controller board required for Edge Server support. Prior to RMX v7.2, edge server support is not supported on MPMx cards.</td>
</tr>
<tr>
<td>Polycom DMA 7000 system</td>
<td>v4.0</td>
<td>Virtualizes MCU conferencing resources. Highly recommended for deployments that include two or more Polycom RMX systems.</td>
</tr>
<tr>
<td>Polycom CMA 4000 or 5000 system</td>
<td>v6.0</td>
<td>Enables automatic provisioning of Polycom HDX endpoint systems. Recommended for remote management of endpoints.</td>
</tr>
<tr>
<td><strong>Endpoints</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Polycom HDX system                           | v3.0.3  | Video endpoint systems that can be integrated into a Microsoft environment. Advance Microsoft Support
RTV video requires an RTV option key as well as the one of the following HDX hardware versions:
- Polycom HDX 4000 (hardware version C)
- Polycom HDX 4500
- Polycom HDX 6000
- Polycom HDX 7000 (hardware version C)
- Polycom HDX 8000 (hardware version B)
- Polycom HDX 9006 |
| Polycom Immersive Telepresence (ITP) systems | v3.0.3  | Telepresence endpoint systems that can be integrated into a Microsoft environment.  
- Polycom RPX 200 and 400 systems  
- Polycom OTX 300 and 100 systems  
- Polycom TPX 306M system  
- Polycom ATX SDK and ATX 300 system |
### Product, Version, Description

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom CX100, 200, 300, 700, and 5000</td>
<td>All</td>
<td>Voice endpoint systems that can be integrated into a Microsoft environment.</td>
</tr>
</tbody>
</table>

### Peripherals

<table>
<thead>
<tr>
<th>Peripheral</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Touch Control</td>
<td>1.3.0</td>
<td>Provides HDX call control and administration.</td>
</tr>
</tbody>
</table>

### Note: Using Enterprise Voice with Office Communications Server

If you are deploying Polycom CX700, CX500, CX300 or CX3000 phones, you must implement the Enterprise Voice option in Office Communications Server and enable users for Enterprise Voice. See Microsoft’s Office Communications Server 2007 Enterprise Voice Planning and Deployment Guide.

### Deploying Office Communications Server

This section explains how to configure Office Communications Server for this solution. Before proceeding, you need to configure your Microsoft Office Communicator in Microsoft Active Directory and Microsoft Office Communications Server.

You must perform the following seven tasks in order:

1. **Task 1: Implementing Requirements for Office Communications Server**
2. **Task 2: Configure Authentication in Office Communications Server**
3. **Task 3: Add Conference Rooms with Polycom HDX Systems to Active Directory**
4. **Task 4: Enable Conference Rooms for the Office Communications Server**
5. **Task 5: Enable Conference Rooms for Remote Access and Federation**
6. **Task 6: Add Contacts to the Conference Room Local Address Book**
7. **Task 7: Configure the Office Communications Server Pool Encryption Setting**

#### Task 1: Implementing Requirements for Office Communications Server

Implementing this solution requires you to have:

- Prior knowledge and experience with Office Communications Server components
- Access to Office Communications Server product documentation and relevant software
- Prior knowledge and experience with the Polycom RMX 2000/4000 system and HDX systems
• Access to Polycom RMX 2000/4000 system and HDX system product documentation and relevant software

**Task 2: Configure Authentication in Office Communications Server**

You must enable NTLM on your Microsoft Lync or Office Communications Server. By default, NTLM is enabled in Lync Server. If NTLM has been disabled for any reason, you need to enable it.

Keep in mind that the Polycom HDX systems, Polycom ITP systems, and RMX 1500/2000/4000 systems support only NTLM authentication, and do not support Kerberos.

**To set authentication correctly in Office Communications Server:**

1. Navigate to **Start > All Programs > Administrative Tools > Office Communications Server** to open the Office Communications Server management console.

2. In the tree, expand **Enterprise pools**, right-click the server pool entry, and select **Properties > Front End Properties**. In the Front End Properties dialog, select the **Authentication** tab.

3. Set Authentication protocol to either NTLM or Both NTLM and Kerberos. Then click **OK**.

**Task 3: Add Conference Rooms with Polycom HDX Systems to Active Directory**

Each HDX system in your deployment must have 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 Conferencing 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 then **Finish**.

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

**Task 4: Enable Conference Rooms for the Office Communications Server**

After adding the conference room users to the Active Directory, you must enable and configure them for use Office Communications Server.

**To enable a conference room user for Office Communications Server 2007:**

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

2 Right-click the conference room user, and select **Enable for Communications Server**.

3 In the Enable Office Communications Server Users Wizard, select the correct server and click **Next**.

4 In the Specify Sign-in Name dialog, select the format used to generate the conference room’s SIP URI and click **Next**.

5 In the Enable Operation Status dialog, click **Finish**.

**Task 5: Enable Conference Rooms for Remote Access and Federation**

If you are supporting remote users and federated users, you need to configure users on the Office Communications Server. You need to have a properly configured Office Communications Server edge server before you can complete these steps.

**To configure a conference room user for federation and remote user access:**

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

2 Right-click the conference room user, and select **Configure Communications Server Users**.

3 In the Configure Communications Server Users wizard, click **Next**.
4 Check **Federation** if you are supporting federated users.

5 Check **Remote user access** for all deployments that include remote or federated users.

6 Click **Next** and select any additional configuration settings for your deployment.

7 When complete, click **Finish**.

**Task 6: Add Contacts to the Conference Room Local Address Book**

Office Communications Server provides real-time presence information for each contact you add. A Polycom HDX system can have up to 200 contacts per conference room user. You can use the LCSAddContacts script from the Microsoft Office Communications Server Resource Kit to add a list of contacts to the local address book of a conference room. This script accepts two text files as parameters — a file containing a user's list and a file of contacts for the users. If you used the LCSEnableConfigureUsers.wsf script to enable and configure conference room users, you can reuse the user's .txt file.

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

The HDX system displays a maximum of 200 contacts per user.

To add a list of contacts to each conference room user:

1 Create a **users.txt** file that specifies the conference room users you added and configured in Office Communications Server.
The user’s file can contain distinguished names or SIP addresses. If it contains the distinguished name of a container or user group, all the users in that container or user group are enabled and configured.

Here are some examples of user’s file entries:

```
dn:OU=HdxConfRms,DC=polycom,DC=com
dn:CN=WestConf2,CN=Users,DC=eng,DC=polycom,DC=com sip:westconf2@polycom.com
sip:westaspen@polycom.com sip:hdx4000rjones@polycom.com
```

2 Create a contacts.txt file containing the list of contacts to be added to the conference room users in the users.txt file. The contacts in the file must be active and enabled Microsoft Office Communications Server users.

For each entry in the contacts.txt file, specify the name to display in the contacts list followed by the SIP address of that contact. For example:

```
JanDuncan sip:jfduncan@polycom.com
ConfRoom1 sip:conf1@polycom.com
HelpDesk sip:helpdesk@polycom.com
```

3 If you have not already, download and install the Office Communications Server 2007 R2 Resource Kit Tools.

4 At a command prompt, navigate to the \wmisamples subdirectory in your resource kit installation. For example, `C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\wmisamples`.

5 Run the script by entering (all on one line):

```
cscript\lcsaddcontacts.wsf\usersFile:users.txt/contactsFile:contacts.txt[/contactsGroup:<contactsGroupName>] [>contactslog.txt]
```

The optional /contactsGroup parameter lets you specify a group name for the contacts you are adding. If you omit this parameter, contacts are added to the default group of All Contacts.

The script writes detailed output to the command console, showing the result of each operation for each user. Optionally, you can use the redirection operator (>), as shown above, to redirect the output to a log file.

**Task 7: Configure the Office Communications Server Pool Encryption Setting**

Office Communications Server requires encryption by default. You will need to configure support for encryption in the Office Communications Server pool and the Polycom HDX system.

Be aware that if both components have encryption turned off, calls connect without encryption. If one component supports encryption and the other does not, calls fail to connect.

To change the Pool Properties encryption setting:

1 Navigate to **Start > All Programs > Administrative Tools > Office Communications Server** to open the Office Communications Server management console.

2 In the tree, expand Enterprise pools, right-click the server pool entry, and select **Properties > Pool Properties**.
3 Change the media encryption level to the level you want to use for your deployment. Polycom recommends setting this level to **Support Encryption**.

4 Click **OK** to save your changes.

**Deploying Polycom HDX Systems with Office Communications Server**

Before integrating your Polycom HDX system with Office Communications Server, ensure that your Polycom HDX system is installed according to standard installation procedures described in the Polycom HDX System Administrator's Guide. Then perform the following tasks:

- **Task 1: Register Polycom HDX Systems with the Office Communications Server**
- **Task 2: Configure the Polycom HDX System LAN Properties**
- **Task 3: Configure Display Options for Contact List**
- **Task 4: Configure AES Encryption**

**Task 1: Register Polycom HDX Systems with the Office Communications Server**

When you register an HDX system with an Office Communications Server, the Polycom HDX system user can see a list of Office Communications Server 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 choose to configure the HDX system with or without the RTV option key. However, when used with Polycom HDX systems, the RTV option key does not enable you to participate in multi-party conference calls in OCS. The RTV option key does enable P2P HD720p.

**Note: Use the FQDN When Registering a remote HDX System**

When you are registering a remote HDX system with an Office Communications Server edge server, use the fully qualified domain name of the access edge server role.

**To configure an HDX system to register with the Office Communications 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. The IP Network screen is shown next with and without the RTV option key installed.
4 Click **Update**.

Once the Polycom HDX system registers with the Microsoft Office Communications Server, you can continue to **Task 2: Configure 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 server (Lync or Office Communications Server) configuration is set up for automatic discovery. If Microsoft server (Lync or Office Communications 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 or Office Communications 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 Principical 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.

**Task 2: Configure the Polycom HDX System LAN Properties**

To register with Office Communications Server, the Polycom HDX system must be accessible via a DNS server for the Office Communications Server (or Office Communications Server 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 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.
When you are registering a remote Polycom system, use a DNS server that shares DNS zone information with the Polycom system and the Lync Server edge server.

5 Click **Update**.

**Task 3: Configure Display Options for Contact List**

You can configure display options for the contact list.

**To configure the display options for contact list information:**

1. Open a browser window and in the HDX web user interface, 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 Microsoft 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**.

**Task 4: Configure AES Encryption**

The Polycom HDX system supports **Advanced Encryption Standard (AES)**. To use AES, you need to set your HDX system encryption settings to be compatible with your Office Communications Server settings.

Office Communications Server requires encryption by default. If you want to keep this setting, you must ensure that each of the Polycom endpoints has compatible encryption settings.

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

**To turn on AES encryption:**

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 > General Settings > Security**.

3. In the AES Encryption drop-down menu, select **When Available** or **Required**.
Deploying Polycom Immersive Telepresence (ITP) Systems with Office Communications Server

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

Configuring Office Communications Server for Use with an ITP System

When configuring your Microsoft environment, complete the following five tasks:

- Task 1: Configure Authentication on the Office Communications Server
- Task 2: Configure Microsoft Call Admission Control
- Task 3: Enable HD Video on the Office Communications Server
- Task 4: Add a Conference Room User for each Codec within your ITP System
- Task 5: Enable Conference Rooms for the Office Communications Server
- Task 6: Hiding the Secondary Codecs in the Directory
- Task 7: Enable Conference Room Users for Remote Access and Federation

Task 1: Configure Authentication on the Office Communications Server

If you want to include an ITP system, NTLM must be enabled on Office Communications Server. 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 support only NTLM authentication, and do not support Kerberos.

Task 2: Configure Microsoft Call Admission Control

Microsoft Call Admission Control policies are supported and enforced when your ITP system is registered to a Microsoft Office Communications Server edge server.

When a Microsoft Call Admission Control policy is enforced in a Microsoft Office Communications Server environment, the following limitations apply.

- SIP calls between HDX systems or ITP systems are unable to support dual-stream People+Content™.
- The maximum available bandwidth of SIP calls is 2 Mbps.

Task 3: Enable HD Video on the Office Communications Server

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

You must restart the Office Communications Server in order for these changes to take effect.
To change the default video settings for your Lync Server:

1. Open the Microsoft Communications Server console.
2. Navigate to your Server Pool.
3. Right-click the server pool and select **Properties > Front End Properties.**
4. On the Front End Properties dialog, select the Video tab.
5. In the Client video settings area of the Video tabs shown next, select **HD720p - (1.5Mbps)** from the **Maximum video quality** drop-down list.

6. Restart your Office Communications Server.

**Task 4: 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 9-1.

You must also 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 Office Communications Server. If required, you can then enable HDX users for remote access and federation.

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 8-2: ITP Naming Convention**

<table>
<thead>
<tr>
<th>Codec</th>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary codec</td>
<td>&lt;name&gt;itp&lt;number_of_codecs&gt;@&lt;domain&gt;</td>
<td><a href="mailto:vineyarditp4@abc.com">vineyarditp4@abc.com</a></td>
</tr>
</tbody>
</table>
Each ITP 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 Conferencing for Outlook, additional considerations apply when creating this user account. See Configuring Mailboxes for Room-based HDX Systems.

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 5: Enable Conference Rooms for the Office Communications Server

After adding the conference room users to the Active Directory, you must enable and configure them for use Office Communications Server.
To enable a conference room user for Office Communications Server 2007:

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

2. Right-click the conference room user, and select Enable for Communications Server.

3. In the Enable Office Communications Server Users Wizard, select the correct server and click Next.

4. In the Specify Sign-in Name dialog, select the format used to generate the conference room’s SIP URI and click Next.

5. In the Enable Operation Status dialog, click Finish.

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

**Task 6: Hiding the Secondary Codecs in the 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 Office Communications Server.

**Hide 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, shown next, select the **Hide from Exchange address lists** check box.

![Vineyard02 Properties](image)

5 Click **OK**.

**Hide 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 Choose the **Attribute Editor** tab.

5 Select the attribute named **msExchHideFromAddressLists**, and click **Edit**.

The Boolean Attribute Editor displays.

6 On the Boolean Attribute Editor dialog, select **True** in the Value field.

7 Click **OK**.

**Task 7: Enable Conference Room Users for Remote Access and Federation**

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 Office Communications 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:

- **Task 1: Register All Codecs with the Office Communications Server**
- **Task 2: Configure the LAN Properties for each Codec**
- **Task 3: Configure Display Options for the ITP System Contact List**
- **Task 4: Configure AES Encryption**

#### Task 1: Register All Codecs with the Office Communications Server

When an ITP system is registered with a Lync Server, the Polycom ITP system user can see a list of 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 the Office Communications Server or 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 next.
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 Office Communications Server, you can continue on to **Task 2: Configure 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 server (Lync or Office Communications Server) configuration is set up for automatic discovery. If Microsoft server (Lync or Office Communications 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 or Office Communications 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.

**Task 2: Configure the LAN Properties for each Codec**

To register with an Office Communications Server, each codec in your ITP room must be accessible via a DNS server for Office Communications Server (or Office Communications Server 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 Office Communications Server have in common.
To register a remote Polycom system, use a DNS server that the system has in common with the Office Communications Server edge server.

5 Click Update.

**Task 3: Configure 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.

**Task 4: Configure 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.

For Polycom ITP systems, each codec within the system 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 Real-Time Video (RTV)

Microsoft clients, including Office Communicator and Lync client, 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 or an Office Communications Server.

Without RTV support, Microsoft clients receive lesser quality video.

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 client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Microsoft 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.

Deploying Polycom RMX Systems with Office Communications Server

The RMX 2000/4000 systems can host multiple video endpoints in a single conference, as well as host multiple conferences simultaneously. To accommodate these features, you need to configure
your RMX system as a trusted application and not as a single user in the Office Communications Server.

**Supporting Remote Users**

If you need to support remote or federated users, your deployment must include an Office Communications Server edge server.

**Understanding Microsoft Domains and Application Pools**

It is important to understand how the domains are set up in your Microsoft environment. Polycom recommends following best practices when configuring your application pools within Lync Server 2010 and configuring DNS, as shown in Determine DNS Requirements.

**Using Multiple Computer Application Pools**

As a best practice, you should create a multiple trusted application pool and include your RMX system SIP signaling domains as nodes under this pool, as shown in Figure 9-1.

*Figure 8-1: Using a Multiple-computer Trusted Application Server Pool.*

In Figure 3, video.corp.local is the pool name. 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. This method simplifies your Microsoft unified communications environment and also allows you to add additional RMX systems or DMA systems at a later time.
**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 Match URI route and the destination route can be set to the same domain name, Polycom recommends using unique values for each, which 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 in the Active Directory domain.

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

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.

The following tables provide examples of a number of Microsoft environments. Table 9-4 provides example values for an environment that has different namespaces for SIP and Active Directory domains.

**Table 8-3: Namespaces for Active Directory Domain and SIP domain.**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Example</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary SIP domain for Office Communications Server or Lync</td>
<td>sipdomain.com</td>
<td>This domain should be used as the match URI in federated environments.</td>
</tr>
<tr>
<td>Active Directory domain</td>
<td>corp.local</td>
<td>Active Directory FQDN</td>
</tr>
<tr>
<td>DMA system FQDN</td>
<td>dma.corp.local</td>
<td>DMA virtual signaling IP address. FQDN must match security certificate</td>
</tr>
<tr>
<td>RMX system FQDN</td>
<td>rmx.corp.local</td>
<td>RMX SIP signaling IP address. FQDN used for DNS must match security certificate.</td>
</tr>
<tr>
<td>Additional RMX system FQDN</td>
<td>rmx2.corp.local</td>
<td>RMX SIP signaling IP address. FQDN used for DNS must match security certificate.</td>
</tr>
</tbody>
</table>
### Deploying Polycom DMA System with Office Communications Server

The Polycom DMA system can host multiple video endpoints in a single conference and host multiple conferences simultaneously. To accommodate these features, you need to configure your DMA system as a trusted application and not as a single user in the Office Communications Server.

To configure your DMA system, complete the following two major tasks:

- **Task 1: Set the Routing for the Polycom DMA 7000 System**
- **Task 2: Create a Security Certificate for the Polycom DMA 7000 System**

#### Task 1: Set the Routing for the Polycom DMA 7000 System

Set the routing to enable the Polycom DMA system to receive Office Communications Server calls.

**To set the Polycom DMA 7000 system as a trusted host with a static route:**

1. Navigate to **Start > All Programs > Administrative Tools > Office Communications Server** to open the Office Communications Server management console.
2. In the tree, expand **Enterprise** pools, right-click the server pool entry, and select **Properties > Front End Properties**.
3. In the Front End Properties dialog, select the **Host Authorization** tab and click **Add**.
   - The Add Authorized Host dialog displays.
4. Select **FQDN** and enter the fully qualified domain name associated with the Polycom DMA 7000 system’s virtual interface.

**Note: Refer to the DMA system by FQDN of its virtual interface.**

Always refer to the system by the fully qualified domain name of its virtual interface. Register only the DMAs signaling IP address in the DNS server.

5. Check **Throttle As Server** and **Treat As Authenticated** and click **OK**.
6 In the Front End Properties dialog, select the Routing tab and click Add. The Add Static Route dialog displays.

7 In the Domain field enter the fully qualified domain name to use for the Polycom DMA 7000 system.

8 To use encrypted SIP signaling, set Transport field to TLS. Then click OK.

**Note: Install a Security Certificate if you enable TLS**

If you enable TLS security, you must also install a security certificate on the Polycom DMA 7000 system and configure the system to use TLS, as shown in Task 2: Create a Security Certificate for the Polycom DMA 7000 System. In addition, you should install security certificates on your Polycom RMX systems and configure them to use TLS security, as shown in Appendix H of the Polycom RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide.

The Polycom DMA 7000 system is now set as a trusted host and now routes calls from an Office Communicator client to a SIP address in the Polycom DMA system's domain.

**Task 2: Create a Security Certificate for the Polycom DMA 7000 System**

If your solution includes a Polycom DMA 7000 system and are using TLS transport, you must install a security certificate on the Polycom DMA 7000 system so that Office Communications Server trusts it.

Before you install a security certificate, 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.

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 online help for Certificate Management to create a Certificate Signing Request and to install the certificate(s) received 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 the submission of certificate requests directly to the enterprise’s CA server, use the Office Communications Server Certificate Wizard to export the certificate to your PC and install it on the Polycom DMA system. This procedure is described below.

To request a security certificate for the Polycom DMA system using Office Communications Server:

1. In the OCS Management Console, navigate to Start > All Programs > Administrative Tools > Office Communications Server.

2. In the tree, expand Enterprise pools and the server pools list, right-click the pool front end entry, and select Certificate.

   The Office Communications Server Certificate Wizard displays.

3. Follow the steps in the wizard, making the following choices:
   a. Select Send request immediately to an online certification authority.
   b. Select Mark cert as exportable.
   c. Set Subject name to the fully-qualified domain name (FQDN) of the Polycom DMA system’s virtual interface.
   d. Enter the FQDN(s) of the physical interface(s) in the Alternate name field.
   e. Select a certificate authority from the list, choosing the local Office Communications Server front end entity.
   f. Skip assignment, selecting Assign certificate later.
   g. When done, click Finished to close the Wizard.

To export the received security certificate from Office Communications Server to your computer:

1. In the Office Communications Server tree, expand Enterprise pools and the server pools list, right-click the pool front end entry, and select Certificate.

   The Office Communications Server Certificate Wizard displays.

2. Follow the steps in the wizard, making the following choices:
   a. Select Export a certificate to a *.pfx file.
   b. Select the certificate you created for the Polycom DMA system.
   c. Specify a path and name for the *.pfx file on your computer and select Include all certificates in the certification path if possible.
d Enter a password and record it for later use.

e Click Finished to download the file and close the wizard.

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.

### Setting Up Dialing Plans

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

- **Numeric Dialing**  You assign numeric values and routes to meeting rooms and entry queues that enable users to dial a number instead of a URI. Numeric dialing configurations are enterprise-specific and not supported across federated environments.

- **Matched URI Dialing**  The user dials 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 the Polycom Conferencing for Outlook add-in.

- **RMX User Name Dialing**  Enables users in federated environments to create ad-hoc conferences. Users dial their RMX user name and use DTMF tones to enter a conference ID to be shared between participants. RMX registered name dialing is available only in environments that include an Office Communications Server edge server and an RMX that has been registered to that edge server.

### Numeric Dialing

When you enable numeric dialing for a virtual meeting room (VMR) on an RMX or DMA system, you:

- Simplify dialing by enabling HDX system users or Office Communicator users to dial a number to call into a meeting room rather than a full SIP URI.

- Enable a common dialing plan for VMRs across Office Communications Server and H.323 infrastructures. With a common dialing plan, users can to insert a single number into a calendar invitation. That number is valid for Office Communications Server endpoints and H.323 endpoints.

**Note:** You cannot use numeric dialing for federated calls.

Numeric dialing cannot be used to make calls to federated users. Typically, each enterprise has its own numeric dialing plan. Calls between federated users can be made with matched URI dialing or RMX user name dialing.
Perform the following two tasks in the Office Communications Server infrastructure to set up numeric dialing into VMRs:

- **Task 1: Configure the DMA as a Routable Gateway**
- **Task 2: Configure an Office Communications Server Voice Route to the RMX/DMA**

**Admin Tip: Removing Numeric Dialing**

You can remove numeric dialing at any time.

**Task 1: Configure the DMA as a Routable Gateway**

You must set the DMA system as a routable voice gateway in the Office Communications Server infrastructure, which enables you to set the DMA system as a destination for a voice route. This does not restrict the DMA system to voice operation.

The Office Communications Server infrastructure uses the WMI class MSFT_SIPTrustedAddInServiceSetting to store information for each voice gateway in the infrastructure. Typically, these gateways are Office Communications Server Mediation Servers. In this case, you set the DMA as a voice gateway by creating a new instance of the class MSFT_SIPTrustedAddInServiceSetting.

Polycom recommends using the Office Communications Server 2007 R2 Resource Kit Tools to create a trusted service.

**To set up the DMA as a voice gateway:**

1. If you have not already, download and install the Office Communications Server 2007 R2 Resource Kit Tools.
2. Open a command prompt and navigate to the location you installed the Office Communications Server 2007 R2 resource kit, for example C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\.
3. Run the following command:

   ```
   ```
   
   where `<your FQDN>` is the FQDN of your DMA system.

   The script automatically generates the GUID and discovers the proper Active Directory container to store the object.
Your DMA system is now established as a trusted gateway by all Office Communications Server pools in the domain and displays in the list of voice gateways when you establish a voice route.

4 Ensure that your DMA is not in the Authorized Hosts list for your Office Communications Server.

You need to set the TrustedService object you just created to be the only trusted entry for this particular DMA. For each Office Communications Server pool, you must do the following:

a From the Office Communications Server management console, navigate to your server pool.

b Right-click the pool name and select Front End Properties. Then select the Host Authorization tab.

c Make sure the same DMA system you created an TrustedService instance for is not also in the list of authorized hosts. If it is, you must completely remove the entry from the list.

Note: Changes can take up to five minutes to apply.

It may take up to five minutes for these changes to be replicated from Active Directory to the Office Communications Server repository.

Task 2: Configure an Office Communications Server Voice Route to the RMX/DMA

Next, configure the voice route to the DMA system in the Office Communications Server.

The Office Communications Server infrastructure enables you to establish a voice route to a voice gateway. Typically, this means that all SIP INVITEs to phone numbers that match a particular pattern will be routed to a specific gateway. In this example, all INVITEs to numbers starting with 73 will be routed to RMX210 (DNS name rmx210.r13.vsg.local2).

To establish a Voice Route to the RMX/DMA Voice Gateway:

1 Navigate to Start > All Programs > Administrative Tools > Office Communications Server to open the Office Communications Server management console.

2 Right-click Forest. Then select Properties > Voice Properties.

3 Select the Routes tab in the Office Communications Server Voice Properties dialog.

4 Choose Add in the Routes tab.

5 Fill in the Add Route dialog. For example, the regex expression ^73 causes this route to be applied to all numbers starting with 73.
Note: Use Regular Expressions
When establishing call routes, ensure that your expressions account for typical scenarios within your enterprise. For example, if the regex expression is ^73 and users call phone numbers with a 732 area code, these calls would fail. The example presented here assumes numbers that start with 73 are used exclusively for video calls. You can create more complex expressions that allow 73 to be used for PBX phone numbers as well. For more information about call routing expressions, see Microsoft Plan for User Authorization and Outbound Call Routing in Office Communications Server.

6 In the Add Route dialog, choose Add to set the destination gateway. The RMX gateway set up in Step 1 displays on the drop-down list of gateways.

7 In the Phone Usages section of the Add Route dialog, select a Phone Usage record for this route.

8 In the Edit Route dialog, click OK to save the route.

9 On the DMA that you set up as the gateway, create meeting rooms which start with 73, for example 73111. On the Office Communicator or DMA, dial 73111 and verify that the Office Communicator or DMA connects to the meeting room.

Remove Numeric Dialing
You can remove numeric dialing capability at any time.

To remove numeric dialing:

1 Remove any voice routes to the DMA that you defined.

2 Remove the trusted service definition you created.
   a Open a command prompt and navigate to the location you installed the Office Communications Server 2007 R2 resource kit. For example, C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\.
   b Run the following command to list each trusted service definition: cscript OCSTrustEntry.vbs /action:list /type:trustedservice
An example of a returned TrustEntry is shown next in Table 9.

### Table 8-4: Example TrustEntry

| TrustEntry[6]: CN={56A93378-FEA9-4EAE-845D-AAF0BD8073C0},CN=Trusted Services, CN=RTC Service,CN=Services,CN=Configuration, DC=ocs2, DC=eng, DC=westminster, DC=po lycom, DC=com objectClass:
| top
| contain r
| msRTCSIP-Truste dService cn: {56A93378-FEA9-4EAE-845D-AAF0BD8073C0} distinguishedName: CN={56A93378-FEA9-4EAE-845D-AAF0BD8073C0},CN=Trusted Services,CN=RTC Service,CN=Services,CN=Configuration, DC=ocs2, DC=eng, DC=westminst er, DC=polycom, DC=com instanceType: 4 (0x4)
| whenCreated: 7/2/2009 8:36:57 PM
| whenChanged: 7/2/2009 8:36:57 PM
| name: {56A93378-FEA9-4EAE-845D-AAF0BD8073C0}
| objectCategory: CN=ms-RTC-SIP-Truste dService,CN=Schema,CN=Configuration, DC=ocs2, DC=eng, DC=westminster, DC=polycom, DC=com dSCorePropagationData: 1/1/1601
| msRTCSIP-Truste dServicePort: 5073 (0x13D1)
| msRTCSIP-Truste dServerFQDN: QAOC5.ocs2.eng.westminster.polycom.
| com
| msRTCSIP-Trus te dServiceType:
| Microsoft.Rtc.Applications.Cas
| msRTCSIP-Trus te dServerVersion: 4 (0x4)
| msRTCSIP-Routa ble: True
| msRTCSIP-Extens ionData:

TlsTarget=QAOC5.ocs2.eng.westminster.polycom.com

c Find the TrustEntry that includes your FQDN and use the value of the name: property in the next step d. This is the GUID of the TrustEntry.

d Run the following command:
cscript OCSTrustEntry.vbs /action:remove /type:trustedservice /CN:<GUID>

where <GUID> is the value of the name: property of the TrustEntry you listed in the previous step c.
3 Add a Matched URI route to the DMA by right-clicking the Office Communications Server Pool, and selecting Properties > Front End Properties > Route.

4 Add a host authorization for the DMA by right-clicking the OCS Pool, and selecting Properties > Front End Properties > Host Authorization.

**Note:** Changes can take up to five minutes to apply.

It may take up to five minutes for these changes to be replicated from Active Directory to the Office Communications Server repository.

### Setting up Simultaneous Numeric and Matched URI Routing

You can set up a DMA system on the Office Communications Server to simultaneously use numeric and matched URI dialing.

Matched URI dialing requires a user 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 required to use connect links included in meeting invitations generated from the Polycom Conferencing for Outlook add-in.

To set up simultaneous use of numerical and matched URI routing:

1. Set the DMA as a trusted service (MediationServer) using the instructions in Task 1: Configure the DMA as a Routable Gateway.
2. Set up a matching URI route to the DMA by right-clicking the OCS Pool, and selecting Properties > Front End Properties > Routing tab.
3. Also set up a voice route to the same DMA using instructions in Task 1: Configure the DMA as a Routable Gateway.

**Note:** You can define only one trusted service entry for the DMA.

You cannot add a DMA system as an authorized host using the Front End Properties > Host Authorization tab. Though there are two routes to the DMA – the matched URI and voice route – you can define only one trusted service entry for the DMA. Only TLS connections to the DMA system will work. TCP connections will not work.

### Setting Up Registered RMX User Name Dialing

The Office Communications Server edge server enables you to set up remote and federated connections to the RMX system using the registered user name for dialing. The endpoint connects to the DMA system by entering the DMA registered user name in the following format:
[RMX registered user name]@[OCS domain name]

For example: rmx1234567890@ilsnd.vsg.local

The call reaches the Transit Entry Queue of the RMX and via IVR is routed to the destination conference.
Chapter 7: Supporting Remote and Federated Users for Microsoft® Office Communications Server

You can support federated or remote users by including an Office Communications Server edge server in your environment. The Office Communications Server with an access edge server role supports the Interactive Connectivity Establishment (ICE) protocol. The ICE protocol allows devices outside an organization’s network to call devices that are part of the Polycom®-enabled unified communications solution. This functionality is supported in the Microsoft Office Communications Server, the Polycom video infrastructure, and Polycom HDX systems. This configuration supports both remote and federated users.

- **Remote workers** refers to workers connecting to an organization’s firewall from outside that enterprise firewall. When registered to an enterprise’s Office Communication Server edge server, remote users can communicate with enterprise users without the use of a VPN or additional firewall traversal devices.
- **Federation** is a trust relationship between two or more SIP domains that permits users in separate organizations to communicate in real-time across networks as federated partners.
- **Federated users** are workers registered to separate enterprise Office Communications Server edge servers that are able to communicate across an external network from behind their respective firewalls.

In a Microsoft Office Communications Server edge server environment, calls are supported to the following devices:

- Polycom HDX systems
- Microsoft Office Communicator clients
- Polycom RMX systems
- Polycom DMA systems

Figure 4 illustrates an example of an edge server deployment scenario. Enterprise A and B are federated. Enterprise B has a branch office, which in this example is a Polycom HDX user behind more than one firewall. The user in the branch office can communicate to other enterprises and remote users.
In this example, users in enterprise A and B can communicate with remote users C and D. The remote users can communicate with each other and with federated users in enterprise A and B.

**Deploying Microsoft Office Communications Edge Server for Federation**

If you need more details on deploying an Office Communications Edge Server for federation, download the Edge Configuration Guide from Microsoft Office Communications Server 2007 R2 Documentation.

Microsoft also provides an Edge Server Planning Tool, available on the Edge Planning Tool for Office Communications Server 2007.

**Requirements**

Ensure that you meet the following requirements for the deployment process.

- TLS is required for federated environments and for remote users.
- You must use the Access Edge Server IP address to register Polycom devices to an Office Communications Server edge server.
Note: Federation does not support numeric dialing.
Numeric dialing is not supported for federated environments.

You need to complete the following three major steps to deploy Office Communications Server for federation:

- Deploying Microsoft Office Communications Edge Server
- Deploying RMX Systems with Office Communications Server Edge Server
- Deploying a Remote HDX System

**Deploying Microsoft Office Communications Edge Server**

Deploying the Office Communications Edge Server requires you to complete the following two tasks:

- Task 1: Configure the RMX/DMA as a Routable Gateway
- Task 2: Ensure SIP Signaling Domains are Allowed

**Task 1: Configure the RMX/DMA as a Routable Gateway**

You must set the RMX or DMA system as a routable voice gateway in the Office Communications Server infrastructure, which enables you to set the RMX or DMA system as a destination for a voice route. This does not restrict the system to voice operation.

**Note: Complete these tasks on the same network as the RMX or DMA system resides.**

Complete this task on the Office Communications Server on the network where the RMX system or DMA system resides. Perform configurations on the internal Office Communications Server, not the edge server.

The Office Communications Server infrastructure uses the WMI class MSFT_SIPTrustedAddInServiceSetting to store information for each voice gateway in the infrastructure. Typically, these gateways are Office Communications Server Mediation Servers. In this case, you set the RMX or DMA as a voice gateway by creating a new instance of the class MSFT_SIPTrustedAddInServiceSetting.

**To set up an RMX or DMA system as a voice gateway:**

1. If you have not already, download and install the Office Communications Server 2007 R2 Resource Kit Tools.
2 Open a command prompt and navigate to the location you installed the Office Communications Server 2007 R2 resource kit, for example, C:\Program Files\Microsoft Office Communications Server 2007R2\ResKit\.

3 Run the following command:


where <your FQDN> is the FQDN of your RMX or DMA system.

The script automatically generates the GUID and discovers the proper Active Directory container to store the object.

Your RMX or DMA system is now established as a trusted gateway by all Office Communications Server pools in the domain and displays in the list of voice gateways when you establish a voice route.

4 Ensure that your DMA system or RMX system is not in the Authorized Hosts list for your Office Communications Server.

   a You need to set the TrustedService object you just created to be the only trusted entry for the RMX or DMA. For each Office Communications Server pool, you must do the following:

   b From the Office Communications Server management console, navigate to your server pool.

   c Right-click the pool name and select Front End Properties. Then select the Host Authorization tab.

   d Make sure the same RMX system or DMA system you created a TrustedService instance for is not also in the list of authorized hosts. If it is, you must completely remove the entry from the list.

**Task 2: Ensure SIP Signaling Domains are Allowed**

When federating with another Office Communications Server environment that includes a Polycom RMX system or a Polycom DMA system, you need to ensure that the Office Communications Server edge server domain and the SIP signaling domain are allowed on the federated Office Communications Server edge server.

For example, if company A wants to connect to calls managed by a DMA or RMX system on company B, company A must add the company B domains to its list of allowed SIP domains in the Office Communications Server edge server.

**To federate an Office Communications Server edge server with another Office Communications Server environment:**

1 On the Office Communications Server edge server, navigate to the Computer Management console. For example, right-click My Computer and choose Manage.
2. In the console tree, expand **Computer Management > Services and Applications > Office Communications Server 2007** and right-click **Office Communications Server 2007** and then click **Properties**.

3. Click the **Internal** tab.

4. In the **Internal SIP Domains support by Office Communications Servers in your organizations**, click **Add Domain**.

5. In the Add SIP Domain dialog, add each SIP domain to be supported in your Office Communications Server 2007 deployment. In the box, type the FQDN of the SIP domain, and then click **Add**. After adding all SIP domains to be supported, click **Next**.

You need to add the following SIP domains:
- The Office Communications Server edge server you want to federate, for example, **OCS.companyB.com**.
- The SIP signaling domain of the DMA system or RMX system. For example, if you are using a DMA system, **DMA.OCS.companyname.com**. If you are using only an RMX system, use the FQDN of the RMX system. Use the following format for the FQDN of the SIP signaling domain: **RMX_DMA_NAME.OCS_EDGE_SERVER_NAME.DOMAIN.COM**.

**Note:** Configure your RMX or DMA on the network it resides on.

You must configure your RMX system or DMA system on the network it resides as a static route for Office Communications Server.

### Deploying RMX Systems with Office Communications Server Edge Server

The second major step in deploying Office Communications Edge Server for federation is to enable remote and federated connections in the Polycom RMX system. Before this, ensure that you consider the following requirements:

- The Office Communications Server Edge Server is supported only in MPM+ Card Configuration Mode.
- The firewall must be UDP enabled.
- The RMX system must have a unique account in Active Directory and must be registered with the Office Communications Server edge server.
- A TLS connection is required.

Complete the following four tasks:

- **Task 1:** Create an Active Directory Account for the RMX System
- **Task 2:** Create the RMX User Account for Office Communication Server Edge Server
Task 3: Enable the RMX Account for Remote Access and Federation

Task 4: Configure the RMX for ICE Dialing

Task 5: Add the SIP Signaling Domain to the Federated Office Communications Server Edge Server (if your deployment does not include a DMA system).

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 Office Communications Server and to automatically synchronize with the Office Communications Server edge server.

This account must be a dedicated account that is enabled for Office Communications Server. Because the RMX system has been added as a trusted application, the RMX system is able to use its trusted application configuration to register with the Office Communications 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 Object - User wizard shown next, enter the user information. Polycom recommends using 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**.
   
The new user is added to the Active Directory Users list.

**Task 2: Create the RMX User Account for Office Communication Server Edge Server**

Next, register the new RMX user you created in Active Directory with the Office Communications Server Edge Server.

**To enable the RMX User Account for Office Communication Server:**

1 In the Active Directory Users and Computers window, right-click the RMX user you created and then click **Properties**.

2 In the Properties dialog, click the **Communications** tab.

3 In the Sign in name field, enter the RMX user name in the format `SIP:rmx user name`, for example `sip:rmx1234567890`, and select the domain name, for example, `ilsnd.vsg.local`.

4 Select the Server or Pool from the list.

5 Click **Apply** and **OK**.

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

You need to configure the RMX user account for remote access and federation. The following instructions assume you have configured an Office Communications Server edge server.

**To configure the RMX account for federation and remote user access:**

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

2 Right-click the conference room user, and select **Configure Communications Server Users**.

3 In the **Configure Communications Server Users** wizard, click **Next**.
4 In the Configure User Settings page, mark the Federation and Remote user access check boxes.

○ Remote user access is required for all deployments that include remote or federated users.

○ Federation is only required when you are supporting federated users.

5 Click Next and select any additional configuration settings for your deployment.

6 When complete, click Finish.

Task 4: Configure the RMX for ICE Dialing

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

Before you begin this task, ensure that you meet the following requirements:

- The RMX must be configured to work in Microsoft environment. Set the MS_ENVIRONMENT flag to YES.
- The IP Network Service is set to work with Office Communications Server as the SIP Server
- The TLS certificate must be installed.

For a detailed description of these requirements, see Appendix H of the Polycom RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator's Guide.

To configure the RMX for ICE 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 Make sure that the following registration options are not selected:
   - Ongoing Conferences
   - Meeting Rooms
   - Gateway Profiles
   - Entry Queues
   - SIP factories

5 Specify the IP address of the Office Communications Server 2007 edge server and ensure that the Server Domain Name is the same name you defined in the Office Communications Server edge server and in the Management Network for the DNS.

6 Click the **SIP Advanced** tab.

7 In the Server User Name field, enter the RMX User name you defined in the Active Directory, for example, enter `rmx1234567890`.

8 In the ICE Environment field, select **MS** to enable Microsoft ICE implementation.

9 Click **OK**.

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

---

**Task 5: Add the SIP Signaling Domain to the Federated Office Communications Server Edge Server**

If your deployment does not include a DMA system, you must add the RMX SIP signaling domain to the Office Communications Server edge server in the enterprise you are federating, as shown in **Task 2: Ensure SIP Signaling Domains are Allowed**.

**Monitor 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.
Deploying a Remote HDX System

Office Communications Server edge server supports remote HDX system users. You need to register the remote HDX systems with the edge server to enable users to communicate across their separate networks.

If remote HDX system users are using a virtual private network (VPN), they can register directly to an Office Communications Server and no edge server is required.

Requirements for Deploying a Remote HDX System

- Polycom HDX systems are automatically provisioned to support ICE in SIP calls during registration with the Office Communications Server. No additional provisioning or configuration is required.
- Calls over an Office Communications Server edge server support call rates of up to 1564 kbps.
- People + Content (H.239) is supported in SIP calls that have ICE enabled only if the users are communicating within the same network and firewall.
- The Polycom HDX supports a single video stream - either People Video or Content Video. People + Content (H.239 / Dual Streams) is not supported and Content Video is sent over the People Channel.
- The Polycom HDX system cannot detect presence for federated contacts.
- A TLS connection is required.

To register an HDX system to an Office Communications Server edge server:

1. Use the instructions on Deploying Polycom® HDX Systems with the following consideration:
   - If you are registering a remote HDX system with an Office Communications Server edge server, use the FQDN of the access edge server role.
Chapter 8: Polycom® Conferencing for Microsoft® Outlook

Polycom Conferencing for Microsoft® 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 Conferencing for Outlook feature, and shows you how to deploy Polycom® Conferencing for Microsoft 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 Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations.

Please see Polycom Services or contact your local Polycom representative for more information.

This chapter includes the following sections:
- Polycom Products for Use with Conferencing for Outlook
- Microsoft Products for Use with Conferencing for Outlook
- Deploying Polycom Conferencing for Outlook

Polycom Products for Use with Conferencing for Outlook

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

Table 10-1: Polycom Products for Use with Conferencing for Outlook

<table>
<thead>
<tr>
<th>System</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Conferencing Add-in for Outlook</td>
<td>v1.0.3</td>
<td>Allows Outlook users to schedule meetings that include video, audio, and recording. Allows invitees to join a video-enabled meeting by clicking a link.</td>
</tr>
<tr>
<td>System</td>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Polycom HDX systems</td>
<td>v3.0.3</td>
<td>Monitor the Microsoft Exchange calendar of the configured account and display on-screen notifications of meetings. Users can join meetings via these notifications.</td>
</tr>
<tr>
<td>Polycom RMX 2000 or 4000 systems</td>
<td>v7.6</td>
<td>Monitors the Exchange mailbox for the Polycom Conferencing service and hosts Polycom Conferencing for Outlook conferences. Displays meeting information at the start of a meeting, called the Gathering Phase. 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 to RMX system v7.1.</td>
</tr>
<tr>
<td>Polycom CMA 4000 or 5000 system</td>
<td>v6.0</td>
<td>Provisions Polycom HDX systems for Polycom Conferencing for Outlook functionality and routes H.323 calls to the appropriate Polycom RMX or DMA system.</td>
</tr>
<tr>
<td>Polycom CMA Desktop</td>
<td>v5.2</td>
<td>Allows users to join video-enabled meetings by clicking a link in a meeting invitation.</td>
</tr>
<tr>
<td>Polycom DMA 7000 system</td>
<td>v4.0</td>
<td>Monitors the Exchange mailbox for the Polycom Conferencing service and determines the appropriate Polycom RMX system to host a given Polycom Conferencing for Outlook conference.</td>
</tr>
<tr>
<td>Polycom RSS 4000 system</td>
<td>v7.0</td>
<td>Via a connection from the Polycom RMX system, records Polycom Conferencing for Outlook conferences in H.323 format when selected in the Polycom Conferencing Add-in.</td>
</tr>
<tr>
<td>Polycom VBP-S/T system</td>
<td>v11.2.3</td>
<td>Enables H.323 Polycom HDX systems to support Polycom Conferencing for Outlook in a remote small office/home office (SOHO) network.</td>
</tr>
</tbody>
</table>
Microsoft Products for Use with Conferencing for Outlook

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

**Table 10-2: Microsoft Products for Use with Conferencing for Outlook**

<table>
<thead>
<tr>
<th>System</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Active Directory</td>
<td>2003 or 2008</td>
<td>Enables account logins and integrates with Microsoft Exchange.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note that Polycom products currently support only a single-forest Active Directory deployment.</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td>2007 with SP2 2010</td>
<td></td>
</tr>
<tr>
<td>Microsoft Lync Server</td>
<td>2010 2010 Cumulative Update 3</td>
<td>Provides presence-based real-time instant messaging (IM), voice, video, and data communications.</td>
</tr>
<tr>
<td>Microsoft Lync (client)</td>
<td>2010</td>
<td>Can join video-enabled meetings by clicking a link in a meeting invitation.</td>
</tr>
<tr>
<td>Microsoft Office Communications Server</td>
<td>2007 R2</td>
<td>Provides presence-based real-time instant messaging (IM), voice, video, and data communications.</td>
</tr>
<tr>
<td>Microsoft Office Communicator client</td>
<td>2007</td>
<td>Can join video-enabled meetings by clicking a link in a meeting invitation.</td>
</tr>
<tr>
<td>DNS</td>
<td>N/A</td>
<td>Permits call routing to Polycom RMX and DMA systems and DMA subscription to Exchange for mail notifications.</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>2007 2010 (32-bit only)</td>
<td>Microsoft Outlook and Microsoft Word® are required for sending Polycom Conferencing for Outlook invitations. Users of older versions of Microsoft Office can receive invitations.</td>
</tr>
</tbody>
</table>
Deploying Polycom Conferencing for Outlook

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

- Configuring DNS Entries for Polycom Devices
- Considerations for Remote Users
- Configuring the Polycom Infrastructure Mailbox and Devices
- Configuring Calendar Settings for Polycom Video Media Center (VMC)
- Configuring Mailboxes for Room-based HDX Systems
- Configure Mailboxes for Polycom HDX Desktop Systems
- Configuring HDX Mailboxes to Prevent Meeting Conflicts
- Configuring Polycom HDX System Calendar Settings
- (Optional) Configure CMA System Automatic Provisioning of Calendar Service Settings on HDX systems
- Configuring and Installing the Polycom Conferencing Add-In
- Testing Polycom Conferencing for Outlook Deployment

Configuring DNS Entries for Polycom Devices

To enable Polycom devices to work correctly with Conferencing 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.
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.

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 Conferencing for Outlook supports H.323 clients, including Polycom HDX systems, and Microsoft unified communications clients.

You can support remote users under the following conditions:

- Polycom HDX system H.323 calls are supported only if a remote Polycom HDX user is registered to a Polycom VBP-S or VBP-S/T device that proxies the Polycom HDX system’s registration to a Polycom CMA system gatekeeper inside the enterprise network.
- Polycom HDX system SIP calls are supported only if the Polycom HDX is registered to Office Communications Server via an Office Communications Server 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 system, you will need to set up your HDX 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 Conferencing 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 Conferencing Add-in for Outlook 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 Conferencing Add-in for Outlook 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 PolycomConferencing@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 Conferencing for Outlook. Figure 7 shows the General tab of the Polycom Conferencing Properties dialog, for an example of configuring a Polycom infrastructure mailbox.

Figure 10-3: 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 Systems

Configure an exchange room mailbox and an Active Directory account for each room-based HDX in your deployment.

Note: Configure Additional Settings for HDX
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, you will need to configure additional settings.

You can use the same workflows to schedule a video-enabled Polycom Conferencing 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 system monitors the exchange calendar for scheduled meetings.

You can configure a mailbox for HDX 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 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 10-3: Features Available with the HDX Room Mailbox

<table>
<thead>
<tr>
<th>Polycom Conferencing for Outlook</th>
<th>An Exchange mailbox with enabled user account</th>
<th>An Exchange mailbox with a disabled user account managed by a service account</th>
<th>Multiple Exchange mailboxes with disabled user accounts managed by a single service account</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
</tbody>
</table>
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
---|---|---
Presence | ✓ | ✓ | ✗
(either with CMA or Office Communications Server) | (only with Office Communications Server) | |
CMA Automatic Provisioning | ✓ | ✗ | ✗
CMA Softupdate | ✓ | ✗ | ✗

### Note: HDX Supports a Single Directory
Polycom HDX systems can have a single directory. If your environment includes a Polycom CMA system and Office Communications Server, presence and directory are provided by Office Communications 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 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.
   
   ```powershell
   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:
      
      ```powershell
      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:**

1. 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>\<hdxActiveDirectoryAccountUserName>' -AccessRights 'FullAccess' -InheritanceType 'All'
```

**Option 3: Associate Multiple Mailboxes with a Service Account**

You can use one service account for all Polycom HDX systems in the Polycom Conferencing 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 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>\hdxActiveDirectoryAccountUserName>' -AccessRights 'FullAccess' -InheritanceType 'All'
```

Figure 8, shown next, provides an example configuration. You can replicate this example association between Aphrodite and SRV~AllHDX~CompanyA for multiple rooms.

**Figure 10-4: Using a service account for all HDX conference rooms.**

---

**Configure Mailboxes for Polycom HDX Desktop Systems**

You need to configure HDX desktop system 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 an HDX system.
**Configuring HDX 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 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 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 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 9 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 10-5: Assigning a User Account for a Room Mailbox.**
Figure 10 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 10-6: Using a service account to manage a mailbox**
Figure 11 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 10-7: Associate Multiple Mailboxes with a Single Account**

![Configure the system for a calendaring service.

![Calendaring Service](image)

Register with Calendaring Service: ✔

Server Address: ca-exch.companya.local

Domain: companya.local

User Name: SRV-AllHDX-CompanyA

Change Password

Mailbox: (Primary SMTP) aphroditeroom@companya.com

Reminder Time in Minutes: 5

Play Reminder Tone: ✔

Show Private Meeting Information: 

Figure 12 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 10-8: User-based Calendar Settings in the Polycom HDX System**

![Configure the system for a calendaring service.

![Calendaring Service](image)

Register with Calendaring Service: ✔

Server Address: ca-exch.companya.local

Domain: companya.local

User Name: dschrute

Change Password

Mailbox: (Primary SMTP) dschrute@companya.com

Reminder Time in Minutes: 5

Play Reminder Tone: ✔

Show Private Meeting Information: 

145
Figure 13 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 10-9: Calendar Configuration for a SOHO User.**

(Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX 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 Conferencing Add-In

The Polycom Conferencing Add-In software and its templates must be installed on each Microsoft Outlook client.
Supporting Remote and Federated Users for Microsoft® Office Communications Server

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

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

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

**Task 1: Configure Polycom Conferencing Add-in Preferences for Installation to Client PCs**

You can configure the client experience of the Polycom Conferencing 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 Conferencing Add-In* in the Polycom Unified Communications Deployment Guide for Microsoft Environments.

**Task 2: Install Polycom Conferencing Add-in for Outlook to Client PCs**

You can install the conferencing 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 Conferencing 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 Conferencing Add-In* in the Polycom Unified Communications Deployment Guide for Microsoft Environments.

**Testing Polycom Conferencing 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.
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 A-0-1: Polycom HDX .dat Files

<table>
<thead>
<tr>
<th>.dat File Name</th>
<th>Description</th>
<th>Value Range</th>
<th>Content Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>langwithcntry</td>
<td>Language and country</td>
<td>Text string</td>
<td>English/en</td>
</tr>
<tr>
<td>connecttomylan</td>
<td>Enable or disable LAN interface</td>
<td>False, True</td>
<td></td>
</tr>
<tr>
<td>lanportspeed</td>
<td>LAN speed</td>
<td>Auto, 10_Mbps, 100_Mbps, 1000_Mbps</td>
<td></td>
</tr>
<tr>
<td>landuplexmode</td>
<td>LAN duplex</td>
<td>Auto, Full, Half</td>
<td></td>
</tr>
<tr>
<td>dot1xenabled</td>
<td>Enable or disable 802.1X</td>
<td>False, True</td>
<td></td>
</tr>
<tr>
<td></td>
<td>authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dot1xid</td>
<td>802.1X authentication user id</td>
<td>Text string</td>
<td>johnsmith</td>
</tr>
<tr>
<td>dot1xpwd</td>
<td>802.1X authentication password</td>
<td>Text string</td>
<td>johnsmithpassword</td>
</tr>
<tr>
<td>vlanmode</td>
<td>Enable or disable VLAN</td>
<td>False, True</td>
<td></td>
</tr>
<tr>
<td>.dat File Name</td>
<td>Description</td>
<td>Value Range</td>
<td>Content Example</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>vlanid</td>
<td>VLAN ID</td>
<td>Integer in [2,4094]</td>
<td>100</td>
</tr>
<tr>
<td>dhcp_flg</td>
<td>Enable or disable DHCP client</td>
<td>Client, Off</td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td>Host name of the Polycom HDX</td>
<td>Text string</td>
<td>hdx334</td>
</tr>
<tr>
<td>userdomain</td>
<td>Domain of the user account used to log into the</td>
<td>Text string</td>
<td>polycom.com</td>
</tr>
<tr>
<td>domainname</td>
<td>Domain of the Polycom HDX system, which will be set by the network itself if DCHP is not provisioned</td>
<td>Text string</td>
<td></td>
</tr>
<tr>
<td>ipaddress</td>
<td>IP address of the Polycom HDX</td>
<td>IP address</td>
<td>172.18.1.222</td>
</tr>
<tr>
<td>subnetmask</td>
<td>Subnet mask of the Polycom HDX</td>
<td></td>
<td>255.255.255.192</td>
</tr>
<tr>
<td>defaultgateway</td>
<td>IP address of the default</td>
<td>IP address</td>
<td>172.18.1.65</td>
</tr>
<tr>
<td>dnsserver</td>
<td>DNS server</td>
<td>IP address</td>
<td>172.18.1.15</td>
</tr>
<tr>
<td>dnsserver1</td>
<td>Alternate DNS server</td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>dnsserver2</td>
<td>Alternate DNS server</td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>dnsserver3</td>
<td>Alternate DNS server</td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>provisionserveraddress</td>
<td>IP address of the Polycom CMA</td>
<td>IP address or host name</td>
<td>polycomCMA.polycom.com</td>
</tr>
<tr>
<td>ldapuserid</td>
<td>LDAP user id</td>
<td>Text string</td>
<td>johnsmith</td>
</tr>
<tr>
<td>ldappassword</td>
<td>LDAP password</td>
<td>Text string</td>
<td>johnsmithpassword</td>
</tr>
</tbody>
</table>
Appendix B: Exchange Calendar Polling Information

This appendix provides information on Exchange Calendar Polling.

Polycom HDX System

When actively viewing the endpoint's calendar onscreen, the Polycom HDX system polls the Exchange server for updates every 20 seconds. When viewing any other screen, or when the Polycom HDX 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 Conferencing 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.

**Why can’t I join or conferences hosted on Lync with my HDX?**

In both OCS releases, Microsoft chose to use different versions of ICE between the Front End server (ICE v6) and the Edge server (ICE v19), as explained in Media Port Range for Office Communications Server 2007 R2. In contrast, Lync Server 2010 uses ICE v19 throughout the entire product line. Because the Polycom implementation of CCCP is compatible only with the current ICE v19 used in Lync Server, an HDX will not be able to join conferences hosted on an OCS AVMCU. In this scenario, an HDX can join conferences hosted on the Lync AVMCU, as explained in RTV Support Released for Polycom Solutions.

**I am no longer able to access the Polycom Conferencing Add-In**

The Polycom Conferencing Add-In can become disabled. If this occurs, navigate to Help > Disabled Items in Microsoft Outlook and enable the Polycom Conferencing Add-In again.

**Polycom HDX 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 system**

In an Office Communications Server deployment, you must enable HDX users for remote access and federation as shown in Task 5: Enable Conference Rooms 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 do so from http://www.slproweb.com/products/Win32OpenSSL.html

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 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.
Chapter 9: Polycom® Unified Communications for Microsoft®

This chapter provides an overview of Polycom® Unified Communications and an overview of Polycom Conferencing for Microsoft® Outlook.

The Polycom Unified Communications solution for Microsoft is enabled by an integrated 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 Conferencing for Microsoft Outlook** offers an integrated and enhanced calendaring experience for both Polycom and Microsoft endpoints.

**Polycom-Enabled Unified Communications**

Polycom Unified Communications (UC) software 4.1.0 enables you to deploy your Polycom video infrastructure and endpoints with Microsoft Office Communications Server (OCS) or Lync Server 2010. The Microsoft Lync or Office Communications Server manages presence for each registered Polycom endpoint or component. The Microsoft UC infrastructure provides full-featured video calls between Lync or Office Communicator 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 the Polycom Conferencing for Outlook Add-in
- 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 or Office Communications Server.)
- Integrate Lync or Office Communicator users into a Polycom HDX favorites list and call them directly from the list
- Employ enhanced presence features of Lync Server or Office Communications Server in a Polycom infrastructure environment
• Call a Lync or Microsoft Office Communicator user with a Companion Mode Polycom HDX system registered to the same Lync Server or Microsoft Office Communications 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 systems in a Lync Server or Office Communications Server environment. The Polycom CMA system provisions the Lync Server or Office Communications Server integration and Polycom Conferencing for Outlook settings, and the Polycom DMA system provides scalable, fault-tolerant multipoint conferencing.

• Use Polycom’s SIP expertise to integrate Lync or Office Communicator clients with your Polycom video network and endpoints in a way that requires a minimum of network administration and maintenance.

Polycom Conferencing for Microsoft Outlook

Polycom Conferencing for Microsoft Outlook is add-in for Microsoft Outlook that enables you to create meeting schedules and send instantly send meeting invitations. This feature requires the Polycom Conferencing Add-in 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 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).
• Polycom Conferencing for Outlook enables administrators to deploy scalable video infrastructure into an existing Exchange environment.
Chapter 10: Using Polycom®-Enabled Communications with Microsoft® Lync™ Server 2010

This chapter provides an overview of the Polycom®-enabled unified communications solution for Microsoft® Lync™ Server 2010 environments. Lync Server 2010 provides 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 discusses details of Lync Server 2010 features.

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

This section includes the following tasks:
- Features of the Polycom-Enabled Lync Server 2010 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 2010 Solution

Integrating Polycom products with Microsoft Lync Server 2010 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 3

**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](#).
- Administrators also require specific knowledge of the following components of Microsoft Lync Server 2010:
  - **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
Using Polycom®-Enabled Unified Communications with Microsoft® Lync™ Server 2010

- 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 and the Polycom RMX systems 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 system.

**Microsoft Real-Time Video (RTV)**

Polycom HDX systems and RMX conferencing bridges include support for Microsoft’s RTV media codec and CCCP. For details on support, use, and limitations of RTV with HDX and RMX systems, and for information on the limitations of Office Communications Server 2007, see RTV Support Released for Polycom Solutions.

- 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 will need to obtain the RTV option key for the following reasons:
  - To support Lync conferencing
  - To support RTV video resolutions beyond CIF resolution using H.263 codec
  - 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 Conferencing for Outlook (PCO) or Microsoft Office Communications 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.

Table 3-1: Polycom Products and Supported Lync Versions

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft OCS 2007 R2</td>
<td>3.5.6907.250</td>
<td>April 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync 2010 SPO</td>
<td>4.0.7577.199</td>
<td>July 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft OC 2007 R2 Client</td>
<td>3.5.6907.261</td>
<td>October 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync 2010 Client</td>
<td>4.0.7577.4356</td>
<td>October 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync Attendee</td>
<td>4.0.7577.4109</td>
<td>October 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync Attendee Console</td>
<td>4.0.7577.4098</td>
<td>June 2012 Cumulative Update</td>
</tr>
<tr>
<td>Microsoft Lync for Mac</td>
<td>14.0.2 (120223)</td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange 2007 SP3</td>
<td>8.3.264.0</td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange 2010 SP2</td>
<td>14.2.318.2</td>
<td></td>
</tr>
<tr>
<td>Microsoft Outlook 2007</td>
<td>12.0.6557.5001 SP2</td>
<td></td>
</tr>
<tr>
<td>Microsoft Outlook 2010</td>
<td>14.0.6112.5000</td>
<td></td>
</tr>
<tr>
<td>F5 BIG-IP Load Balancer 1500</td>
<td>11.2.0.2557</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 8006</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 9006</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 9004</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 7000</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 8000</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 4500</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 6000</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 4003</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom Group Series 300</td>
<td>4.0</td>
<td></td>
</tr>
<tr>
<td>Polycom Group Series 500</td>
<td>4.0 / 4.0.1</td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Polycom Group Series 700</td>
<td>4.0.1</td>
<td></td>
</tr>
<tr>
<td>Polycom RSS 4000</td>
<td>8.5.0.0</td>
<td></td>
</tr>
<tr>
<td>Polycom DMA 7000</td>
<td>5.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom RMX 4000 / 2000 MPMx</td>
<td>7.8.0</td>
<td></td>
</tr>
<tr>
<td>Polycom VBP</td>
<td>11.2.10</td>
<td></td>
</tr>
<tr>
<td>Polycom CMA 5000</td>
<td>6.2.0</td>
<td></td>
</tr>
<tr>
<td>Polycom XMA</td>
<td>7.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom CMAD (PC and Mac)</td>
<td>5.2.3</td>
<td></td>
</tr>
<tr>
<td>Polycom RealPresence Desktop</td>
<td>2.0.0</td>
<td></td>
</tr>
<tr>
<td>Polycom TPX 306</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom TPX 408</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom OTX 306</td>
<td>3.1.0</td>
<td></td>
</tr>
<tr>
<td>Polycom CX100, CX200, CX500, CX 600, CX700, CX5000, CX7000</td>
<td>CX100, 200 – no version number</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CX500 - v4.0.7577.296</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CX600 - v4.0.7577.4100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CX700 - v4.0.7577.4100 (123)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CX5000 - v1.6.5000.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CX7000 - v1.0.2.4821</td>
</tr>
<tr>
<td>Polycom Conferencing for Outlook</td>
<td>1.2.0 Build 1</td>
<td></td>
</tr>
<tr>
<td>Polycom OCS Configurator (RMX)</td>
<td>7.2.0.11</td>
<td></td>
</tr>
<tr>
<td>Polycom VVX 1500</td>
<td>4.1.0</td>
<td></td>
</tr>
</tbody>
</table>
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 the Polycom Conferencing for Outlook add-in.

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.

**Registered RMX User Name Dialing**

The user name dialing feature enables users in federated environments to create ad-hoc conferences. Users dial their RMX user name and use DTMF tones to enter a conference ID which can be shared by participants. RMX registered name dialing is available only in environments that include an Office Communications Server edge server and an RMX that has been registered to that edge server.

The Lync Server edge server enables remote and federated connections to the RMX system using the registered user name for dialing. The endpoint connects to the RMX system by entering the RMX registered user name in the following format:

[RMX registered user name]@[SIP domain name]

For example: vmr10@sipdomain.com

The call reaches the Transit Entry Queue of the RMX and via IVR is routed to the destination conference.

**Note: Numeric Dialing is Not Supported In Lync Server**

Numeric dialing is not supported in Lync Server environments.
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 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 the Lync Server 2010, the Polycom video infrastructure, and Polycom HDX 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.
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 edge server environment, calls are supported to the following devices:

- Polycom HDX systems
- Lync 2010 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 2010 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.
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 system and the Lync Server both need to resolve the RMX 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 3-2: Microsoft Environments with Different SIP and Active Directory Domain Namespaces**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Example</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary SIP domain for</td>
<td>sipdomain.com</td>
<td>This domain should be used as the match URI in federated environments.</td>
</tr>
<tr>
<td>Office Communications Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>or Lync</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory domain</td>
<td>corp.local</td>
<td></td>
</tr>
<tr>
<td>DMA system FQDN</td>
<td>dma.corp.local</td>
<td>DMA virtual signaling IP address. FQDN must match security certificate.</td>
</tr>
<tr>
<td>RMX system FQDN</td>
<td>rmx.corp.local</td>
<td>RMX SIP signaling IP address. FQDN used for DNS must match security certificate.</td>
</tr>
<tr>
<td>Additional RMX system FQDN</td>
<td>rmx2.corp.local</td>
<td>RMX SIP signaling IP address. FQDN used for DNS must match security certificate.</td>
</tr>
<tr>
<td>Application Pool</td>
<td>video.corp.local</td>
<td>Make this domain a friendly name for users to use to dial into conferences. Does not need DNS representation.</td>
</tr>
</tbody>
</table>
Chapter 11: Deploying Polycom® HDX Systems

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

This section contains the following major tasks:

- Configuring Lync Server 2010 for use with an HDX System
- Register Polycom HDX System with the Lync Server
- Supporting Microsoft Real-Time Video (RTV)

Configuring Lync Server 2010 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 2010. Talk to your Microsoft Active Directory and Lync Server administrators or visit Preparing Active Directory Domain Services for Lync Server 2010.

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 or Office Communications 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 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 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. For details on support, use, and limitations of RTV with HDX and RMX systems, and for information on the limitations of Office communications server 2007, see [RTV Support Released for Polycom Solutions](#).

**To change the default video settings for your Lync Server:**

2. Change the video settings for your Lync Server. For example,
   ```powershell
   Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M
   ```
3. Restart the 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 Conferencing 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 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](https://docs.microsoft.com/en-us/previous-versions/windows Server-systemmessage/bb255272(v=msdn.10)).

**To enable a conference room user for the Lync Server:**


2. Enable a conference room user for Lync. For example,
   ```powershell
   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 2010, see Microsoft [Configuring Support for External User Access](https://docs.microsoft.com/en-us/previous-versions/windows-server-systemmessage/bb255272(v=msdn.10)).
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). 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 CIF resolution. If you want to support video graphics array (VGA), high-definition 720p video, or Lync multi-party calling, on your HDX system, you will need to purchase and install an RTV option key before configuring your HDX system.
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 the Office Communications Server or 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 next. Note that the field Sign-in Address is labeled User Name when you install the RTV option key.
4 Click **Update**.

Once the Polycom HDX system registers with Lync Server 2010, 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 server (Lync or Office Communications Server) configuration is set up for automatic discovery, which requires you to correctly configure Lync SRV records. If Microsoft server (Lync or Office Communications 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 or Office Communications 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.

### Configuring the Polycom HDX System LAN Properties

To register with Lync Server 2010, the Polycom HDX system 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 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 server (Lync or Office Communications 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 > General Settings > Security.
3. In the AES Encryption drop-down menu, select *When Available* or *Required*.

**Supporting Lync-hosted Video Conferencing**

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, 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 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.

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 2010, 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 4-1: Managing Participants in a Lync-hosted Call

<table>
<thead>
<tr>
<th>Role</th>
<th>Add a Participant</th>
<th>View Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizer</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Presenter</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Attendee</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>
Table 4-2: Managing a Lync-hosted Call

<table>
<thead>
<tr>
<th>Role</th>
<th>Remove a Participant</th>
<th>End a Conference</th>
<th>Leave a Conference</th>
<th>Mute a Participant</th>
<th>Mute a Conference</th>
<th>Mute Self</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizer</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Presenter</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Attendee</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

Supporting Microsoft Real-Time Video (RTV)

Microsoft clients, including Office Communicator and Lync client, 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 or an Office Communications Server.

If you do not use RTV, Microsoft clients use H.263, CIF resolution, and do not support multi-party conference calls.

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 an HDX system that does not have the RTV key are hosted on the HDX system’s internal multipoint control unit (MCU) and do not use RTV. If a Lync client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Microsoft 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.
Chapter 12: 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 2010 and the Polycom ITP system.

This section contains the following major topics:

- Configuring Lync Server 2010 for use with a Polycom ITP System
- Configuring Your Polycom ITP System for Lync Server
- Supporting Real-Time Video (RTV)

Configuring Lync Server 2010 for use with a Polycom ITP System

When configuring your Microsoft environment, complete the following tasks:

- Configuring Authentication in Lync Server
- Configuring Microsoft Call Admission Control
- Enabling High-Definition (HD) Video on the Lync Server
- Creating and Enabling Conference Room User Accounts
- Hiding the Secondary Codecs in the Lync Directory
- Enabling Conference Room Access for Remote and Federated Users

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 or Office Communications Server. 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 1500/2000/4000 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+Content™.

- 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:

2. Change the video settings for your Lync Server. For example,
   ```powershell
   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 6-1.

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 5-1: ITP Naming Convention

<table>
<thead>
<tr>
<th>Codec</th>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary codec</td>
<td><code>&lt;name&gt;itp&lt;number_of_codecs&gt;@&lt;domain&gt;</code></td>
<td><code>vineyarditp4@abc.com</code></td>
</tr>
</tbody>
</table>
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 Conferencing for Outlook, additional considerations apply when creating this user account. See 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 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.

### Table: Codec Formats

<table>
<thead>
<tr>
<th>Codec</th>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary codec</td>
<td>~&lt;name&gt;itp&lt;codec_number&gt;@&lt;domain&gt;</td>
<td>~<a href="mailto:vineyarditp2@abc.com">vineyarditp2@abc.com</a></td>
</tr>
<tr>
<td>Right codec</td>
<td>~&lt;name&gt;itp&lt;codec_number&gt;@&lt;domain&gt;</td>
<td>~<a href="mailto:vineyarditp3@abc.com">vineyarditp3@abc.com</a></td>
</tr>
<tr>
<td>Left codec</td>
<td>~&lt;name&gt;itp&lt;codec_number&gt;@&lt;domain&gt;</td>
<td>~<a href="mailto:vineyarditp4@abc.com">vineyarditp4@abc.com</a></td>
</tr>
</tbody>
</table>
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:**

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.

![](image1.png)

5 Click **OK**.

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

Active Directory Service Interfaces Editor (ADSI 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**.

![Image of attribute editor](image)

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

![Image of boolean attribute editor](image)

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:

- Configuring Your Polycom ITP System for 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 the Office Communications Server or 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 server (Lync or Office Communications Server) configuration is set up for automatic discovery. If Microsoft server (Lync or Office Communications 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 or Office Communications 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)
Microsoft clients, including Office Communicator and Lync client, 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 or an Office Communications Server.

Without RTV support, Microsoft clients receive lesser quality video.

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 client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Microsoft 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.
Chapter 13: Deploying Polycom® RMX Systems

Integrating your Polycom® RMX system with Lync™ Server 2010 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 2010 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 edge server, see Supporting Remote and Federated Users in Lync Server Environments on page 13

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, the Polycom RMX SIP signaling domain must be accessible via a DNS server for Lync Server 2010. 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.

![New Host dialog](image)

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, refer to *Configuring Encryption Settings for Integration with Microsoft Lync Server 2010* in 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:

```powershell
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:

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

3 Verify your encryption settings:

```powershell
Get-CsMediaConfiguration
Identity: Global
EnableQoS : False
EncryptionLevel: SupportEncryption
EnableSiren: False
MaxVideoRateAllowed: VGA600K
```
Configuring Lync Server for use with a Polycom RMX System

The RMX 1500/2000/4000 system can host multiple video endpoints in a single conference and host multiple conferences simultaneously. To accommodate these features, you need to configure your RMX 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 or Office Communications 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 > 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 > 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 > Lync Server Management Shell to open the Lync PowerShell terminal.

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

```bash
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 > 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](#)
Deploying Polycom® RMX Systems

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

**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.

   ![New Object - User](image)

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 > Lync Server Control Panel.
   
2. Enter the user name and password as configured in the Lync Server and click OK.

3. Click the Users tab.

4. In the User Search dialog, click Enable Users.

5. Click the Add button.

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

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

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

![New Lync Server User](image)

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 2010, 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.

```
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 RMX System 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 > 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 2010 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 2010 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) 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=ICE
- PRESERVE_ICE_CHANNEL_IN_CASE_OF_LOCAL_MODE=YES

For more information about configuring RMX system flags, see the Polycom RealPresence Collaboration Server (RMX) 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.
Chapter 14: 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

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 > 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 > 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.
   ```powershell
   $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:
   ```powershell
   Set-CsStaticRoutingConfiguration -identity global -route@{Add=$route}
   ```

4. **Optional.** To check that the commands were entered correctly in the PowerShell, enter:
   ```powershell
   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 > 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.
   ```powershell
   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 > 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 edge server to your environment. Instructions on how to configure a Lync Server 2010 edge server are available at [Microsoft Deploying Edge Servers](#).

Microsoft provides a [Lync Server 2010 Planning Tool](#), which gets you started with 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 2010:

- **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.

![Image of Server Certificates under IIS](image)

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

![Image of Create Domain Certificate](image)

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

![Create Certificate dialog](image)

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**.

![Certificates snap-in dialog](image)
d On the Select Computer dialog, select **Local Computer**.

![Select Computer dialog]

- 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**.

![Certificate Export Wizard]

- 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, \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 or Microsoft Office Communications 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.

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 Address field, type the FQDN address of the Microsoft server (Office Communications Server or Lync Server).

9 In the Port field, enter the SIP port to use. Use the default SIP port of 5061.

10 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.

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

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

13 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.

14 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](#) for more information.
**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**.
Chapter 15: Polycom®-Enabled Unified Communications for Microsoft® Office Communications Server

This chapter shows you how to implement Polycom®-enabled unified communications (UC), which integrates Polycom systems with the Microsoft® infrastructure for presence-based, real-time instant messaging (IM), voice, video, and data communications. In addition, this chapter shows you how to configure the Microsoft Office Communications Server components and integrate and configure the Polycom components required for this solution.

UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. Polycom Implementation and Maintenance services provide 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 its certified Partners, to help customers successfully design, deploy, optimize and manage Polycom visual communication within their third-party UC environments.

Visit Polycom Services, contact your local Polycom representative for more information.

This chapter shows you how to implement Polycom UC and includes the following sections:

- Understanding Microsoft Office Communications Server Environments
- Deploying Office Communications Server
- Deploying Polycom HDX Systems with Office Communications Server
- Deploying Polycom Immersive Telepresence (ITP) Systems with Office Communications Server
- Deploying Polycom RMX Systems with Office Communications Server
- Deploying Polycom DMA System with Office Communications Server
- Setting Up Dialing Plans

Understanding Microsoft Office Communications Server Environments

This section defines the main features of and key concepts in Microsoft Office Communications Server environments, and lists Polycom products that you can integrate with Office Communications Server.
Features Available with Office Communications Server

Polycom products provide the following features when integrated with Microsoft Office Communication Server:

- Point-to-point calls between Polycom HDX systems and Microsoft communicator clients
- Real-time presence information between Polycom devices and Microsoft Communicator clients
- Support for remote and federated endpoints to participate in point-to-point calls and video conference calls
- High-quality video (720p) between Office Communicator clients and Polycom endpoints
- Enables Microsoft Communicator clients to view the presence for Polycom RMX meeting rooms and start one-click conferences
- Optionally, one-click conferencing from Office Communicator clients to an RMX system. Contact Polycom technical support for more information on this feature.

Key Concepts

Polycom products include native support for Microsoft environments. This means that Polycom components can participate in Microsoft domains, use similar security tools, and easily be enabled to participate in calls hosted by a Microsoft Office Communications Server. This section defines several of these key concepts you will need to know when operating in a Microsoft Office Communications Server environment.

Microsoft Domain Accounts

In order to participate in calls with Microsoft Communicator clients, Polycom components must have an account in a Windows domain accessible by the Office Communications Server domain. This domain can either be an Active Directory domain or an Office Communications Server domain. You will need to configure settings at the domain level with policies and some at the account level.

Encryption and Security

You need to configure TLS security certificates to operate this solution in a Microsoft environment, which means security certificates must be used.

You have the option of configuring call encryption. Encryption settings between the Office Communications Server and Polycom components need to be compatible for calls to succeed.

Remote and Federated Users

You can register Polycom components to your Microsoft Office Communications Server edge server to support remote and federated users.

Polycom Products you can Integrate with Office Communications Server

The following table lists Polycom UC products that you can successfully integrate with Office Communications Server.
<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Systems</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polycom RMX 1500, 2000 or 4000 system</td>
<td>v7.6</td>
<td>Provides MCU conferencing resources. MPMx cards are required to support standard definition (VGA) and high-definition (720p) calls between Microsoft clients and the RMX system. 1 GB controller board required for Edge Server support. Prior to RMX v7.2, edge server support is not supported on MPMx cards.</td>
</tr>
<tr>
<td>Polycom DMA 7000 system</td>
<td>v4.0</td>
<td>Virtualizes MCU conferencing resources. Highly recommended for deployments that include two or more Polycom RMX systems.</td>
</tr>
<tr>
<td>Polycom CMA 4000 or 5000 system</td>
<td>v6.0</td>
<td>Enables automatic provisioning of Polycom HDX endpoint systems. Recommended for remote management of endpoints.</td>
</tr>
<tr>
<td><strong>Endpoints</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polycom HDX system</td>
<td>v3.0.3</td>
<td>Video endpoint systems that can be integrated into a Microsoft environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Advance Microsoft Support</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RTV video requires an RTV option key as well as the one of the following HDX hardware versions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom HDX 4000 (hardware version C)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom HDX 4500</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom HDX 6000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom HDX 7000 (hardware version C)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom HDX 8000 (hardware version B)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom HDX 9006</td>
</tr>
<tr>
<td>Polycom Immersive Telepresence (ITP) systems</td>
<td>v3.0.3</td>
<td>Telepresence endpoint systems that can be integrated into a Microsoft environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom RPX 200 and 400 systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom OTX 300 and 100 systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom TPX 306M system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Polycom ATX SDK and ATX 300 system</td>
</tr>
</tbody>
</table>
### Product Version Description

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom CX100, 200, 300, 700, and 5000</td>
<td>All</td>
<td>Voice endpoint systems that can be integrated into a Microsoft environment.</td>
</tr>
</tbody>
</table>

### Peripherals

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Touch Control</td>
<td>1.3.0</td>
<td>Provides HDX call control and administration.</td>
</tr>
</tbody>
</table>

### Note: Using Enterprise Voice with Office Communications Server

If you are deploying Polycom CX700, CX500, CX300 or CX3000 phones, you must implement the Enterprise Voice option in Office Communications Server and enable users for Enterprise Voice. See Microsoft’s Office Communications Server 2007 Enterprise Voice Planning and Deployment Guide.

### Deploying Office Communications Server

This section explains how to configure Office Communications Server for this solution. Before proceeding, you need to configure your Microsoft Office Communicator in Microsoft Active Directory and Microsoft Office Communications Server.

You must perform the following seven tasks in order:

1. Task 1: Implementing Requirements for Office Communications Server
2. Task 2: Configure Authentication in Office Communications Server
3. Task 3: Add Conference Rooms with Polycom HDX Systems to Active Directory
4. Task 4: Enable Conference Rooms for the Office Communications Server
5. Task 5: Enable Conference Rooms for Remote Access and Federation
6. Task 6: Add Contacts to the Conference Room Local Address Book
7. Task 7: Configure the Office Communications Server Pool Encryption Setting

### Task 1: Implementing Requirements for Office Communications Server

Implementing this solution requires you to have:

- Prior knowledge and experience with Office Communications Server components
- Access to Office Communications Server product documentation and relevant software
- Prior knowledge and experience with the Polycom RMX 2000/4000 system and HDX systems
- Access to Polycom RMX 2000/4000 system and HDX system product documentation and relevant software

**Task 2: Configure Authentication in Office Communications Server**

You must enable NTLM on your Microsoft Lync or Office Communications Server. By default, NTLM is enabled in Lync Server. If NTLM has been disabled for any reason, you need to enable it. Keep in mind that the Polycom HDX systems, Polycom ITP systems, and RMX 1500/2000/4000 systems support only NTLM authentication, and do not support Kerberos.

**To set authentication correctly in Office Communications Server:**

1. Navigate to **Start > All Programs > Administrative Tools > Office Communications Server** to open the Office Communications Server management console.
2. In the tree, expand **Enterprise pools**, right-click the server pool entry, and select **Properties > Front End Properties**. In the Front End Properties dialog, select the **Authentication** tab.
3. Set Authentication protocol to either NTLM or Both NTLM and Kerberos. Then click **OK**.

**Task 3: Add Conference Rooms with Polycom HDX Systems to Active Directory**

Each HDX system in your deployment must have 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 Conferencing 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 then Finish.
6 Repeat for each conference room that has a Polycom HDX system.

**Task 4: Enable Conference Rooms for the Office Communications Server**

After adding the conference room users to the Active Directory, you must enable and configure them for use Office Communications Server.

**To enable a conference room user for Office Communications Server 2007:**

1. Go to Start > Run and open the Active Directory Users and Computers console by entering: dsa.msc.
2. Right-click the conference room user, and select Enable for Communications Server.
3. In the Enable Office Communications Server Users Wizard, select the correct server and click Next.
4. In the Specify Sign-in Name dialog, select the format used to generate the conference room’s SIP URI and click Next.
5. In the Enable Operation Status dialog, click Finish.

**Task 5: Enable Conference Rooms for Remote Access and Federation**

If you are supporting remote users and federated users, you need to configure users on the Office Communications Server. You need to have a properly configured Office Communications Server edge server before you can complete these steps.

**To configure a conference room user for federation and remote user access:**

1. Go to Start > Run and open the Active Directory Users and Computers console by entering: dsa.msc.
2. Right-click the conference room user, and select Configure Communications Server Users.
3. In the Configure Communications Server Users wizard, click Next.
The Configure User Settings page displays, as shown next.

4 Check **Federation** if you are supporting federated users.

5 Check **Remote user access** for all deployments that include remote or federated users.

6 Click **Next** and select any additional configuration settings for your deployment.

7 When complete, click **Finish**.

**Task 6: Add Contacts to the Conference Room Local Address Book**

Office Communications Server provides real-time presence information for each contact you add. A Polycom HDX system can have up to 200 contacts per conference room user. You can use the `LCSAddContacts` script from the Microsoft Office Communications Server Resource Kit to add a list of contacts to the local address book of a conference room. This script accepts two text files as parameters — a file containing a user’s list and a file of contacts for the users. If you used the `LCSEnableConfigureUsers.wsf` script to enable and configure conference room users, you can reuse the user’s `.txt` file.

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

The HDX system displays a maximum of 200 contacts per user.

To add a list of contacts to each conference room user:

1 Create a `users.txt` file that specifies the conference room users you added and configured in Office Communications Server.
The user’s file can contain distinguished names or SIP addresses. If it contains the distinguished name of a container or user group, all the users in that container or user group are enabled and configured.

Here are some examples of user’s file entries:

dn:OU=HdxConfRms,DC=polycom,DC=com
dn:CN=WestConf2,CN=Users,DC=eng,DC=polycom,DC=com sip:westconf2@polycom.com
sip:westaspen@polycom.com sip:hdx4000rjones@polycom.com

2 Create a contacts.txt file containing the list of contacts to be added to the conference room users in the users.txt file. The contacts in the file must be active and enabled Microsoft Office Communications Server users.

For each entry in the contacts.txt file, specify the name to display in the contacts list followed by the SIP address of that contact. For example:

JanDuncan sip:jfduncan@polycom.com
ConfRoom1 sip:conf1@polycom.com
HelpDesk sip:helpdesk@polycom.com

3 If you have not already, download and install the Office Communications Server 2007 R2 Resource Kit Tools.

4 At a command prompt, navigate to the \wmisamples subdirectory in your resource kit installation. For example, C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\wmisamples.

5 Run the script by entering (all on one line):

cscript lcsaddcontacts.wsf/usersFile:users.txt/contactsFile:contacts.txt [/contactsGroup:<contactsGroupName>] [>contactslog.txt]

The optional /contactsGroup parameter lets you specify a group name for the contacts you are adding. If you omit this parameter, contacts are added to the default group of All Contacts.

The script writes detailed output to the command console, showing the result of each operation for each user. Optionally, you can use the redirection operator (>), as shown above, to redirect the output to a log file.

Task 7: Configure the Office Communications Server Pool Encryption Setting

Office Communications Server requires encryption by default. You will need to configure support for encryption in the Office Communications Server pool and the Polycom HDX system.

Be aware that if both components have encryption turned off, calls connect without encryption. If one component supports encryption and the other does not, calls fail to connect.

To change the Pool Properties encryption setting:

1 Navigate to Start > All Programs > Administrative Tools > Office Communications Server to open the Office Communications Server management console.

2 In the tree, expand Enterprise pools, right-click the server pool entry, and select Properties > Pool Properties.
3. Change the media encryption level to the level you want to use for your deployment. Polycom recommends setting this level to **Support Encryption**.

4. Click **OK** to save your changes.

### Deploying Polycom HDX Systems with Office Communications Server

Before integrating your Polycom HDX system with Office Communications Server, ensure that your Polycom HDX system is installed according to standard installation procedures described in the Polycom HDX System Administrator's Guide. Then perform the following tasks:

- **Task 1: Register Polycom HDX Systems with the Office Communications Server**
- **Task 2: Configure the Polycom HDX System LAN Properties**
- **Task 3: Configure Display Options for Contact List**
- **Task 4: Configure AES Encryption**

#### Task 1: Register Polycom HDX Systems with the Office Communications Server

When you register an HDX system with an Office Communications Server, the Polycom HDX system user can see a list of Office Communications Server 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 choose to configure the HDX system with or without the RTV option key. However, when used with Polycom HDX systems, the RTV option key does not enable you to participate in multi-party conference calls in OCS. The RTV option key does enable P2P HD720p.

---

**Note: Use the FQDN When Registering a remote HDX System**

When you are registering a remote HDX system with an Office Communications Server edge server, use the fully qualified domain name of the access edge server role.

---

**To configure an HDX system to register with the Office Communications 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. The IP Network screen is shown next with and without the RTV option key installed.
4 Click **Update**.

Once the Polycom HDX system registers with the Microsoft Office Communications Server, you can continue to **Task 2: Configure 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 server (Lync or Office Communications Server) configuration is set up for automatic discovery. If Microsoft server (Lync or Office Communications Server) is not configured for automatic discovery, 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 or Office Communications 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.

**Task 2: Configure the Polycom HDX System LAN Properties**

To register with Office Communications Server, the Polycom HDX system must be accessible via a DNS server for the Office Communications Server (or Office Communications Server 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 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.
When you are registering a remote Polycom system, use a DNS server that shares DNS zone information with the Polycom system and the Lync Server edge server.

5 Click Update.

**Task 3: Configure Display Options for Contact List**

You can configure display options for the contact list.

**To configure the display options for contact list information:**

1. Open a browser window and in the HDX web user interface, 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 Microsoft 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.

**Task 4: Configure AES Encryption**

The Polycom HDX system supports Advanced Encryption Standard (AES). To use AES, you need to set your HDX system encryption settings to be compatible with your Office Communications Server settings.

Office Communications Server requires encryption by default. If you want to keep this setting, you must ensure that each of the Polycom endpoints has compatible encryption settings.

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

**To turn on AES encryption:**

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 > General Settings > Security.

3. In the AES Encryption drop-down menu, select When Available or Required.
Deploying Polycom Immersive Telepresence (ITP) Systems with Office Communications Server

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

Configuring Office Communications Server for Use with an ITP System

When configuring your Microsoft environment, complete the following five tasks:

- Task 1: Configure Authentication on the Office Communications Server
- Task 2: Configure Microsoft Call Admission Control
- Task 3: Enable HD Video on the Office Communications Server
- Task 4: Add a Conference Room User for each Codec within your ITP System
- Task 5: Enable Conference Rooms for the Office Communications Server
- Task 6: Hiding the Secondary Codecs in the Directory
- Task 7: Enable Conference Room Users for Remote Access and Federation

Task 1: Configure Authentication on the Office Communications Server

If you want to include an ITP system, NTLM must be enabled on Office Communications Server. 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 support only NTLM authentication, and do not support Kerberos.

Task 2: Configure Microsoft Call Admission Control

Microsoft Call Admission Control policies are supported and enforced when your ITP system is registered to a Microsoft Office Communications Server edge server.

When a Microsoft Call Admission Control policy is enforced in a Microsoft Office Communications Server environment, the following limitations apply.

- SIP calls between HDX systems or ITP systems are unable to support dual-stream People+Content™.
- The maximum available bandwidth of SIP calls is 2 Mbps.

Task 3: Enable HD Video on the Office Communications Server

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

You must restart the Office Communications Server in order for these changes to take effect.
To change the default video settings for your Lync Server:

1. Open the Microsoft Communications Server console.
2. Navigate to your Server Pool.
3. Right-click the server pool and select **Properties > Front End Properties**.
4. On the Front End Properties dialog, select the Video tab.
5. In the Client video settings area of the Video tabs shown next, select **HD720p - (1.5Mbps)** from the **Maximum video quality** drop-down list.

6. Restart your Office Communications Server.

**Task 4: 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 9-1.

You must also 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 Office Communications Server. If required, you can then enable HDX users for remote access and federation.

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 8-2: ITP Naming Convention**

<table>
<thead>
<tr>
<th>Codec</th>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary codec</td>
<td>&lt;name&gt;itp&lt;number_of_codecs&gt;@&lt;domain&gt;</td>
<td><a href="mailto:vineyarditp4@abc.com">vineyarditp4@abc.com</a></td>
</tr>
</tbody>
</table>
Each ITP 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 Conferencing for Outlook, additional considerations apply when creating this user account. See 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 then **Finish**.
6. Repeat for each codec within your system.

**Task 5: Enable Conference Rooms for the Office Communications Server**

After adding the conference room users to the Active Directory, you must enable and configure them for use Office Communications Server.
To enable a conference room user for Office Communications Server 2007:

1. Go to Start > Run and open the Active Directory Users and Computers console by entering: dsa.msc.
2. Right-click the conference room user, and select Enable for Communications Server.
3. In the Enable Office Communications Server Users Wizard, select the correct server and click Next.
4. In the Specify Sign-in Name dialog, select the format used to generate the conference room’s SIP URI and click Next.
5. In the Enable Operation Status dialog, click Finish.

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

Task 6: Hiding the Secondary Codecs in the 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 Office Communications Server.

Hide 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, shown next, select the **Hide from Exchange address lists** check box.

![Vineyard2 Properties](image)

5 Click **OK**.

**Hide the Secondary Codecs in the Directory Using the ADSI Edit Tool**

Active Directory Service Interfaces Editor (ADSI 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 Choose the **Attribute Editor** tab.

5 Select the attribute named **msExchHideFromAddressLists**, and click **Edit**.

The Boolean Attribute Editor displays.

6 On the Boolean Attribute Editor dialog, select **True** in the Value field.

7 Click **OK**.

**Task 7: Enable Conference Room Users for Remote Access and Federation**

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 Office Communications 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:

- Task 1: Register All Codecs with the Office Communications Server
- Task 2: Configure the LAN Properties for each Codec
- Task 3: Configure Display Options for the ITP System Contact List
- Task 4: Configure AES Encryption

Task 1: Register All Codecs with the Office Communications Server

When an ITP system is registered with a Lync Server, the Polycom ITP system user can see a list of 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 the Office Communications Server or 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 next.
Click **Update**.

Repeat these steps for each codec within your ITP room.

After you have registered each codec within your ITP room with Office Communications Server, you can continue on to **Task 2: Configure 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 server (Lync or Office Communications Server) configuration is set up for automatic discovery. If Microsoft server (Lync or Office Communications 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.
Polycom®-Enabled Unified Communications for Microsoft® Office Communications Server

- **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 or Office Communications 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.

**Task 2: Configure the LAN Properties for each Codec**

To register with an Office Communications Server, each codec in your ITP room must be accessible via a DNS server for Office Communications Server (or Office Communications Server 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 Office Communications Server have in common.
To register a remote Polycom system, use a DNS server that the system has in common with the Office Communications Server edge server.

5 Click **Update**.

**Task 3: Configure 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**.

**Task 4: Configure 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.

For Polycom ITP systems, each codec within the system 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 Real-Time Video (RTV)

Microsoft clients, including Office Communicator and Lync client, 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 or an Office Communications Server.

Without RTV support, Microsoft clients receive lesser quality video.

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 client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Microsoft 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.

Deploying Polycom RMX Systems with Office Communications Server

The RMX 2000/4000 systems can host multiple video endpoints in a single conference, as well as host multiple conferences simultaneously. To accommodate these features, you need to configure
your RMX system as a trusted application and not as a single user in the Office Communications Server.

**Supporting Remote Users**

If you need to support remote or federated users, your deployment must include an Office Communications Server edge server.

**Understanding Microsoft Domains and Application Pools**

It is important to understand how the domains are set up in your Microsoft environment. Polycom recommends following best practices when configuring your application pools within Lync Server 2010 and configuring DNS, as shown in Determine DNS Requirements.

**Using Multiple Computer Application Pools**

As a best practice, you should create a multiple trusted application pool and include your RMX system SIP signaling domains as nodes under this pool, as shown in Figure 9-1.

*Figure 8-1: Using a Multiple-computer Trusted Application Server Pool.*

In Figure 3, `video.corp.local` is the pool name. 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. This method simplifies your Microsoft unified communications environment and also allows you to add additional RMX systems or DMA systems at a later time.
**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 Match URI route and the destination route can be set to the same domain name, Polycom recommends using unique values for each, which 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 in the Active Directory domain.

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

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.

The following tables provide examples of a number of Microsoft environments. Table 9-4 provides example values for an environment that has different namespaces for SIP and Active Directory domains.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Example</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary SIP domain for Office Communications Server or Lync</td>
<td>sipdomain.com</td>
<td>This domain should be used as the match URI in federated environments.</td>
</tr>
<tr>
<td>Active Directory domain</td>
<td>corp.local</td>
<td>Active Directory FQDN</td>
</tr>
<tr>
<td>DMA system FQDN</td>
<td>dma.corp.local</td>
<td>DMA virtual signaling IP address. FQDN must match security certificate</td>
</tr>
<tr>
<td>RMX system FQDN</td>
<td>rmx.corp.local</td>
<td>RMX SIP signaling IP address. FQDN used for DNS must match security certificate.</td>
</tr>
<tr>
<td>Additional RMX system FQDN</td>
<td>rmx2.corp.local</td>
<td>RMX SIP signaling IP address. FQDN used for DNS must match security certificate.</td>
</tr>
</tbody>
</table>
### Domain Example Usage Notes

<table>
<thead>
<tr>
<th>Domain</th>
<th>Example</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Pool</td>
<td>video.corp.local</td>
<td>Make this domain a friendly name for users to use to dial into conferences. Does not need DNS representation.</td>
</tr>
</tbody>
</table>

---

### Deploying Polycom DMA System with Office Communications Server

The Polycom DMA system can host multiple video endpoints in a single conference and host multiple conferences simultaneously. To accommodate these features, you need to configure your DMA system as a trusted application and not as a single user in the Office Communications Server.

To configure your DMA system, complete the following two major tasks:

- **Task 1: Set the Routing for the Polycom DMA 7000 System**
- **Task 2: Create a Security Certificate for the Polycom DMA 7000 System**

#### Task 1: Set the Routing for the Polycom DMA 7000 System

Set the routing to enable the Polycom DMA system to receive Office Communications Server calls.

**To set the Polycom DMA 7000 system as a trusted host with a static route:**

1. Navigate to **Start > All Programs > Administrative Tools > Office Communications Server** to open the Office Communications Server management console.

2. In the tree, expand **Enterprise** pools, right-click the server pool entry, and select **Properties > Front End Properties**.

3. In the Front End Properties dialog, select the **Host Authorization** tab and click **Add**. The Add Authorized Host dialog displays.

4. Select **FQDN** and enter the fully qualified domain name associated with the Polycom DMA 7000 system’s virtual interface.

   **Note:** Refer to the DMA system by FQDN of its virtual interface. Always refer to the system by the fully qualified domain name of its virtual interface. Register only the DMAs signaling IP address in the DNS server.

---

5. Check **Throttle As Server** and **Treat As Authenticated** and click **OK**.
6 In the Front End Properties dialog, select the **Routing** tab and click **Add**. The Add Static Route dialog displays.

7 In the Domain field enter the fully qualified domain name to use for the Polycom DMA 7000 system.

8 To use encrypted SIP signaling, set Transport field to **TLS**. Then click **OK**.

**Note: Install a Security Certificate if you enable TLS**

If you enable TLS security, you must also install a security certificate on the Polycom DMA 7000 system and configure the system to use TLS, as shown in Task 2: Create a Security Certificate for the Polycom DMA 7000 System. In addition, you should install security certificates on your Polycom RMX systems and configure them to use TLS security, as shown in Appendix H of the Polycom RealPresence Collaboration Server (RMX) 1500/2000/4000 Administrator’s Guide.

The Polycom DMA 7000 system is now set as a trusted host and now routes calls from an Office Communicator client to a SIP address in the Polycom DMA system’s domain.

**Task 2: Create a Security Certificate for the Polycom DMA 7000 System**

If your solution includes a Polycom DMA 7000 system and are using TLS transport, you must install a security certificate on the Polycom DMA 7000 system so that Office Communications Server trusts it.

Before you install a security certificate, 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.

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 online help for Certificate Management to create a Certificate Signing Request and to install the certificate(s) received 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 the submission of certificate requests directly to the enterprise’s CA server, use the Office Communications Server Certificate Wizard to export the certificate to your PC and install it on the Polycom DMA system. This procedure is described below.

To request a security certificate for the Polycom DMA system using Office Communications Server:

1. In the OCS Management Console, navigate to Start > All Programs > Administrative Tools > Office Communications Server.
2. In the tree, expand Enterprise pools and the server pools list, right-click the pool front end entry, and select Certificate.
   The Office Communications Server Certificate Wizard displays.
3. Follow the steps in the wizard, making the following choices:
   a. Select Send request immediately to an online certification authority.
   b. Select Mark cert as exportable.
   c. Set Subject name to the fully-qualified domain name (FQDN) of the Polycom DMA system’s virtual interface.
   d. Enter the FQDN(s) of the physical interface(s) in the Alternate name field.
   e. Select a certificate authority from the list, choosing the local Office Communications Server front end entity.
   f. Skip assignment, selecting Assign certificate later.
   g. When done, click Finished to close the Wizard.

To export the received security certificate from Office Communications Server to your computer:

1. In the Office Communications Server tree, expand Enterprise pools and the server pools list, right-click the pool front end entry, and select Certificate.
   The Office Communications Server Certificate Wizard displays.
2. Follow the steps in the wizard, making the following choices:
   a. Select Export a certificate to a *.pfx file.
   b. Select the certificate you created for the Polycom DMA system.
   c. Specify a path and name for the *.pfx file on your computer and select Include all certificates in the certification path if possible.
d Enter a password and record it for later use.
e Click Finished to download the file and close the wizard.

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.

Setting Up Dialing Plans

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

- **Numeric Dialing**  You assign numeric values and routes to meeting rooms and entry queues that enable users to dial a number instead of a URI. Numeric dialing configurations are enterprise-specific and not supported across federated environments.

- **Matched URI Dialing**  The user dials 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 the Polycom Conferencing for Outlook add-in.

- **RMX User Name Dialing**  Enables users in federated environments to create ad-hoc conferences. Users dial their RMX user name and use DTMF tones to enter a conference ID to be shared between participants. RMX registered name dialing is available only in environments that include an Office Communications Server edge server and an RMX that has been registered to that edge server.

### Numeric Dialing

When you enable numeric dialing for a virtual meeting room (VMR) on an RMX or DMA system, you:

- Simplify dialing by enabling HDX system users or Office Communicator users to dial a number to call into a meeting room rather than a full SIP URI.

- Enable a common dialing plan for VMRs across Office Communications Server and H.323 infrastructures. With a common dialing plan, users can to insert a single number into a calendar invitation. That number is valid for Office Communications Server endpoints and H.323 endpoints.

**Note:** You cannot use numeric dialing for federated calls.

Numeric dialing cannot be used to make calls to federated users. Typically, each enterprise has its own numeric dialing plan. Calls between federated users can be made with matched URI dialing or RMX user name dialing.
Perform the following two tasks in the Office Communications Server infrastructure to set up numeric dialing into VMRs:

- **Task 1: Configure the DMA as a Routable Gateway**
- **Task 2: Configure an Office Communications Server Voice Route to the RMX/DMA**

**Admin Tip: Removing Numeric Dialing**
You can remove numeric dialing at any time.

---

**Task 1: Configure the DMA as a Routable Gateway**

You must set the DMA system as a routable voice gateway in the Office Communications Server infrastructure, which enables you to set the DMA system as a destination for a voice route. This does not restrict the DMA system to voice operation.

The Office Communications Server infrastructure uses the WMI class `MSFT_SIPTrustedAddInServiceSetting` to store information for each voice gateway in the infrastructure. Typically, these gateways are Office Communications Server Mediation Servers. In this case, you set the DMA as a voice gateway by creating a new instance of the class `MSFT_SIPTrustedAddInServiceSetting`.

Polycom recommends using the Office Communications Server 2007 R2 Resource Kit Tools to create a trusted service.

**To set up the DMA as a voice gateway:**

2. Open a command prompt and navigate to the location you installed the Office Communications Server 2007 R2 resource kit, for example `C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\`.
3. Run the following command:
   ```
   ```
   where `<your FQDN>` is the FQDN of your DMA system.
   The script automatically generates the GUID and discovers the proper Active Directory container to store the object.
Your DMA system is now established as a trusted gateway by all Office Communications Server pools in the domain and displays in the list of voice gateways when you establish a voice route.

4 Ensure that your DMA is not in the **Authorized Hosts** list for your Office Communications Server.

You need to set the **TrustedService** object you just created to be the only trusted entry for this particular DMA. For each Office Communications Server pool, you must do the following:

a From the Office Communications Server management console, navigate to your server pool.

b Right-click the pool name and select **Front End Properties**. Then select the **Host Authorization** tab.

c Make sure the same DMA system you created an TrustedService instance for is not also in the list of authorized hosts. If it is, you must completely remove the entry from the list.

**Note: Changes can take up to five minutes to apply.**

It may take up to five minutes for these changes to be replicated from Active Directory to the Office Communications Server repository.

**Task 2: Configure an Office Communications Server Voice Route to the RMX/DMA**

Next, configure the voice route to the DMA system in the Office Communications Server.

The Office Communications Server infrastructure enables you to establish a voice route to a voice gateway. Typically, this means that all SIP INVITEs to phone numbers that match a particular pattern will be routed to a specific gateway. In this example, all INVITEs to numbers starting with 73 will be routed to RMX210 (DNS name rmx210.r13.vsg.local2).

**To establish a Voice Route to the RMX/DMA Voice Gateway:**

1 Navigate to **Start > All Programs > Administrative Tools > Office Communications Server** to open the Office Communications Server management console.

2 Right-click **Forest**. Then select **Properties > Voice Properties**.

3 Select the **Routes** tab in the Office Communications Server Voice Properties dialog.

4 Choose **Add** in the Routes tab.

5 Fill in the Add Route dialog. For example, the regex expression \(^73\) causes this route to be applied to all numbers starting with 73.
Note: Use Regular Expressions
When establishing call routes, ensure that your expressions account for typical scenarios within your enterprise. For example, if the regex expression is ^73 and users call phone numbers with a 732 area code, these calls would fail. The example presented here assumes numbers that start with 73 are used exclusively for video calls. You can create more complex expressions that allow 73 to be used for PBX phone numbers as well. For more information about call routing expressions, see Microsoft Plan for User Authorization and Outbound Call Routing in Office Communications Server.

6 In the Add Route dialog, choose Add to set the destination gateway. The RMX gateway set up in Step 1 displays on the drop-down list of gateways.

7 In the Phone Usages section of the Add Route dialog, select a Phone Usage record for this route.

8 In the Edit Route dialog, click OK to save the route.

9 On the DMA that you set up as the gateway, create meeting rooms which start with 73, for example 73111. On the Office Communicator or DMA, dial 73111 and verify that the Office Communicator or DMA connects to the meeting room.

Remove Numeric Dialing
You can remove numeric dialing capability at any time.

To remove numeric dialing:

1 Remove any voice routes to the DMA that you defined.

2 Remove the trusted service definition you created.

a Open a command prompt and navigate to the location you installed the Office Communications Server 2007 R2 resource kit. For example, C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\.

b Run the following command to list each trusted service definition: cscript OCSTrustEntry.vbs /action:list /type:trustedservice
An example of a returned TrustEntry is shown next in Table 9.

Table 8-4: Example TrustEntry

<table>
<thead>
<tr>
<th>TrustEntry[6]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN={56A93378-FEA9-4EAE-845D-AAF0BD8073C0},CN=Trusted Services,</td>
</tr>
<tr>
<td>CN=RTC</td>
</tr>
<tr>
<td>Service,CN=Services,CN=Configuration,DC=ocs2,DC=eng,DC=westminster,DC=polycom,DC=com</td>
</tr>
<tr>
<td>objectClass: top</td>
</tr>
<tr>
<td>contained</td>
</tr>
<tr>
<td>msRTCSIP-TrustedService</td>
</tr>
<tr>
<td>cn: {56A93378-FEA9-4EAE-845D-AAF0BD8073C0}</td>
</tr>
<tr>
<td>distinguishedName:</td>
</tr>
<tr>
<td>CN={56A93378-FEA9-4EAE-845D-AAF0BD8073C0},CN=Trusted Services,CN=RTC</td>
</tr>
<tr>
<td>Service,CN=Services,CN=Configuration,DC=ocs2,DC=eng,DC=westminster,DC=polycom,DC=com</td>
</tr>
<tr>
<td>instanceType: 4 (0x4)</td>
</tr>
<tr>
<td>whenCreated: 7/2/2009 8:36:57 PM</td>
</tr>
<tr>
<td>whenChanged: 7/2/2009 8:36:57 PM</td>
</tr>
<tr>
<td>name: {56A93378-FEA9-4EAE-845D-AAF0BD8073C0}</td>
</tr>
<tr>
<td>objectCategory:</td>
</tr>
<tr>
<td>CN=ms-RTC-SIP-TrustedService,CN=Schema,CN=Configuration,DC=ocs2,DC=eng,DC=westminster,DC=polycom,DC=com</td>
</tr>
<tr>
<td>dSCorePropagationData: 1/1/1601</td>
</tr>
<tr>
<td>msRTCSIP-TrustedServicePort: 5073 (0x13D1)</td>
</tr>
<tr>
<td>msRTCSIP-TrustedServerFQDN: QAOC1.ocs2.eng.westminster.polycom.com</td>
</tr>
<tr>
<td>msRTCSIP-TrustedServiceType: Microsoft.Rtc.Applications.Cas</td>
</tr>
<tr>
<td>msRTCSIP-TrustedServerVersion: 4 (0x4)</td>
</tr>
<tr>
<td>msRTCSIP-Routable: True</td>
</tr>
<tr>
<td>msRTCSIP-ExtensionData:</td>
</tr>
<tr>
<td>TLSTarget=QAOC1.ocs2.eng.westminster.polycom.com</td>
</tr>
</tbody>
</table>

c Find the TrustEntry that includes your FQDN and use the value of the name: property in the next step d. This is the GUID of the TrustEntry.

d Run the following command:

cscript OCSTrustEntry.vbs /action:remove /type:trustedservice /CN:<GUID>

where <GUID> is the value of the name: property of the TrustEntry you listed in the previous step c.
3 Add a Matched URI route to the DMA by right-clicking the Office Communications Server Pool, and selecting Properties > Front End Properties > Route.

4 Add a host authorization for the DMA by right-clicking the OCS Pool, and selecting Properties > Front End Properties > Host Authorization.

Note: Changes can take up to five minutes to apply.
It may take up to five minutes for these changes to be replicated from Active Directory to the Office Communications Server repository.

Setting up Simultaneous Numeric and Matched URI Routing

You can set up a DMA system on the Office Communications Server to simultaneously use numeric and matched URI dialing.

Matched URI dialing requires a user 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 required to use connect links included in meeting invitations generated from the Polycom Conferencing for Outlook add-in.

To set up simultaneous use of numerical and matched URI routing:

1 Set the DMA as a trusted service (MediationServer) using the instructions in Task 1: Configure the DMA as a Routable Gateway.

2 Set up a matching URI route to the DMA by right-clicking the OCS Pool, and selecting Properties > Front End Properties > Routing tab.

3 Also set up a voice route to the same DMA using instructions in Task 1: Configure the DMA as a Routable Gateway.

Note: You can define only one trusted service entry for the DMA.
You cannot add a DMA system as an authorized host using the Front End Properties > Host Authorization tab. Though there are two routes to the DMA – the matched URI and voice route – you can define only one trusted service entry for the DMA. Only TLS connections to the DMA system will work. TCP connections will not work.

Setting Up Registered RMX User Name Dialing

The Office Communications Server edge server enables you to set up remote and federated connections to the RMX system using the registered user name for dialing. The endpoint connects to the DMA system by entering the DMA registered user name in the following format:
[RMX registered user name]@[OCS domain name]

For example: rmx1234567890@ilsnd.vsg.local

The call reaches the Transit Entry Queue of the RMX and via IVR is routed to the destination conference.
Chapter 16: Supporting Remote and Federated Users for Microsoft® Office Communications Server

You can support federated or remote users by including an Office Communications Server edge server in your environment. The Office Communications Server with an access edge server role supports the Interactive Connectivity Establishment (ICE) protocol. The ICE protocol allows devices outside an organization’s network to call devices that are part of the Polycom®-enabled unified communications solution. This functionality is supported in the Microsoft Office Communications Server, the Polycom video infrastructure, and Polycom HDX systems.

This configuration supports both remote and federated users.

- **Remote workers** refers to workers connecting to an organization’s firewall from outside that enterprise firewall. When registered to an enterprise’s Office Communication Server edge server, remote users can communicate with enterprise users without the use of a VPN or additional firewall traversal devices.

- **Federation** is a trust relationship between two or more SIP domains that permits users in separate organizations to communicate in real-time across networks as federated partners.

- **Federated users** are workers registered to separate enterprise Office Communications Server edge servers that are able to communicate across an external network from behind their respective firewalls.

In a Microsoft Office Communications Server edge server environment, calls are supported to the following devices:

- Polycom HDX systems
- Microsoft Office Communicator clients
- Polycom RMX systems
- Polycom DMA systems

Figure 4 illustrates an example of an edge server deployment scenario. Enterprise A and B are federated. Enterprise B has a branch office, which in this example is a Polycom HDX user behind more than one firewall. The user in the branch office can communicate to other enterprises and remote users.
In this example, users in enterprise A and B can communicate with remote users C and D. The remote users can communicate with each other and with federated users in enterprise A and B.

**Deploying Microsoft Office Communications Edge Server for Federation**

If you need more details on deploying an Office Communications Edge Server for federation, download the Edge Configuration Guide from [Microsoft Office Communications Server 2007 R2 Documentation](https://docs.microsoft.com/en-us/previous-editions/office-communications-server-2007-r2/).


**Requirements**

Ensure that you meet the following requirements for the deployment process.

- TLS is required for federated environments and for remote users.
- You must use the Access Edge Server IP address to register Polycom devices to an Office Communications Server edge server.
Note: Federation does not support numeric dialing.
Numeric dialing is not supported for federated environments.

You need to complete the following three major steps to deploy Office Communications Server for federation:

- Deploying Microsoft Office Communications Edge Server
- Deploying RMX Systems with Office Communications Server Edge Server
- Deploying a Remote HDX System

**Deploying Microsoft Office Communications Edge Server**

Deploying the Office Communications Edge Server requires you to complete the following two tasks:

- **Task 1: Configure the RMX/DMA as a Routable Gateway**
- **Task 2: Ensure SIP Signaling Domains are Allowed**

**Task 1: Configure the RMX/DMA as a Routable Gateway**

You must set the RMX or DMA system as a routable voice gateway in the Office Communications Server infrastructure, which enables you to set the RMX or DMA system as a destination for a voice route. This does not restrict the system to voice operation.

**Note: Complete these tasks on the same network as the RMX or DMA system resides.**

Complete this task on the Office Communications Server on the network where the RMX system or DMA system resides. Perform configurations on the internal Office Communications Server, not the edge server.

The Office Communications Server infrastructure uses the WMI class `MSFT_SIPTrustedAddInServiceSetting` to store information for each voice gateway in the infrastructure. Typically, these gateways are Office Communications Server Mediation Servers. In this case, you set the RMX or DMA as a voice gateway by creating a new instance of the `MSFT_SIPTrustedAddInServiceSetting` class.

**To set up an RMX or DMA system as a voice gateway:**

1. If you have not already, download and install the Office Communications Server 2007 R2 Resource Kit Tools.
2 Open a command prompt and navigate to the location you installed the Office Communications Server 2007 R2 resource kit, for example, C:\Program Files\Microsoft Office Communications Server 2007R2\ResKit. 

3 Run the following command:


where <your FQDN> is the FQDN of your RMX or DMA system.
The script automatically generates the GUID and discovers the proper Active Directory container to store the object.

Your RMX or DMA system is now established as a trusted gateway by all Office Communications Server pools in the domain and displays in the list of voice gateways when you establish a voice route.

4 Ensure that your DMA system or RMX system is not in the Authorized Hosts list for your Office Communications Server.
   a You need to set the TrustedService object you just created to be the only trusted entry for the RMX or DMA. For each Office Communications Server pool, you must do the following:
   b From the Office Communications Server management console, navigate to your server pool.
   c Right-click the pool name and select Front End Properties. Then select the Host Authorization tab.
   d Make sure the same RMX system or DMA system you created a TrustedService instance for is not also in the list of authorized hosts. If it is, you must completely remove the entry from the list.

Task 2: Ensure SIP Signaling Domains are Allowed

When federating with another Office Communications Server environment that includes a Polycom RMX system or a Polycom DMA system, you need to ensure that the Office Communications Server edge server domain and the SIP signaling domain are allowed on the federated Office Communications Server edge server.

For example, if company A wants to connect to calls managed by a DMA or RMX system on company B, company A must add the company B domains to its list of allowed SIP domains in the Office Communications Server edge server.

To federate an Office Communications Server edge server with another Office Communications Server environment:

   1 On the Office Communications Server edge server, navigate to the Computer Management console. For example, right-click My Computer and choose Manage.
2 In the console tree, expand **Computer Management > Services and Applications > Office Communications Server 2007** and right-click **Office Communications Server 2007** and then click **Properties**.

3 Click the **Internal** tab.

4 In the **Internal SIP Domains support by Office Communications Servers in your organizations**, click **Add Domain**.

5 In the Add SIP Domain dialog, add each SIP domain to be supported in your Office Communications Server 2007 deployment. In the box, type the FQDN of the SIP domain, and then click **Add**. After adding all SIP domains to be supported, click **Next**.

You need to add the following SIP domains:

- The Office Communications Server edge server you want to federate, for example, **OCS.companyB.com**.
- The SIP signaling domain of the DMA system or RMX system. For example, if you are using a DMA system, **DMA.OCS.companyname.com**. If you are using only an RMX system, use the FQDN of the RMX system. Use the following format for the FQDN of the SIP signaling domain: **RMX_DMA_NAME.OCS_EDGE_SERVER_NAME.DOMAIN.COM**.

**Note**: Configure your RMX or DMA on the network it resides on.
You must configure your RMX system or DMA system on the network it resides as a static route for Office Communications Server.

### Deploying RMX Systems with Office Communications Server Edge Server

The second major step in deploying Office Communications Edge Server for federation is to enable remote and federated connections in the Polycom RMX system. Before this, ensure that you consider the following requirements:

- The Office Communications Server Edge Server is supported only in MPM+ Card Configuration Mode.
- The firewall must be UDP enabled.
- The RMX system must have a unique account in Active Directory and must be registered with the Office Communications Server edge server.
- A TLS connection is required.

Complete the following four tasks:

- **Task 1**: Create an Active Directory Account for the RMX System
- **Task 2**: Create the RMX User Account for Office Communication Server Edge Server
Polycom® Unified Communications Deployment Guide for Microsoft® Environments

- **Task 3**: Enable the RMX Account for Remote Access and Federation
- **Task 4**: Configure the RMX for ICE Dialing
- **Task 5**: Add the SIP Signaling Domain to the Federated Office Communications Server Edge Server (if your deployment does not include a DMA system).

**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 Office Communications Server and to automatically synchronize with the Office Communications Server edge server.

This account must be a dedicated account that is enabled for Office Communications Server. Because the RMX system has been added as a trusted application, the RMX system is able to use its trusted application configuration to register with the Office Communications 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 Object - User** wizard shown next, enter the user information. Polycom recommends using 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**.

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

**Task 2: Create the RMX User Account for Office Communication Server Edge Server**

Next, register the new RMX user you created in Active Directory with the Office Communications Server Edge Server.

**To enable the RMX User Account for Office Communication Server:**

1. In the Active Directory Users and Computers window, right-click the RMX user you created and then click **Properties**.

2. In the Properties dialog, click the **Communications** tab.

3. In the Sign in name field, enter the RMX user name in the format **SIP:rmx user name**, for example **sip:rmx1234567890**, and select the domain name, for example, **ilsnd.vsg.local**.

4. Select the Server or Pool from the list.

5. Click **Apply** and **OK**.

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

You need to configure the RMX user account for remote access and federation. The following instructions assume you have configured an Office Communications Server edge server.

**To configure the RMX account for federation and remote user access:**

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

2. Right-click the conference room user, and select **Configure Communications Server Users**.

3. In the **Configure Communications Server Users** wizard, click **Next**.
4 In the **Configure User Settings** page, mark the **Federation** and **Remote user access**
check boxes.

- **Remote user access** is required for all deployments that include remote or federated
  users.
- **Federation** is only required when you are supporting federated users.

5 Click **Next** and select any additional configuration settings for your deployment.

6 When complete, click **Finish**.

**Task 4: Configure the RMX for ICE Dialing**

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

Before you begin this task, ensure that you meet the following requirements:

- The RMX must be configured to work in Microsoft environment. Set the
  MS_ENVIRONMENT flag to YES.
- The IP Network Service is set to work with Office Communications Server as the SIP
  Server
- The TLS certificate must be installed.

For a detailed description of these requirements, see **Appendix H** of the Polycom RealPresence

**To configure the RMX for ICE 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 (, , or ) entry.
   The Default IP Service - Networking IP dialog opens.

3 Click the SIP Servers tab.

4 Make sure that the following registration options are not selected:
   ○ Ongoing Conferences
   ○ Meeting Rooms
   ○ Gateway Profiles
   ○ Entry Queues
   ○ SIP factories

5 Specify the IP address of the Office Communications Server 2007 edge server and ensure that the Server Domain Name is the same name you defined in the Office Communications Server edge server and in the Management Network for the DNS.

6 Click the SIP Advanced tab.

7 In the Server User Name field, enter the RMX User name you defined in the Active Directory, for example, enter rmx1234567890.

8 In the ICE Environment field, select MS to enable Microsoft ICE implementation.

9 Click OK.
   The RMX system will register with the Office Communications Server edge server and enable automatic retrieval of the STUN server and Relay server parameters for ICE dialing.

**Task 5: Add the SIP Signaling Domain to the Federated Office Communications Server Edge Server**

If your deployment does not include a DMA system, you must add the RMX SIP signaling domain to the Office Communications Server edge server in the enterprise you are federating, as shown in Task 2: Ensure SIP Signaling Domains are Allowed.

**Monitor 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.
Deploying a Remote HDX System

Office Communications Server edge server supports remote HDX system users. You need to register the remote HDX systems with the edge server to enable users to communicate across their separate networks.

If remote HDX system users are using a virtual private network (VPN), they can register directly to an Office Communications Server and no edge server is required.

Requirements for Deploying a Remote HDX System

- Polycom HDX systems are automatically provisioned to support ICE in SIP calls during registration with the Office Communications Server. No additional provisioning or configuration is required.
- Calls over an Office Communications Server edge server support call rates of up to 1564 kbps.
- People + Content (H.239) is supported in SIP calls that have ICE enabled only if the users are communicating within the same network and firewall.
- The Polycom HDX supports a single video stream - either People Video or Content Video. People + Content (H.239 / Dual Streams) is not supported and Content Video is sent over the People Channel.
- The Polycom HDX system cannot detect presence for federated contacts.
- A TLS connection is required.

To register an HDX system to an Office Communications Server edge server:

1. Use the instructions on Deploying Polycom® HDX Systems with the following consideration:
   ○ If you are registering a remote HDX system with an Office Communications Server edge server, use the FQDN of the access edge server role.
Chapter 17: Polycom® Conferencing for Microsoft® Outlook

Polycom Conferencing for Microsoft® 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 Conferencing for Outlook feature, and shows you how to deploy Polycom® Conferencing for Microsoft 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 Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations.

Please see Polycom Services or contact your local Polycom representative for more information.

This chapter includes the following sections:

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

Polycom Products for Use with Conferencing for Outlook

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

Table 10-1: Polycom Products for Use with Conferencing for Outlook

<table>
<thead>
<tr>
<th>System</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Conferencing Add-in for Outlook</td>
<td>v1.0.3</td>
<td>Allows Outlook users to schedule meetings that include video, audio, and recording. Allows invitees to join a video-enabled meeting by clicking a link.</td>
</tr>
<tr>
<td>System</td>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Polycom HDX systems</td>
<td>v3.0.3</td>
<td>Monitor the Microsoft Exchange calendar of the configured account and display on-screen notifications of meetings. Users can join meetings via these notifications.</td>
</tr>
<tr>
<td>Polycom RMX 2000 or 4000 systems</td>
<td>v7.6</td>
<td>Monitors the Exchange mailbox for the Polycom Conferencing service and hosts Polycom Conferencing for Outlook conferences. Displays meeting information at the start of a meeting, called the Gathering Phase.</td>
</tr>
<tr>
<td>Polycom CMA 4000 or 5000 system</td>
<td>v6.0</td>
<td>Provisions Polycom HDX systems for Polycom Conferencing for Outlook functionality and routes H.323 calls to the appropriate Polycom RMX or DMA system.</td>
</tr>
<tr>
<td>Polycom CMA Desktop</td>
<td>v5.2</td>
<td>Allows users to join video-enabled meetings by clicking a link in a meeting invitation.</td>
</tr>
<tr>
<td>Polycom DMA 7000 system</td>
<td>v4.0</td>
<td>Monitors the Exchange mailbox for the Polycom Conferencing service and determines the appropriate Polycom RMX system to host a given Polycom Conferencing for Outlook conference.</td>
</tr>
<tr>
<td>Polycom RSS 4000 system</td>
<td>v7.0</td>
<td>Via a connection from the Polycom RMX system, records Polycom Conferencing for Outlook conferences in H.323 format when selected in the Polycom Conferencing Add-in.</td>
</tr>
<tr>
<td>Polycom VBP-S/T system</td>
<td>v11.2.3</td>
<td>Enables H.323 Polycom HDX systems to support Polycom Conferencing for Outlook in a remote small office/home office (SOHO) network.</td>
</tr>
</tbody>
</table>
Microsoft Products for Use with Conferencing for Outlook

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

Table 10-2: Microsoft Products for Use with Conferencing for Outlook

<table>
<thead>
<tr>
<th>System</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Active Directory</td>
<td>2003 or 2008</td>
<td>Enables account logins and integrates with Microsoft Exchange. Note that Polycom products currently support only a single-forest Active Directory deployment.</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td>2007 with SP2 2010</td>
<td></td>
</tr>
<tr>
<td>Microsoft Lync Server</td>
<td>2010 2010 Cumulative Update 3</td>
<td>Provides presence-based real-time instant messaging (IM), voice, video, and data communications.</td>
</tr>
<tr>
<td>Microsoft Lync (client)</td>
<td>2010</td>
<td>Can join video-enabled meetings by clicking a link in a meeting invitation.</td>
</tr>
<tr>
<td>Microsoft Office Communications Server</td>
<td>2007 R2</td>
<td>Provides presence-based real-time instant messaging (IM), voice, video, and data communications.</td>
</tr>
<tr>
<td>Microsoft Office Communicator client</td>
<td>2007</td>
<td>Can join video-enabled meetings by clicking a link in a meeting invitation.</td>
</tr>
<tr>
<td>DNS</td>
<td>N/A</td>
<td>Permits call routing to Polycom RMX and DMA systems and DMA subscription to Exchange for mail notifications.</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>2007 2010 (32-bit only)</td>
<td>Microsoft Outlook and Microsoft Word® are required for sending Polycom Conferencing for Outlook invitations. Users of older versions of Microsoft Office can receive invitations.</td>
</tr>
</tbody>
</table>
Deploying Polycom Conferencing for Outlook

This section shows you how to deploy the Polycom Conferencing for Outlook feature. You need to complete steps in each of the following sections to deploy Polycom Conferencing 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 Systems
- Configure Mailboxes for Polycom HDX Desktop Systems
- Configuring HDX Mailboxes to Prevent Meeting Conflicts
- Configuring Polycom HDX System Calendaring Settings
- (Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX systems
- Configuring and Installing the Polycom Conferencing Add-In
- Testing Polycom Conferencing for Outlook Deployment

Configuring DNS Entries for Polycom Devices

To enable Polycom devices to work correctly with Conferencing 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 10-1: 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 10-2: 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 Conferencing for Outlook supports H.323 clients, including Polycom HDX systems, and Microsoft unified communications clients.

You can support remote users under the following conditions:

- Polycom HDX system H.323 calls are supported only if a remote Polycom HDX user is registered to a Polycom VBP-S or VBP-S/T device that proxies the Polycom HDX system’s registration to a Polycom CMA system gatekeeper inside the enterprise network.
- Polycom HDX system SIP calls are supported only if the Polycom HDX is registered to Office Communications Server via an Office Communications Server 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 system, you will need to set up your HDX 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 Conferencing 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 Conferencing Add-in for Outlook 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 Conferencing Add-in for Outlook 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 PolycomConferencing@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 Conferencing for Outlook. Figure 7 shows the General tab of the Polycom Conferencing Properties dialog, for an example of configuring a Polycom infrastructure mailbox.

Figure 10-3: 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:

```bash
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 Systems

Configure an exchange room mailbox and an Active Directory account for each room-based HDX in your deployment.

**Note: Configure Additional Settings for HDX**

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, you will need to configure additional settings.

You can use the same workflows to schedule a video-enabled Polycom Conferencing 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 system monitors the exchange calendar for scheduled meetings.

You can configure a mailbox for HDX 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 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 10-3: Features Available with the HDX Room Mailbox**

<table>
<thead>
<tr>
<th></th>
<th>An Exchange mailbox with enabled user account</th>
<th>An Exchange mailbox with a disabled user account managed by a service account</th>
<th>Multiple Exchange mailboxes with disabled user accounts managed by a single service account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Conferencing for Outlook</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### 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 system uses this data to display call information and complete calls.

### Note: HDX Supports a Single Directory

Polycom HDX systems can have a single directory. If your environment includes a Polycom CMA system and Office Communications Server, presence and directory are provided by Office Communications Server.
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:
   ```powershell
   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:
   ```powershell
   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:**

1 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>\<hdxActiveDirectoryAccountUserName>' -AccessRights 'FullAccess' -InheritanceType 'All'
```

**Option 3: Associate Multiple Mailboxes with a Service Account**

You can use one service account for all Polycom HDX systems in the Polycom Conferencing 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\hdxActiveDirectoryAccountUserName>' -AccessRights 'FullAccess' -InheritanceType ‘All’
```

Figure 8, shown next, provides an example configuration. You can replicate this example association between Aphrodite and SRV-AllHDX-CompanyA for multiple rooms.

*Figure 10-4: Using a service account for all HDX conference rooms.*

Configure Mailboxes for Polycom HDX Desktop Systems

You need to configure HDX desktop system 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 an HDX system.
Configuring HDX 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 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 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 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 9 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 10-5: Assigning a User Account for a Room Mailbox.**
Figure 10 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 10-6: Using a service account to manage a mailbox**
Figure 11 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 10-7: Associate Multiple Mailboxes with a Single Account**

Configure the system for a calendaring service.

<table>
<thead>
<tr>
<th>General Settings</th>
<th>Network</th>
<th>Monitors</th>
<th>Cameras</th>
<th>Audio Settings</th>
<th>LAN Properties</th>
<th>Global Services</th>
<th>Directory Servers</th>
<th>SNMP</th>
<th>Management Servers</th>
<th>Provisioning Service</th>
<th>Calendaring Service</th>
<th>Account Validation</th>
<th>My Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Calendaring Service**

- Register with Calendaring Service: [on]
- Server Address: ca-exchange.companyA.local
- Domain: companyA.local
- User Name: SRV-AllHDX-CompanyA
- Change Password
- Mailbox: (Primary SMTP) aphroditeroom@companyA.com
- Reminder Time in Minutes: 5
- Play Reminder Tone: [on]
- Show Private Meeting Information: [off]
- Update

Figure 12 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 10-8: User-based Calendar Settings in the Polycom HDX System**
Figure 13 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 10-9: Calendar Configuration for a SOHO User.**

(Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX 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 Conferencing Add-In**

The Polycom Conferencing Add-In software and its templates must be installed on each Microsoft Outlook client.
For complete instructions, see *Configure and Install the Polycom Conferencing Add-In* in the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

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

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

**Task 1: Configure Polycom Conferencing Add-in Preferences for Installation to Client PCs**

You can configure the client experience of the Polycom Conferencing 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 Conferencing Add-In* in the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

**Task 2: Install Polycom Conferencing Add-in for Outlook to Client PCs**

You can install the conferencing 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 Conferencing 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 Conferencing Add-In* in the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

**Testing Polycom Conferencing 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*. 
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>
<thead>
<tr>
<th>.dat File Name</th>
<th>Description</th>
<th>Value Range</th>
<th>Content Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>lanwithcntry</td>
<td>Language and country</td>
<td>Text string</td>
<td>English/en</td>
</tr>
<tr>
<td>connecttomylan</td>
<td>Enable or disable LAN interface</td>
<td>False, True</td>
<td></td>
</tr>
<tr>
<td>lanportspeed</td>
<td>LAN speed</td>
<td>Auto, 10_Mbps, 100_Mbps, 1000_Mbps</td>
<td></td>
</tr>
<tr>
<td>landuplexmode</td>
<td>LAN duplex</td>
<td>Auto, Full, Half</td>
<td></td>
</tr>
<tr>
<td>dot1xenabled</td>
<td>Enable or disable 802.1X</td>
<td>False, True</td>
<td></td>
</tr>
<tr>
<td>dot1xid</td>
<td>802.1X authentication user id</td>
<td>Text string</td>
<td>johnsmith</td>
</tr>
<tr>
<td>dot1xpwd</td>
<td>802.1X authentication password</td>
<td>Text string</td>
<td>johnsmithpassword</td>
</tr>
<tr>
<td>vlanmode</td>
<td>Enable or disable VLAN</td>
<td>False, True</td>
<td></td>
</tr>
<tr>
<td>.dat File Name</td>
<td>Description</td>
<td>Value Range</td>
<td>Content Example</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>vlanid</td>
<td>VLAN ID</td>
<td>Integer in [2,4094]</td>
<td>100</td>
</tr>
<tr>
<td>dhcp_flg</td>
<td>Enable or disable DHCP client</td>
<td>Client, Off</td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td>Host name of the Polycom HDX</td>
<td>Text string</td>
<td>hdx334</td>
</tr>
<tr>
<td>userdomain</td>
<td>Domain of the user account used to log into the Polycom CM</td>
<td>Text string</td>
<td>polycom.com</td>
</tr>
<tr>
<td>domainname</td>
<td>Domain of the Polycom HDX system, which will be set by the network itself if DCHP is unprovisioned</td>
<td>Text string</td>
<td></td>
</tr>
<tr>
<td>ipaddress</td>
<td>IP address of the Polycom HDX</td>
<td>IP address</td>
<td>172.18.1.222</td>
</tr>
<tr>
<td>subnetmask</td>
<td>Subnet mask of the Polycom HDX</td>
<td></td>
<td>255.255.255.192</td>
</tr>
<tr>
<td>defaultgateway</td>
<td>IP address of the default</td>
<td>IP address</td>
<td>172.18.1.65</td>
</tr>
<tr>
<td>dnsserver</td>
<td>DNS server</td>
<td>IP address</td>
<td>172.18.1.15</td>
</tr>
<tr>
<td>dnsserver1</td>
<td>Alternate DNS server</td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>dnsserver2</td>
<td>Alternate DNS server</td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>dnsserver3</td>
<td>Alternate DNS server</td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>provisionserveraddress</td>
<td>IP address of the Polycom CMA</td>
<td>IP address or host name</td>
<td>polycomCMA.polycom.com</td>
</tr>
<tr>
<td>ldapuserid</td>
<td>LDAP user id</td>
<td>Text string</td>
<td>johnsmith</td>
</tr>
<tr>
<td>ldappassword</td>
<td>LDAP password</td>
<td>Text string</td>
<td>johnsmithpassword</td>
</tr>
</tbody>
</table>
Appendix B: Exchange Calendar Polling Information

This appendix provides information on Exchange Calendar Polling.

**Polycom HDX System**

When actively viewing the endpoint's calendar onscreen, the Polycom HDX system polls the Exchange server for updates every 20 seconds. When viewing any other screen, or when the Polycom HDX 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 Conferencing 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.

**Why can’t I join or conferences hosted on Lync with my HDX?**

In both OCS releases, Microsoft chose to use different versions of ICE between the Front End server (ICE v6) and the Edge server (ICE v19), as explained in [Media Port Range for Office Communications Server 2007 R2](#). In contrast, Lync Server 2010 uses ICE v19 throughout the entire product line. Because the Polycom implementation of CCCP is compatible only with the current ICE v19 used in Lync Server, an HDX will not be able to join conferences hosted on an OCS AVMCU. In this scenario, an HDX can join conferences hosted on the Lync AVMCU, as explained in [RTV Support Released for Polycom Solutions](#).

**I am no longer able to access the Polycom Conferencing Add-In**

The Polycom Conferencing Add-In can become disabled. If this occurs, navigate to Help > Disabled Items in Microsoft Outlook and enable the Polycom Conferencing Add-In again.

**Polycom HDX 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 system**

In an Office Communications Server deployment, you must enable HDX users for remote access and federation as shown in Task 5: Enable Conference Rooms 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 do so from http://www.slproweb.com/products/Win32OpenSSL.html

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.
   o 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 solution with this Polycom partner, see Polycom Unified Communications Solution for Microsoft Environments on Polycom Strategic Global Partner Solutions site.


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.