Polycom Unified Communications Deployment Guide for Microsoft Environments
Trademark Information

Polycom®, the Polycom “Triangles” logo, and the names and marks associated with Polycom’s products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

Patent Information

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

1 About This Guide .................................................. 1
   Required Skills .................................................. 1
   Polycom Solution Support Services ............................. 2

2 Polycom Unified Communications ......................... 3
   Polycom-enabled Unified Communications ....................... 4
      End User Advantages ........................................ 4
      System Administrator Advantages ........................... 4
   Polycom Conferencing for Microsoft Outlook .................... 5
      End User Advantages ........................................ 5
      System Administrator Advantages ........................... 5

3 Polycom-enabled Unified Communications for Microsoft Lync Server ................................................. 7
   Before You Begin ............................................... 8
   Polycom Solution Support Services ............................. 8
   Solution Overview for Lync Environments ..................... 9
      Key Concepts ................................................ 9
         Microsoft Domain Accounts ............................... 9
         Encryption and Security ..................................... 10
         Remote and Federated Users ............................... 10
         Microsoft Call Admission Control ......................... 10
         High Quality Video ......................................... 10
   Supported Microsoft Versions .................................. 10
   Products that Enable Unified Communications ................. 11
   Setting up Dialing Plans for a Lync Server Environment .... 12
      Matched URI Dialing ........................................ 12
      Registered RMX User Name Dialing .......................... 12
   Supporting Remote and Federated Users in Lync Server Environments ................................................. 13
   Understanding Microsoft Domains and Application Pools ........ 14
      Using Multiple Computer Application Pools .................. 14
      Static Routes and the Match URI ............................. 15
      Microsoft Domains and DNS Entries ........................ 15
4 Deployment Process for Polycom HDX Systems ........... 17

   Configure Lync Server 2010 for use with an HDX System ............ 17
   Configure Authentication in Lync Server .......................... 18
   Using Microsoft Call Admission Control ............................ 18
   Enable HD Video on the Lync Server ............................... 18
   Add Conference Rooms with Polycom HDX Systems to Active
   Directory ........................................................................ 19
   Enable Conference Rooms for the Lync Server ...................... 20
   Enable Conference Room Users for Remote Access and Federation . 20
   Add Lync Contacts to Conference Room Local Address Book ....... 21
   Configure Your Polycom HDX System for the Microsoft Environment . . . . 22
   Install the RTV Option Key on your HDX System ................. 23
   Register Polycom HDX System with the Lync Server .............. 23
   Configure the Polycom HDX System LAN Properties ............. 27
   Configure Display Options for the HDX System Contact List .... 28
   Configure AES Encryption ........................................... 28
   Support for Lync-hosted Video Conferencing ...................... 29
      Using the Polycom Touch Control with Lync Conferencing .... 29
      Roles in Lync-hosted Calls ...................................... 30
   Support for High-Quality (RTV) Video ............................... 31
      RTV Requirements ................................................. 31
      Call Quality Scenarios for RTV Video ........................... 31

5 Deployment Process for Polycom Immersive Telepresence
   Systems ........................................................................ 33

   Configure Lync Server 2010 for Use with an ITP System ........ 33
   Configure Authentication on the Lync Server ..................... 34
   Using Microsoft Call Admission Control ............................ 34
   Enable HD Video on the Lync Server ................................ 34
   Creating and Enabling Conference Room User Accounts ...... 35
      Add a Conference Room User for each Codec within your ITP
      System ..................................................................... 35
      Enable Conference Rooms for the Lync Server ............... 36
      Hiding the Secondary CODECS in the Lync Directory ...... 37
      Hiding the Secondary CODECS in the Directory Using the Exchange
      Management Console ............................................... 37
      Hiding the Secondary CODECS in the Directory Using the ADSI Edit
      Tool ....................................................................... 38
   Enable Conference Room Users for Remote Access and Federation . 39
   Configure Your Polycom ITP System for the Microsoft Environment . . . 40
      Register All CODECS with the Lync Server .................. 41
6 Deployment Process for Polycom RMX Systems 49

Configuring Your RMX System for use with the Lync Server 50
Set up the RMX System for Security and SIP 50
  Configuring the RMX IP Network Service 50
  Add the RMX FQDN (SIP signaling IP address) in DNS 51
Create a Security Certificate for the Polycom RMX System 52
Install the certificate on your RMX system 56
Configure Encryption for your Deployment 57
Configure Your Lync Server for Use with an RMX System 58
  Use Lync Topology Builder to define your trusted application pool 58
  Use Lync Powershell to set the Polycom RMX system as a trusted host with a static route 59
  Use Lync Powershell to create the trusted application 60
  Use Lync Powershell to update the topology 61
Enabling Microsoft Presence 61
Configure your Microsoft Environment to Support RMX Room Presence 61
  Creating an Active Directory Account for the Conferencing Entity 62
  Enabling the Active Directory Account for Lync Server 63
  Enable the RMX Account for Remote Access and Federation 64
Configure your RMX System for Microsoft Presence 65
  Enabling SIP Registration in the Conference Profile 65
  Create or Modify the RMX Conferencing Entity 66
Enabling Edge Server Integration with your RMX System 67
  Edge Server Considerations for the Polycom RMX System 67
  Creating an Active Directory Account for the RMX System 68
  Enabling the RMX User Account for Lync Server Edge Server 69
  Enable the RMX Account for Remote Access and Federation 70
  Configuring the RMX System for Federated Dialing 70
  Configure RMX System Flags for Federation and Microsoft Call Admission Control 71
  Monitoring the connection to the STUN and Relay Servers in the ICE environment 71
7 Deployment Process for Polycom DMA Systems ............ 73

Configure Your DMA System for your Environment .............. 74
Ensure DNS is Configured Properly .................................. 74
Create a Security Certificate for the Polycom DMA 7000 System .... 74
Configure a DMA System SIP Peer for the Lync Server .......... 79
  Configure a SIP Peer in the DMA System ......................... 79
  OPTIONAL Configure your DMA System to Route to Specific SIP Domains ........................................... 80
Set up a Dial Rule for the Lync Server .............................. 81
Configure Your Microsoft Environment for Use with a DMA System ... 83
  Set the Routing for the Polycom DMA System ..................... 83
  Use Lync Topology Builder to define your trusted application pool 83
  Use Lync Powershell to set the Polycom DMA system as a trusted host with a static route ............................. 85
  Use Lync Powershell to create the trusted application ............ 86
  Use Lync Powershell to update the topology ...................... 86
Enable Federation in your Environment .............................. 87
  Ensure the Microsoft Lync Edge Server Role is Configured ....... 87
  Ensure the Primary SIP Signaling Domain is Allowed ........... 87

8 Polycom-enabled Unified Communications for Microsoft Office Communications Server .................. 89

Polycom Solution Support Services ................................. 90
Solution Overview for Office Communications Server Environments ... 90
  Key Concepts ......................................................... 90
  Microsoft Domain Accounts ........................................ 91
  Encryption and Security ........................................... 91
  Remote and Federated Users ...................................... 91
Products that Enable Unified Communications ....................... 92
Deployment Process for Office Communications Server ................ 94
  Prepare for the Implementation .................................... 94
  Configure Authentication in Office Communications Server .... 94
  Add Conference Rooms with Polycom HDX Systems to Active Directory ..................................................... 96
Enable Conference Rooms for the Office Communications Server 96
Enable Conference Rooms for Remote Access and Federation 97
Add Contacts to the Conference Room Local Address Book 98
Configure the Office Communications Server Server Pool Encryption Setting ............................................ 100
Deployment Process for Polycom HDX Systems ...................... 101
  Register Polycom HDX Systems with the Office Communications Server .................................................. 101
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the Polycom HDX System LAN Properties</td>
<td>105</td>
</tr>
<tr>
<td>Configure Display Options for Contact List</td>
<td>106</td>
</tr>
<tr>
<td>Configure AES Encryption</td>
<td>107</td>
</tr>
<tr>
<td><strong>Deployment Process for Polycom Immersive Telepresence Systems</strong></td>
<td>108</td>
</tr>
<tr>
<td>Configure Office Communications Server for Use with an ITP System</td>
<td>108</td>
</tr>
<tr>
<td>Configure Authentication on the Office Communications Server</td>
<td>108</td>
</tr>
<tr>
<td>Using Microsoft Call Admission Control</td>
<td>108</td>
</tr>
<tr>
<td>Enable HD Video on the Office Communications Server</td>
<td>109</td>
</tr>
<tr>
<td>Add a Conference Room User for each Codec within your ITP System</td>
<td>110</td>
</tr>
<tr>
<td>Enable Conference Rooms for the Office Communications Server</td>
<td>111</td>
</tr>
<tr>
<td>Hiding the Secondary Codecs in the Directory</td>
<td>112</td>
</tr>
<tr>
<td>Hiding the Secondary Codecs in the Directory Using the Exchange</td>
<td>112</td>
</tr>
<tr>
<td>Management Console</td>
<td></td>
</tr>
<tr>
<td>Hiding the Secondary Codecs in the Directory Using the ADSI Edit Tool</td>
<td>113</td>
</tr>
<tr>
<td>Enable Conference Room Users for Remote Access and Federation</td>
<td>114</td>
</tr>
<tr>
<td>Configure Your Polycom ITP System for the Microsoft Environment</td>
<td>115</td>
</tr>
<tr>
<td>Register All Codecs with the Office Communications Server</td>
<td>115</td>
</tr>
<tr>
<td>Configure the LAN Properties for each Codec</td>
<td>120</td>
</tr>
<tr>
<td>Configure Display Options for the ITP System Contact List</td>
<td>120</td>
</tr>
<tr>
<td>Configure AES Encryption</td>
<td>121</td>
</tr>
<tr>
<td><strong>Support for High-Quality (RTV) Video</strong></td>
<td>122</td>
</tr>
<tr>
<td>RTV Requirements</td>
<td>122</td>
</tr>
<tr>
<td>Call Quality Scenarios for RTV Video</td>
<td>122</td>
</tr>
<tr>
<td><strong>Deployment Process for Polycom RMX Systems</strong></td>
<td>123</td>
</tr>
<tr>
<td>Supporting Remote Users</td>
<td>123</td>
</tr>
<tr>
<td>Understanding Microsoft Domains and Application Pools</td>
<td>123</td>
</tr>
<tr>
<td>Using Multiple Computer Application Pools</td>
<td>123</td>
</tr>
<tr>
<td>Static Routes and the Match URI</td>
<td>124</td>
</tr>
<tr>
<td>Microsoft Domains and DNS Entries</td>
<td>124</td>
</tr>
<tr>
<td>Configuring the Polycom RMX System</td>
<td>125</td>
</tr>
<tr>
<td><strong>Deployment Process for Polycom DMA System</strong></td>
<td>126</td>
</tr>
<tr>
<td>Set the Routing for the Polycom DMA 7000 System</td>
<td>126</td>
</tr>
<tr>
<td>Create a Security Certificate for the Polycom DMA 7000 System</td>
<td>127</td>
</tr>
<tr>
<td><strong>Setting up Dialing Plans</strong></td>
<td>129</td>
</tr>
<tr>
<td>Numeric Dialing</td>
<td>129</td>
</tr>
<tr>
<td>Configure the RMX/DMA as a Routable Gateway</td>
<td>130</td>
</tr>
<tr>
<td>Configure an Office Communications Server Voice Route to the RMX/DMA</td>
<td>131</td>
</tr>
</tbody>
</table>
Enable the user account associated with the room mailbox  . . . 165
Modify the room mailbox settings ................................. 166
Option 2: Use a Service Account with a Single Room Mailbox  . 168
Create the service account ..................................... 168
Grant the service account the permission to manage the Room  
Mailbox ............................................................. 168
Option 3: Use a Single Service Account for Multiple Room  
Mailboxes ....................................................... 170
Configure Mailboxes for Polycom HDX Desktop Systems ........ 171
Configure HDX Mailboxes to Prevent Meeting Conflicts ........ 171
Configure Polycom HDX System Calendaring Settings ........... 172
(Optional) Configure CMA System Automatic Provisioning of 
Calendaring Service Settings on HDX systems ................. 176
Configure and Install the Polycom Conferencing Add-In ........ 176
Configure Polycom Conferencing Add-in Preferences For    
Installation to Client PCs .................................... 176
Install Polycom Conferencing Add-in for Outlook to Client PCs 177
Deploy Customization Files ..................................... 177
Test Polycom Conferencing for Outlook Deployment .......... 177

A Polycom HDX System Configuration Files ...................... 179

B Exchange Calendar Polling Information ......................... 181

Polycom HDX System ............................................. 181
Polycom DMA System .......................................... 181
Polycom RMX System .......................................... 181
Polycom RSS System .......................................... 182

C Troubleshooting .................................................. 183
About This Guide

This guide describes how to deploy Polycom® Unified Communications in a Microsoft environment.

This document’s primary purpose is to describe how to enable Polycom products within a Microsoft environment. Please refer to the product documentation for more in-depth information about individual Polycom products. You can find Polycom product documentation online at http://www.polycom.com/support.

Required Skills

Deploying Polycom Unified Communications in a Microsoft environment requires planning and elementary knowledge of video conferencing and video conferencing administration. It is also helpful to have knowledge of the following third-party products:

• A domain name server
• Microsoft Active Directory server
• Microsoft Exchange Server
• Microsoft Lync or Office Communications Server

This document assumes that these systems are already deployed and that the administrators for these applications are available to aide the administrator deploying Polycom Unified Communications.
Polycom Solution Support Services

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. UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations.

Please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative for more information.
The Polycom® Unified Communications experience for Microsoft is enabled by an integrated suite of Polycom hardware devices and software applications that allow 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** which allows you to integrate the Microsoft SIP infrastructure for 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-enabled unified communications allows you to integrate your Polycom video conferencing infrastructure and Polycom endpoints with Microsoft unified communications (both Microsoft Lync Server and Office Communications Server) to provide seamless video conferencing functionality for Microsoft UC clients.

With Polycom-enabled unified communications, the Microsoft Lync or Office Communications Server manages presence for each registered Polycom component and allows full-featured video calls between Lync or Office Communicator clients and Polycom components. This includes both point-to-point calls and video conferencing, high-quality video, and calling directly from a contact list.

Polycom devices use SIP to connect to Lync Server or Office Communications Server.

End User Advantages

For end-users, this solution makes it simple 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.
- Use a contact list in Microsoft Outlook or Sharepoint to initiate video calls to Polycom endpoints (Polycom components, the Exchange or Sharepoint server must have been 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.
- Take advantage of the 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

For system administrators, this solution makes it easier 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, while 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, which requires the Polycom Conferencing Add-in for Outlook, offers an integrated and enhanced experience for all of those involved in video conferencing.

End User Advantages

• Users can easily add video to meetings as well as ensure a meeting is recorded, without the direct help of IT or a video conferencing administrator. Joining video conferences is done with a single-click from an Outlook calendar entry.

• It allows meeting participants to track their video- and audio-enabled meetings on the same calendar that they track their other meetings.

• It also allows meeting participants to simply click a link in a calendar entry to join conferences on their associated video or audio endpoint system.

• Makes real-time calendar information available for Polycom HDX endpoints. Creates “smart rooms” that automatically display meeting details so users immediately know they are in the right video conference.

• Incorporates virtual meeting rooms (VMRs) that ensure a reliable experience for end users. End users connect to unique VMRs instead of re-usable video bridge numbers.

System Administrator Advantages

• Allows IT departments and video administrators/operators to offer users a simple, familiar procedure for scheduling video- and audio-enabled meetings, which requires less IT support.

• Maximizes the use of visual communication assets and their return on investment (ROI).

• Polycom Conferencing for Outlook allows IT to easily deploy a scalable video infrastructure into an existing Exchange environment.
This chapter describes how to implement Polycom-enabled unified communications, which integrates Polycom systems with the Microsoft Lync Server 2010 for presence-based real-time instant messaging (IM), voice, video, and data communications. It includes instructions for configuring the Lync Server 2010 components and integrating and configuring supported Polycom components.

This chapter includes the following sections:

- “Before You Begin” on page 8
- “Polycom Solution Support Services” on page 8
- “Solution Overview for Lync Environments” on page 9
- “Setting up Dialing Plans for a Lync Server Environment” on page 12
- “Supporting Remote and Federated Users in Lync Server Environments” on page 13
- “Understanding Microsoft Domains and Application Pools” on page 14

Note

This guide does not describe or provide full administration or maintenance processes or procedures for Microsoft Lync Server 2010. For any questions or assistance on Microsoft Office Lync Server 2010, see the Microsoft documentation and/or Microsoft Support Services.
Before You Begin

Before beginning, the person deploying this solution must have:


- Prior knowledge and experience with the Polycom RMX systems, HDX systems, and DMA systems and access to Polycom systems product documentation and relevant software.

Polycom Solution Support Services

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. UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations.

Please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative for more information.
Solution Overview for Lync Environments

Polycom’s integration with Microsoft Lync Server 2010 provides the following functionality:

• Enables point-to-point calls between Polycom HDX systems and Microsoft Lync clients.
• Provides real-time presence information between Polycom devices and Microsoft Lync clients.
• Enables support for remote and federated endpoints to participate in point-to-point calls and video conference calls.
• Supports high-quality video (720p) between Lync clients and Polycom endpoints.
• Allows Polycom endpoints to participate in Lync Server-hosted multi-point conferences.
• Allows Microsoft Lync clients to view the presence for Polycom RMX meeting rooms and start one-click conferences. (One-click conferencing from Lync clients to an RMX system is an optional feature. Contact Polycom technical support for more information.)

The section includes the following topics:

• “Key Concepts” on page 9
• “Supported Microsoft Versions” on page 10
• “Products that Enable Unified Communications” on page 11
• “Before You Begin” on page 8

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 integrated into your Microsoft Lync Server environment.

Be sure you are familiar with the following concepts before proceeding.

Microsoft Domain Accounts

In order to participate in calls with Microsoft components (Lync clients, Lync-hosted multipoint calls), Polycom components must have an account in a Windows domain accessible by the Lync Server environment.

• This domain can either be an Active Directory domain or a SIP domain.
• Domain accounts need the proper capabilities and settings. Some settings are set at the domain level (with policies) and some are set at the account level.
Encryption and Security

• TLS is required in Microsoft environments, which means SSL certificates must be used.

• You can configure call encryption. Remember that encryption settings between the Lync server and Polycom components need to be compatible for calls to succeed.

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

Both the Polycom HDX and the Polycom RMX systems can take advantage of Microsoft Call Admission Control. 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 RMX System” on page 67.

• There is no additional configuration necessary on HDX systems.

High Quality Video

• High quality video is supported on an HDX system only if you have the RTV option key installed. Contact Polycom technical support for more information.

• High quality video is supported on an RMX system only if you have an MPMx card.

Supported Microsoft Versions

Polycom supports the following Lync Server environments:

• Lync Server 2010

• Lync Server 2010 Cumulative Update 3
## Products that Enable Unified Communications

The following table describes the Polycom products that enable unified communications with supported Lync Server versions.

### Table 3-1 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 Lync 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>
</tbody>
</table>

**Advance Microsoft Support**

RTV video and the ability to join a Lync-hosted conference 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 TPD 306M system                                                                                                                    |
|                                               |         | • Polycom ATX SDK and ATX 300 system                                                                                                         |
|                                               |         | Lync Server-hosted calls are not supported for Polycom ITP systems.                                                                         |

| Polycom CX100, 200, 300, 500, 600, 700, 3000 and 5000 phones | All     | Voice endpoint systems that can be integrated into a Microsoft environment. If your deployment includes Polycom CX phones (CX700, CX500, CX300 or CX3000), Lync Server must have the Enterprise Voice option implemented. |
Setting up Dialing Plans for a Lync Server Environment

Within a Lync Server environment, you can include several dialing plans, depending on your environment.

You can use these dialing methods concurrently.

- 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 also required to use connect links included in meeting invitations generated from the Polycom Conferencing for Outlook add-in.

- RMX User Name Dialing allows users in federated environments to create ad-hoc conferences by dialing the RMX user name and then using DTMF tones to enter a conference ID to be shared between participants. RMX registered name dialing is only available in environments that include a Lync Server edge server and an RMX that has been registered to that edge server.

**Note**

Numeric dialing is not supported in Lync Server environments.

**Matched URI Dialing**

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 “Configuring Your RMX System for use with the Lync Server” on page 50 or “Set the Routing for the Polycom DMA System” on page 83, respectively.

**Registered RMX User Name Dialing**

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.

Supporting Remote and Federated Users in Lync Server Environments

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

• Remote users are users who are outside of an organization’s firewall. When a remote user is registered to an enterprise’s Lync Server 2010 Edge server, it can make and receive calls to/from 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 network boundaries as federated partners.

Federated users are users from another enterprise (registered to a different Lync Server on a different network) that are able to make and receive calls to endpoints and video infrastructure on an external network that is behind one or more firewalls.

The Lync Server with an installed access edge server role supports the Interactive Connectivity Establishment (ICE) protocol which allows 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.

Figure 3-1 illustrates a possible Edge Server deployment 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 who is behind more than one firewall. The user in the Branch Office can also place and receive calls from other enterprises and remote users.
Figure 3-1  Lync Server environment with a Lync Server Edge Server (for simplicity, only endpoints are shown).

Users in both enterprises 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 configuring DNS.

Using Multiple Computer Application Pools

As a best practice, you should create a multiple trusted application pool and include your DMA system or RMX system SIP signaling domains as nodes under this pool. See Figure 3-2 for an example.

This method simplifies your Microsoft unified communications environment and also allows you to add additional RMX systems or DMA systems at a later time.
In Figure 3-2, video.corp.local is the pool name. Refer to Microsoft documentation for more information about pool names.

The FQDNs of the 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. This can be done by 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 then Polycom recommends placing the DNS host record for the RMX Signaling Host IP Address or DMA system in the Active Directory domain (e.g. 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 tables provide examples of different Microsoft environments. Table 3-2 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</td>
<td>sipdomain.com</td>
<td>This domain should be used as the match URI in federated environments.</td>
</tr>
<tr>
<td>for Office Communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server 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>dmacorp.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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not need DNS representation.</td>
</tr>
</tbody>
</table>
Deployment Process for 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 topics:

- “Configure Lync Server 2010 for use with an HDX System” on page 17
- “Configure Your Polycom HDX System for the Microsoft Environment” on page 22

Configure Lync Server 2010 for use with an HDX System

This section describes how to configure Lync Server settings as well as HDX account settings in Lync as required for using a Polycom HDX in a Microsoft environment. You must perform these tasks in the following order:

1. “Configure Authentication in Lync Server” on page 18
2. “Using Microsoft Call Admission Control” on page 18
3. “Enable HD Video on the Lync Server” on page 18
4. “Add Conference Rooms with Polycom HDX Systems to Active Directory” on page 19
5. “Enable Conference Rooms for the Lync Server” on page 20
6. “Enable Conference Room Users for Remote Access and Federation” on page 20
7. “Add Lync Contacts to Conference Room Local Address Book” on page 21
Configure Authentication in Lync Server

Your Microsoft Lync or Office Communications Server must have NTLM enabled in order for an HDX system or ITP system to participate in your Microsoft environment. 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, not Kerberos.

Using 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 of SIP calls is 2 Mbps.

Enable HD Video on the Lync Server

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

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

To change the default video settings for your Lync Server:

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

   Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M

3. Restart your Lync Server.

Note

Your Lync client users should already be properly configured in Microsoft Active Directory and Lync Server 2010.

See your Microsoft Active Directory and Lync Server administrators or the Microsoft web site if you have questions regarding the configuration of Microsoft Active Directory and Lync Server.
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.

You can use a script, the Active Directory Users and Computers management console, or custom software for this purpose. The procedure below describes adding a conference room user manually in the Active Directory Users and Computers management console.

If your deployment will also include Polycom Conferencing for Outlook, there are additional considerations when creating this user account. See “Configure Mailboxes for Room-based HDX Systems” on page 164.

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.

Note  If these conference room users have an expiring password, you must keep track of the users and passwords and make sure to update the accounts as required. Polycom recommends setting the passwords to never expire.
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 about Lync Server 2010 Powershell, see http://blogs.technet.com/b/cspb/.

To enable a conference room user for the Lync Server:

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

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

Enable Conference Room Users for Remote Access and Federation

If you need to support remote users and federated users, you need to configure your Lync Server edge server for that purpose. The following instructions assume you have configured a Lync Server edge server.

In order to support external users, you need to do both of the following:

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

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

Add Lync Contacts to Conference Room Local Address Book

You can add Lync contacts to your Polycom system local address book. To do this, you need to 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, those contacts will be displayed in the HDX system the next time you log on.

For more information about displaying contacts in your HDX system, see “Configure Display Options for the HDX system Contact List” on page 28.

Note
Polycom recommends that the Lync Server be configured to allow no more than 200 contacts per user (the default setting). The HDX system displays only 200 contacts per user. If the Lync Server user has more than 200 contacts, the HDX system will not display them consistently.
Configure Your Polycom HDX System for the Microsoft Environment

Your Polycom HDX system should be installed according to standard installation procedures. See the Setting Up the Polycom HDX System guide for your model of Polycom HDX system, which describes how to set up the hardware. Then perform the following tasks:

• “Register Polycom HDX System with the Lync Server” on page 23
• “Configure the Polycom HDX System LAN Properties” on page 27
• “Configure Display Options for the HDX system Contact List” on page 28
• “Configure AES Encryption” on page 28
Install the RTV Option Key on your HDX System

If you want to support RTV video on your HDX system, you need to purchase and install an RTV option key for your HDX system.

You need to install the RTV option key (if applicable) before configuring your HDX system.

Note

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

Register Polycom HDX System with the Lync Server

When an HDX system is registered with a Lync Server, the Polycom HDX 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 and can also be displayed on the home screen.

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. For guidance, see the below table.

Figure 4-1 Polycom system settings when an RTV option key is installed.
Figure 4-2 Polycom system settings without the RTV option key installed.
### Table 4-1  SIP Settings fields and their descriptions

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Mark this check box to enable the HDX system to receive and make SIP calls.</td>
</tr>
<tr>
<td>SIP Server Configuration</td>
<td>Select <strong>Auto</strong> 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 <strong>Specify</strong>.</td>
</tr>
</tbody>
</table>
| 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 an Lync Server environment, specify the DNS name of the Lync Server server. The default port is 5061.  
  • If registering a remote HDX system with an 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**.
Deployment Process for Polycom HDX Systems

Once the Polycom HDX system registers with Lync Server 2010, you can continue on to “Configure the Polycom HDX System LAN Properties” on page 27.

Configure 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.
   
   When registering a remote Polycom system, use a DNS server that the system shares DNS zone information with the Lync Server edge server.
5. Click Update.
Configure Display Options for the HDX system Contact List

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

To configure the 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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Contacts</td>
<td>Specifies whether to display your contacts on the contact list home screen and in the directory.</td>
</tr>
<tr>
<td>Show My Offline Contacts</td>
<td>Specifies whether to include offline contacts on the contact list home screen or in the directory.</td>
</tr>
</tbody>
</table>

4. Click Update.

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 is set to require 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.

**Support for Lync-hosted Video Conferencing**

Polycom HDX systems can participate directly with Lync-hosted video conferences. To do this, the Polycom HDX system must meet the following requirements:

- It must have the RTV key installed.
- It must be paired with a Polycom Touch Control in order to use call management capabilities.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>• When in a Lync-hosted call, the Polycom HDX system displays a Busy presence state. It rejects any inbound calls.</td>
</tr>
<tr>
<td>• When in a Lync-hosted call, other multipoint calling methods, such as internal multipoint hosting, RMX hosted conferencing, and Conference on Demand, are disabled.</td>
</tr>
<tr>
<td>• Lync-hosted conferencing is only supported when Polycom endpoints are registered to Lync Server.</td>
</tr>
</tbody>
</table>

When the Polycom HDX system has the RTV key installed AND is registered to a Lync Server:

- Participate in Lync-hosted conferences.
- Use 720p high-definition video between Lync clients and Polycom HDX systems.

A Polycom Touch Control is also 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 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 combination of the following methods.

- a Touch **Keypad**, then enter SIP addresses. Each time you enter a SIP address, touch **Add** to add it to the list of 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 the individual names to add them.

- c Touch **Favorites**, then touch the names you want to include in the list of participants.

3 To initiate the conference call, touch **Join** when your list of participants is complete.

After you touch **Join**, the In Call screen is displayed on the Polycom Touch Control. You can touch **Add Participant** to add other participants as described in step 2 without putting other participants on hold, although you might experience a brief audio or video pause.

To view the participants in a call, touch **Participants** from the call screen. You can also view which participants are muted.

**Roles in Lync-hosted Calls**

Participants of Lync-hosted calls are either the organizers, presenters, or attendees. You set up these roles on Microsoft Lync Server 2010, but if you are the conference organizer, you can change roles by using the Lync client. The organizer is the person who set up the call, presenters have some privileges, and attendees have the fewest privileges.

The organizer of a Lync-hosted conference can also choose to leave the conference by touching **Hang Up**.

The following table illustrates privileges given to conference organizers, presenters, and attendees.

<table>
<thead>
<tr>
<th>Role</th>
<th>Add Participant</th>
<th>View Participants</th>
<th>Hang Up Participant</th>
<th>Conference</th>
<th>Self</th>
<th>Mute Participant</th>
<th>Conference</th>
<th>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>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Presenter</td>
<td>Y</td>
<td>Y</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>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

**Note:** Attendees can un mute themselves only if they have been selectively muted. If the organizer has muted the audience, attendees cannot un mute themselves.
Support for High-Quality (RTV) Video

Polycom supports using high-quality video among Microsoft components, Polycom ITP, Polycom HDX endpoints and the Polycom RMX system.

Microsoft clients (both Office Communicator and Lync client) use the RTV (Real-time Video) protocol by default which provides VGA and HD (720p) video. Polycom components support the RTV protocol when participating on calls with Microsoft clients.

Without RTV support, Microsoft clients receive lesser quality video.

RTV Requirements

Polycom supports the RTV protocol with the following products:

• 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.

• 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 are hosted on the HDX system’s internal MCU and use RTV video. If a non-RTV HDX system joins the call, the entire call will be conducted on CIF instead of RTV.
• 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 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.
• For Polycom ITP systems, RTV is used only on point-to-point calls with a Lync client. For point-to-point calls with a Lync client, the Polycom ITP system connects with only the primary codec.
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 topics:

- “Configure Lync Server 2010 for Use with an ITP System” on page 33
- “Configure Your Polycom ITP System for the Microsoft Environment” on page 40
- “Support for High-Quality (RTV) Video” on page 48

**Configure Lync Server 2010 for Use with an ITP System**

When configuring your Microsoft environment, you must:

- “Configure Authentication on the Lync Server” on page 34
- “Enable HD Video on the Lync Server” on page 34
- “Creating and Enabling Conference Room User Accounts” on page 35
- “Hiding the Secondary Codecs in the Lync Directory” on page 37
- “Enable Conference Room Users for Remote Access and Federation” on page 39
Configure Authentication on the Lync Server

Your Microsoft Lync or Office Communications Server must have NTLM enabled in order for an HDX system or ITP system to participate in your Microsoft environment. 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, not Kerberos.

Using Microsoft Call Admission Control

Microsoft Call Admission Control policies are supported and enforced on your HDX system or ITP system.

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 of SIP calls is 2 Mbps.

Enable HD Video on the Lync Server

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

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

To change the default video settings for your Lync Server:

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

   Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M

3. Restart your Lync Server.
Creating and Enabling Conference Room User Accounts

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

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

Each ITP system in your deployment must have a set of conference room user accounts in Active Directory.

The names used for the user accounts must follow the ITP naming convention. 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><a href="mailto:vineyarditp4@abc.com">vineyarditp4@abc.com</a></td>
</tr>
<tr>
<td>Secondary codec</td>
<td><code>~&lt;name&gt;&lt;codec_number&gt;@&lt;domain&gt;</code></td>
<td>~<a href="mailto:vineyard2@abc.com">vineyard2@abc.com</a></td>
</tr>
<tr>
<td>Right codec</td>
<td><code>~&lt;name&gt;&lt;codec_number&gt;@&lt;domain&gt;</code></td>
<td>~<a href="mailto:vineyard3@abc.com">vineyard3@abc.com</a></td>
</tr>
<tr>
<td>Left codec</td>
<td><code>~&lt;name&gt;&lt;codec_number&gt;@&lt;domain&gt;</code></td>
<td>~<a href="mailto:vineyard4@abc.com">vineyard4@abc.com</a></td>
</tr>
</tbody>
</table>

You can use a script, the Active Directory Users and Computers management console, or custom software for this purpose. The procedure below describes adding a conference room user manually in the Active Directory Users and Computers management console.

If your deployment will also include Polycom Conferencing for Outlook, there are additional considerations when creating this user account. See “Configure Mailboxes for Room-based HDX Systems” on page 164.

Note

If these conference room users have an expiring password, you must 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. The

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 about Lync Server 2010 Powershell, see http://blogs.technet.com/b/csp/. 

To enable a conference room user for the Lync Server:

1. Access Lync Powershell.

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

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

You need to enable each conference room user account you created for your ITP system.
Hiding the Secondary Codecs in the Lync Directory

You can hide the Secondary (and subsequent codecs) in the Lync directory in either of these ways:

- 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 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.
5. Click OK.
Hiding the Secondary Codecs in the Directory Using the ADSI Edit Tool


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, and click Edit.

5. On the Boolean Attribute Editor dialog box, select True in the Value field.
6 Click OK.

Enable Conference Room Users for Remote Access and Federation

If you need to support remote users and federated users, you need to configure your Lync Server edge server for that purpose. The following instructions assume you have configured a Lync Server edge server.

In order to support external users, you need to do both of the following:

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

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

Configure Your Polycom ITP System for the Microsoft Environment

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:

- “Register All Codecs with the Lync Server” on page 41
- “Configure the LAN Properties for each Codec” on page 45
- “Configure Display Options for the ITP System Contact List” on page 46
- “Configure AES Encryption” on page 46
Register 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** 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. For guidance, see the below table.

![Polycom system settings when an RTV option key is installed.](image)
Figure 5-5 Polycom system settings without the RTV option key installed.
### Table 5-1  SIP Settings fields and their descriptions

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Mark this check box to enable the HDX system to receive and make SIP calls.</td>
</tr>
<tr>
<td>SIP Server Configuration</td>
<td>Select <strong>Auto</strong> 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 <strong>Specify</strong>.</td>
</tr>
</tbody>
</table>
| 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 an Lync Server environment, specify the DNS name of the Lync Server server. The default port is 5061.  
  - If registering a remote HDX system with an 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.** |
<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server</td>
<td>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 <strong>Auto</strong> for your <strong>SIP Server Configuration</strong> 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. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required. <strong>Auto</strong> enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for Microsoft environments. <strong>TCP</strong> provides reliable transport via TCP for SIP signaling. <strong>UDP</strong> provides best-effort transport via UDP for SIP signaling. <strong>TLS</strong> provides secure communication of the SIP signaling. <strong>TLS</strong> 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. <strong>TLS</strong> is required when connecting to a Microsoft Lync or Office Communications server.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the domain name for authentication with the LDAP server. You can leave this field blank when you use a UPN (<a href="mailto:username@domainname.com">username@domainname.com</a>) in the <strong>User Name</strong> field (recommended).</td>
</tr>
<tr>
<td>Sign-in Address</td>
<td>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. <strong>Note:</strong> If you have not installed the RTV option key, this setting is named <strong>User Address</strong>.</td>
</tr>
</tbody>
</table>
Deployment Process for Polycom Immersive Telepresence Systems

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 on to “Configure the LAN Properties for each Codec” on page 45.

**Configure 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.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Specifies the name to use for authentication when registering with a SIP Registrar Server—for example, <a href="mailto:jsmith@company.com">jsmith@company.com</a>.</td>
</tr>
<tr>
<td></td>
<td>Polycom supports the User Principal Name format (<a href="mailto:username@domain.com">username@domain.com</a>) as well as the legacy Microsoft DOMAIN\username format.</td>
</tr>
<tr>
<td></td>
<td>If the SIP server requires authentication, this field and the password cannot be blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you have not installed the RTV option key, this setting is named <strong>Domain User Name</strong>.</td>
</tr>
<tr>
<td>Password</td>
<td>When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP Server.</td>
</tr>
<tr>
<td>Directory: Microsoft Lync Server</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 on to “Configure the LAN Properties for each Codec” on page 45.

**Configure 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.
Click Update.

**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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Contacts</td>
<td>Specifies whether to display your contacts on the contact list home screen and in the directory.</td>
</tr>
<tr>
<td>Show My Offline Contacts</td>
<td>Specifies whether to include offline contacts on the contact list home screen or in the directory.</td>
</tr>
</tbody>
</table>

4. Click **Update**.

**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 is set to require 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.

Lync-hosted Video Conferencing Not Supported

Polycom ITP systems cannot participate in multipoint calls hosted by a Lync AVMCU.
Support for High-Quality (RTV) Video

Polycom supports using high-quality video among Microsoft components, Polycom ITP, Polycom HDX endpoints and the Polycom RMX system.

Microsoft clients (both Office Communicator and Lync client) use the RTV (Real-time Video) protocol by default which provides VGA and HD (720p) video. Polycom components support the RTV protocol when participating on calls with Microsoft clients.

Without RTV support, Microsoft clients receive lesser quality video.

Note

- RTV video is only supported when Polycom endpoints are registered to Lync Server or an Office Communications Server.

RTV Requirements

Polycom supports the RTV protocol with the following products:

- 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.

- 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 are hosted on the HDX system’s internal MCU and use RTV video. If a non-RTV HDX system joins the call, the entire call will be conducted on CIF instead of RTV.
- 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 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.
- For Polycom ITP systems, RTV is used only on point-to-point calls with a Lync client. For point-to-point calls with a Lync client, the Polycom ITP system connects with only the primary codec.
Deployment Process for 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.

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

You need to do the following:

1. “Configuring Your RMX System for use with the Lync Server” on page 50
2. “Configure Your Lync Server for Use with an RMX System” on page 58
3. “Enabling Microsoft Presence” on page 61
4. See “Enabling Edge Server Integration with your RMX System” on page 67 if you need to configure federation.

Note: 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.
Configuring Your RMX System for use with the Lync Server

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

Do the following:

- “Set up the RMX System for Security and SIP” on page 50
- “Create a Security Certificate for the Polycom RMX System” on page 52
- “Configure Encryption for your Deployment” on page 57
- “Enabling Edge Server Integration with your RMX System” on page 67

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 tasks:

- “Configuring the RMX IP Network Service” on page 50
- “Add the RMX FQDN (SIP signaling IP address) in DNS” on page 51

Task 1: Configuring 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 ( , or ) entry.
   The Default IP Service - Networking IP dialog box opens.
4. Make sure the IP Network Type is set to H.323 & SIP even though SIP will be the only call setup used 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 selected 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 box 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 10.10.10.1 as the IP address of the RMX signaling host.

**Figure 6-1** Create the DNS A record for the RMX system.

4 Click **Add Host**.

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

**Create a Security Certificate for the Polycom RMX System**

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

This can be accomplished in 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 certificate requests must be submitted through the enterprise’s CA team or group, use the procedures in the Polycom RMX 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 Internet Information Services (IIS) Manager on the Lync Server. From it, you can then
download an export file of the certificate to your PC for later installation on the Polycom RMX system. This procedure is described below.

**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.

*Figure 6-2*  Create a security certificate in IIS 7.

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

*Figure 6-3*  Select Create Domain Certificate.

The **Create Certificate** wizard displays.
5 In the **Distinguished Name Properties** panel, complete all fields. Do not leave any fields blank.

*Figure 6-4  Create the new certificate.*

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, 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 page, select Computer Account and click Next.

   \[Figure 6-5 \ Select \ Computer \ Account.\]

   ![Select Computer Account](image)

   d. On the Select Computer page, select Local Computer.

   \[Figure 6-6 \ Select \ Local \ Computer.\]

   ![Select Local Computer](image)

   e. Click Finish.

2. Click OK.

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

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

![Figure 6-7: Select Include all certificates in the certification path if possible.](image)

d. Click Next.

e. In the Password panel, enter a simple password, e.g., 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, e.g., `c:\temp\rmxcert.pfx`.

**Install 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.
Configure Encryption for your Deployment

By default, Microsoft Lync Server is enabled to require encryption. You need to ensure that your RMX system encryption settings are compatible with your Lync Server.

For example, you may need to support legacy H.323 endpoints that 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 encryption for the RMX system, see Chapter 2, Additional Conferencing Information in the Polycom RMX System Administrator’s Guide.


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 needed, 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
Configure Your Lync Server for Use with an RMX System

The RMX 1500/2000/4000 system can host multiple video endpoints in a single conference, as well as host multiple conferences simultaneously. For these reasons, the RMX 1500/2000/4000 system is configured as a trusted application rather than 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 http://technet.microsoft.com/en-us/library/gg398474.aspx.

In this section, do the following to set the Lync routing for the Polycom RMX system:

• “Use Lync Topology Builder to define your trusted application pool” on page 58
• “Use Lync Powershell to set the Polycom RMX system as a trusted host with a static route” on page 59
• “Use Lync Powershell to create the trusted application” on page 60
• “Use Lync Powershell to update the topology” on page 61

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.

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" on page 14 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 set the Polycom RMX 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 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.


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

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.

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


   Table 6-1  CsTrustedApplication parameter definitions.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>-ApplicationId</td>
<td>A descriptive name for the application. Must be unique within your Lync deployment.</td>
</tr>
<tr>
<td>-TrustedApplicationPoolFQDN</td>
<td>The FQDN of the application pool. In our example, sipdomain.com.</td>
</tr>
<tr>
<td>-port</td>
<td>The SIP port. The default port number for SIP is 5061.</td>
</tr>
</tbody>
</table>

Task 4: Use Lync Powershell 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 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 Lync clients. To do this you need to complete steps in both your Microsoft environment and in your RMX system.

You can register a limited number of RMX system meeting rooms with Lync.

- The RMX 1500 and 2000 systems support registration of up to 24 rooms.
- The RMX 4000 system supports registration of up to 48 rooms.

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

- “Configure your Microsoft Environment to Support RMX Room Presence” on page 61
- “Configure your RMX System for Microsoft Presence” on page 65

Configure your Microsoft Environment to Support RMX Room Presence

To register RMX conferencing entities, do the following:

- “Creating an Active Directory Account for the Conferencing Entity” on page 62
- “Enabling the Active Directory Account for Lync Server” on page 63
- “Enable the RMX Account for Remote Access and Federation” on page 64
**Task 1: Creating 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 which was previously defined as the **Server Domain Name** entry in the RMX SIP Servers configuration (see “Configuring the RMX IP Network Service” on page 50).

Note: Each RMX conferencing entity must have a unique Active Directory account. For example, you cannot 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, enter the required user information.

   *Figure 6-8 Use the RMX VMR name in the User logon name field.*

   ![New Object - User](image)

   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.
Click Next and then Finish.

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 is how this room will appear 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: Enabling 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.

   The Windows Security window opens.

2. Enter the 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 box 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 box.

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

   The selected user appears in the New Lync Server User pane.

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 you will use only the vmr10 portion of the address.

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.

Figure 6-9  Generate the user SIP URI.

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

You should also enable remote access if the conferencing entity will be used in federated conference calls.


For detailed information on setting up a federated environment, see “Enabling Edge Server Integration with your RMX System” on page 67
Configure your RMX System for Microsoft Presence

After you have completed the steps listed in “Configure your Microsoft Environment to Support RMX Room Presence” on page 61, you need to ensure that the conference entity has been enabled for SIP within the RMX system. Do the following:

- “Enabling SIP Registration in the Conference Profile” on page 65
- “Create or Modify the RMX Conferencing Entity” on page 66

Task 1: Enabling SIP Registration in the Conference Profile

Conference entities that require SIP registration must use a conference profile that has been enabled for SIP.

If meeting rooms are not assigned a conference profile that is enabled for SIP registration, the meeting room will not register.

By default, SIP registration is disabled in conference profiles, and must be enabled in the profile assigned to conferencing entities that require SIP registration.

To enable SIP registration for a conference profile

1. Using the RMX management console, create a new profile or edit an existing profile.

2. On the Network Services tab, mark the SIP Registration check box.

Figure 6-10  Register the RMX conference profile with the Lync Server.

3. Click OK.
Task 2: Create or Modify the RMX Conferencing Entity

You must edit or create an RMX conferencing entity that matches the Active Directory account you created.

1. Create or edit an RMX meeting room or conferencing entity.
   - 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.

   Figure 6-11  Use the SIP URI of the Lync account as the Routing Name.

2. In the Profile drop-down menu, be sure to select a conference profile that has been 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 RMX System

This topic assumes that you have already configured the RMX SIP signalling domain as a trusted application. See “Configure Your Lync Server for Use with an RMX System” on page 58.

When your RMX system is configured with a Microsoft Edge Server, you can take advantage of the following Microsoft features:

- ICE media support
- Federation
- External User Access
- Call Admission Control

Call Admission Control policies are managed on your Microsoft Lync Server.

To enable federated connections with the Polycom RMX system and support Microsoft Call Admission Control policies, do the following steps.

- “Creating an Active Directory Account for the RMX System” on page 68
- “Enabling the RMX User Account for Lync Server Edge Server” on page 69.
- “Enable the RMX Account for Remote Access and Federation” on page 70
- “Configuring the RMX System for Federated Dialing” on page 70
- “Configure RMX System Flags for Federation and Microsoft Call Admission Control” on page 71

Edge Server Considerations for the Polycom RMX System

- The firewall must be UDP enabled.
- The RMX system must have a unique account in Active Directory and must be registered with the Lync Server edge server.
- A TLS connection is required.
- 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). See “Enable Federation in your Environment” on page 87 for an overview of scenarios with and without a DMA system.
Task 1: Creating 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.

This account must be a dedicated account that is enabled for the Lync Server. Because the RMX system has been added as a trusted application, the password is not important. 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, enter the required user information.

   Figure 6-12 Enter the information for the RMX edge server account.

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: Enabling 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. This SIP URI will be entered 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 box opens.
6. Enter the conferencing entity user name you defined in the Active Directory, and then click the **Find** button.
   The requested user is listed in the **Select From Active Directory** dialog box.
7. Select the listed user and click **OK**.
   The selected user appears 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 selected user appears as enabled in the User Search pane.
Task 3: Enable the RMX Account for Remote Access and Federation

You need to configure the RMX system account for remote access and federation. The following instructions assume you have configured a Lync Server edge server.

In order to support 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:


Task 4: Configuring the RMX System for Federated Dialing

The Default IP Network Service for the RMX system must be configured to work with the Lync Server 2010 edge server as the SIP Server and the RMX user defined in the Active Directory must also be defined in the RMX ICE environment parameters.

The procedure described here assumes that the RMX is configured to work in Microsoft environment; 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 the RMX Administrator’s Guide, Appendix H.

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 ( , , or ) entry.
   The Default IP Service - Networking IP dialog box 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.
7. In the Server User Name field, enter the SIP URI that was defined for the user you created in Active Directory. For example, enter rmx1edge.
8. In the ICE Environment field, select MS (for Microsoft ICE implementation).
Figure 6-13  Configure the RMX system for an Microsoft edge server.

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**

You need to 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 *RMX 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 box.

**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 to which it is connected and the connection status.

   It addition, the system indicates the status of the firewall detection in the RMX system.
Deployment Process for Polycom DMA Systems

When you incorporate a Polycom DMA system within your Microsoft 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.

You need to perform steps in both your DMA system and the Microsoft environment.

- “Configure Your DMA System for your Environment” on page 74
- “Configure Your Microsoft Environment for Use with a DMA System” on page 83
Configure Your DMA System for your Environment

This section provides an outline of the tasks required to configure Polycom DMA system with Lync Server 2010.

• “Ensure DNS is Configured Properly” on page 74
• “Create a Security Certificate for the Polycom DMA 7000 System” on page 74
• “Configure a DMA System SIP Peer for the Lync Server” on page 79

Ensure DNS is Configured Properly

Before you proceed, make certain that:

• You have all the fully qualified domain names (FQDNs) of the system for which you’re creating a certificate. A two-node system has three: one virtual and two physical; a single-node system has two: one virtual and one physical.

• These host names 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

You must install a security certificate on the DMA system so that Lync Server trusts it. This can be accomplished in 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 DMA 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 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 Internet Information Services (IIS) Manager on the Lync Server. From it, you can then download an export file of the certificate to your PC for later installation on the Polycom DMA system. This procedure is described below.
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.

**Figure 7-1** Create a security certificate in IIS 7.

4. In the Actions pane (far right), select the Create Domain Certificate action.

**Figure 7-2** Select Create Domain Certificate.

The Create Certificate wizard displays.

5. In the Distinguished Name Properties panel, complete all fields. Do not leave any fields blank.
Create the new certificate.

- In the Common Name field, enter the FQDN of DMA virtual host name. This name must match what is in the DNS.
- Do not leave any fields blank.

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, 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 page, select Computer Account and click Next.

   **Figure 7-4** Select Computer Account.

   ![Select Computer Account](image)

   d. On the Select Computer page, select Local Computer.

   **Figure 7-5** Select Local Computer.

   ![Select Local Computer](image)

   e. Click Finish.

2. Click OK.

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

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

5. In the Certificate Export wizard, do the following:
   a. In the Export Private Key panel, select Yes, export the private key.
   b. Click Next.
   c. In the Export File Format panel, select Include all certificates in the certification path if possible.
Figure 7-6  Select Include all certificates in the certification path if possible.

- Click Next.
- In the Password panel, enter a simple password, e.g., password.
- Click Next.
- In the File to Export panel, enter a path where you want to save the new file, e.g., c:\temp\dmacert.pfx.
- 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 the Lync Server

You can configure the Polycom DMA system as a SIP proxy and registrar for your Polycom environment.

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

**Note**

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

Perform the following steps to create a SIP peer and establish the call routing infrastructure.

- “Configure a SIP Peer in the DMA System” on page 79
- “OPTIONAL Configure your DMA System to Route to Specific SIP Domains” on page 80
- “Set up a Dial Rule for the Lync Server” on page 81

**Task 1: Configure a SIP Peer in the DMA System**

Within the DMA system, you need to 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.
4. In the Actions menu, click Add.
5. Ensure that the Enabled check box is marked.
6. Type a name and description for the SIP Peer.
7. In the Address field, type the FQDN address of Microsoft server (Office Communications Server or Lync Server).
8. In the Port field, enter the SIP port to use. Use the default SIP port of 5061.
9. Leave the Prefix field blank.

Prefixes can be used if your environment includes heterogenous 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.
10 In the **Type** drop-down list, select **Microsoft OCS**.

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

*Figure 7-7*  
*Create and enable the SIP peer.*

12 Ensure the **Register Externally** check box is unmarked.

Some external SIP peers (Acme SBC, for example) require peer proxies to register with them. The Microsoft Lync Server does not.

13 Click **OK**.

Once these steps have been completed, outgoing SIP calls will be routed to the endpoints registered to the Microsoft (Office Communications Server or Lync Server) server.

**Note**

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 Preliminary Script that will ensure the string is compatible with Microsoft call extensions. For example, you can include a Preliminary script that strips the dial string of any prefix that isn’t compatible with Lync.

Please consult the *Polycom DMA 7000 System Operations Guide* for more information.

**Task 2: OPTIONAL Configure your DMA System to Route to Specific SIP Domains**

Optionally, you can configure specific SIP domains that are associated with the SIP peer you created. If you do not configure specific SIP domains, the DMA system will route calls to any SIP domain.

When you configure specific SIP domains, DMA restricts call routing to only the SIP domains you configure.
To configure the DMA system to use a specific SIP Domain

1. Navigate to Network > External SIP Peer.
2. Select Domain List.
3. Enter the name of the SIP domain and click Add. For example, sipdomain.com.

Figure 7-8 An authorized domain if you want to restrict calls to specific domains.

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

As a best practice, the dial rule you use for the Lync Server should be last in your logical list of dial rules. Please see the DMA system documentation for detailed information about using dial rules.

To set up a dial rule for Lync Server calls

1. Select Admin > Call Server > Dial Rules.
2. Click Add.
3. In the Add Dial Rule dialog box, enter a description for your dial rule.
4. In the Action drop-down menu, select Resolve to external SIP peer.
5. In the Available SIP Peers area, select the Microsoft server and move it to the Selected Peers area using the arrow.
6 Ensure you mark the **Enabled** check box.
7 Click **OK**.
Configure Your Microsoft Environment for Use with a DMA System

You need to set up your Microsoft environment to route calls to the DMA system.

In this section, do the following steps:

• “Set the Routing for the Polycom DMA System” on page 83
• “Enable Federation in your Environment” on page 87

Set the Routing for the Polycom DMA System

Perform the following procedure to enable the Polycom DMA system to receive Lync Server calls.

Polycom recommends using Lync Powershell commands to perform the following tasks. For detailed documentation for Lync Powershell, see http://technet.microsoft.com/en-us/library/gg398474.aspx.

Do the following to set the Lync routing for the Polycom DMA system:

• “Use Lync Topology Builder to define your trusted application pool” on page 83
• “Use Lync Powershell to set the Polycom DMA system as a trusted host with a static route” on page 85
• “Use Lync Powershell to create the trusted application” on page 86
• “Use Lync Powershell to update the topology” on page 86

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.

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” on page 14 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.

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.

Figure 7-10 Click Yes on the Missing Machine warning.
Task 2: Use Lync Powershell to set the Polycom 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).


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
   ```

Table 7-1  CsTrustedApplication parameter definitions.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>-ApplicationId</td>
<td>A descriptive name for the application. Must be unique within your Lync deployment.</td>
</tr>
<tr>
<td>-TrustedApplicationPoolFQDN</td>
<td>The FQDN of the application pool.</td>
</tr>
<tr>
<td>-port</td>
<td>Enter the SIP port. The default port for SIP is 5061.</td>
</tr>
</tbody>
</table>


Task 4: Use Lync Powershell 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.

   ```powershell
   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 Environment

Federation is only supported for Polycom endpoints and devices registered to a Microsoft Lync Server or Microsoft Office Communications Edge Server.

Task 1: Ensure the Microsoft Lync Edge Server Role is Configured

Consult your Lync Server 2010 documentation for full instructions on how to include a Lync Server 2010 edge server to your environment.

For more information, see the Edge Configuration Guide which is available at: http://technet.microsoft.com/en-us/library/gg398918.aspx

Microsoft also provides an Edge Server Planning Tool which is available at: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=bc64040-40c4-4714-9e68-c649785cc43a

Deployment Considerations:
• 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 used 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.

Examples:
1 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
2 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 signalling 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
This chapter describes how to implement Polycom-enabled unified communications, which integrates Polycom systems with the Microsoft infrastructure for presence-based real-time instant messaging (IM), voice, video, and data communications. It includes instructions for configuring the Microsoft Office Communications Server components and integrating and configuring the Polycom components required for this solution.

This guide does not describe or provide full administration or maintenance processes or procedures for Microsoft Office Communications Server 2007. For any questions or assistance on Microsoft Office Communications Server 2007, see the Microsoft documentation and/or Microsoft Support Services.

This chapter includes the following sections:

- “Solution Overview for Office Communications Server Environments” on page 90
- “Deployment Process for Office Communications Server” on page 94
- “Deployment Process for Polycom HDX Systems” on page 101
- “Deployment Process for Polycom RMX Systems” on page 123
- “Deployment Process for Polycom RMX Systems” on page 123
- “Deployment Process for Polycom DMA System” on page 126
- “Setting up Dialing Plans” on page 129
Polycom Solution Support Services

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. UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations.

Please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative for more information.

Solution Overview for Office Communications Server Environments

Polycom’s integration with Microsoft Office Communication Server provides the following functionality:

- Enables point-to-point calls between Polycom HDX systems and Microsoft communicator clients.
- Provides real-time presence information between Polycom devices and Microsoft Communicator clients.
- Enables support for remote and federated endpoints to participate in point-to-point calls and video conference calls.
- Supports high-quality video (720p) between Office Communicator clients and Polycom endpoints.
- Allows Microsoft Communicator clients to view the presence for Polycom RMX meeting rooms and start one-click conferences.

One-click conferencing from Office Communicator clients to an RMX system is an optional feature. Contact Polycom technical support for more information.

Key Concepts

Polycom products in the unified communications solution 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.
Be sure you are familiar with the following concepts before proceeding.

**Microsoft Domain Accounts**

In order to be 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.
- Domain accounts need the proper capabilities and settings. Some settings are set at the domain level (with policies) and some are set at the account level.

**Encryption and Security**

- TLS is required in Microsoft environments, which means security certificates must be used.
- You can configure call encryption. Remember that 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.
# Products that Enable Unified Communications

The following table describes the Polycom products that support or enhance the Polycom integration 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>
<tr>
<td>Polycom HDX system</td>
<td>v3.0.3</td>
<td>Video endpoint systems that can be integrated into a Microsoft environment. <strong>Advance Microsoft Support</strong> 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</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. • Polycom RPX 200 and 400 systems • Polycom OTX 300 and 100 systems • Polycom TPX 306M system • Polycom ATX SDK and ATX 300 system</td>
</tr>
<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>
<tr>
<td><strong>Peripherals</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polycom Touch Control</td>
<td>1.3.0</td>
<td>Provides HDX call control and administration.</td>
</tr>
</tbody>
</table>
Note

If your deployment includes Polycom CX phones (CX700, CX500, CX300 or CX3000), Office Communications Server must have the Enterprise Voice option implemented, and the users must be enabled for enterprise voice. See Microsoft’s Office Communications Server 2007 Enterprise Voice Planning and Deployment Guide.
Deployment Process for Office Communications Server

This section describes how to configure Office Communications Server as required for this solution. You must perform these tasks in this order:

1. “Prepare for the Implementation” on page 94
2. “Configure Authentication in Office Communications Server” on page 94
3. “Add Conference Rooms with Polycom HDX Systems to Active Directory” on page 96
4. “Enable Conference Rooms for the Office Communications Server” on page 96
5. “Enable Conference Rooms for Remote Access and Federation” on page 97
6. “Add Contacts to the Conference Room Local Address Book” on page 98
7. “Configure the Office Communications Server Server Pool Encryption Setting” on page 100

Note: Your Microsoft Office Communicator users should already be properly configured in Microsoft Active Directory and Microsoft Office Communications Server. See your Microsoft Active Directory and Office Communications Server administrators or the Microsoft web site if you have questions regarding the configuration of Microsoft Active Directory and Office Communications Server.

Task 1: Prepare for the Implementation

Before beginning, the person deploying this solution must 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

For this solution, you must enable NTLM in Office Communications Server. The Polycom HDX system and RMX 2000/4000 systems support only NTLM authentication, not 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.

3. In the Front End Properties dialog box, select the Authentication tab.

4. 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

In Active Directory, you must first create a conference room user for each conference room that will have a Polycom HDX system. You can use a script, the Active Directory Users and Computers management console, or custom software for this purpose. The procedure below describes adding a conference room user manually in the Active Directory Users and Computers management console.

If your deployment will also include Polycom Conferencing for Outlook, there are additional considerations when creating this user account, see “Configure Mailboxes for Room-based HDX Systems” on page 164.

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 box, select the format used to generate the conference room’s SIP URI and click **Next**.

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

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

If you need to support remote users and federation, you need to configure the conference room users for that purpose. The following instructions assume you have configured an Office Communications Server edge server. For additional information about supporting federation and remote users, see “Supporting Remote Users” on page 123.

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. 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 6: Add Contacts to the Conference Room Local Address Book

You can use the LCSAddContacts script from the Microsoft Office Communications Server Resource Kit to add a list of contacts to the local address books of conference rooms with Polycom HDX systems.

Office Communications Server will provide real-time presence information for these contacts. A Polycom HDX system can have up to 200 such contacts per conference room user.

The script accepts two text files as parameters — a users list file 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 users.txt file that it used.

Note: Polycom recommends that the Office Communications Server be configured to allow no more than 200 contacts per user (the default setting). The HDX system displays only 200 contacts per user. If the Office Communications Server user has more than 200 contacts, the HDX system will not display them consistently.

To add a list of contacts to each conference room user

1. Create a users.txt file that specifies the conference room users you enabled and configured in Office Communications Server.

   The users 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 users 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:
If you have not already, download and install the Office Communications Server 2007 R2 Resource Kit Tools from the following URL:


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.

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 being added. If you omit it, the 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 Server Pool Encryption Setting

Office Communications Server is set to require encryption by default. Both the Office Communications Server server pool and the Polycom HDX system need to be configured to support encryption in order for calls to connect with some level of encryption.

- If both components have encryption turned off, calls connect without encryption.
- If one component is set to require encryption and the other is 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.
Deployment Process for Polycom HDX Systems

Your Polycom HDX system should be installed according to standard installation procedures. See the Setting Up the System guide for your model of Polycom HDX system, which describes how to set up the hardware. Then perform the following tasks:

- “Register Polycom HDX Systems with the Office Communications Server” on page 101
- “Configure the Polycom HDX System LAN Properties” on page 105
- “Configure Display Options for Contact List” on page 106
- “Configure AES Encryption” on page 107

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

When an HDX system is registered with an Office Communications Server, the Polycom HDX system user can see a list of Office Communications Server contacts, see if the contacts are online, and call them without knowing or remembering their addresses. Contacts appear in the directory and can also be displayed on the home screen.

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. For guidance, see the below table.

Note: If registering a remote HDX system with an Office Communications Server edge server, use the fully qualified domain name of the access edge server role, see “Setting up Dialing Plans” on page 129 for complete information.
**Figure 8-1** Polycom system settings when an RTV option key is installed.

**Figure 8-2** Polycom system settings without the RTV option key installed.
<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Mark this check box to enable the HDX system to receive and make SIP calls.</td>
</tr>
<tr>
<td>SIP Server Configuration</td>
<td>Select <strong>Auto</strong> 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 <strong>Specify</strong>.</td>
</tr>
<tr>
<td>Server Name or IP Address</td>
<td>If you selected <strong>Specify</strong> in the <strong>SIP Server Configuration</strong> field, you need to specify the IP address or DNS name of the SIP Registrar Server.</td>
</tr>
<tr>
<td></td>
<td>• In an Lync Server environment, specify the DNS name of the Lync Server server. The default port is 5061.</td>
</tr>
<tr>
<td></td>
<td>• If registering a remote HDX system with an 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.</td>
</tr>
<tr>
<td></td>
<td>• You can also enter the name of a Lync Director Server.</td>
</tr>
<tr>
<td></td>
<td>Polycom recommends using the DNS name. The format for entering the address and port is the following:</td>
</tr>
<tr>
<td></td>
<td>&lt;DNS_NAME&gt;::&lt;TCP_Port&gt;::&lt;TLS_Port&gt;</td>
</tr>
<tr>
<td></td>
<td>Syntax Examples:</td>
</tr>
<tr>
<td></td>
<td>• To use the default port for the protocol you have selected:</td>
</tr>
<tr>
<td></td>
<td>lyncserver.corp.local</td>
</tr>
<tr>
<td></td>
<td>• To specify a different TLS port (and use the default TCP port):</td>
</tr>
<tr>
<td></td>
<td>lyncserver.corp.local::443</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If you have not installed the RTV option key, this setting is named <strong>Registrar Server</strong>.</td>
</tr>
<tr>
<td>Settings</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>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. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required. <strong>Auto</strong> enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for Microsoft environments. <strong>TCP</strong> provides reliable transport via TCP for SIP signaling. <strong>UDP</strong> provides best-effort transport via UDP for SIP signaling. <strong>TLS</strong> provides secure communication of the SIP signaling. <strong>TLS</strong> 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.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the domain name for authentication with the LDAP server. You can leave this field blank when you use a UPN (<a href="mailto:username@domainname.com">username@domainname.com</a>) in the User Name field (recommended).</td>
</tr>
<tr>
<td>Sign-in Address</td>
<td>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. <strong>Note:</strong> If you have not installed the RTV option key, this setting is named User Address.</td>
</tr>
</tbody>
</table>
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 registering a remote Polycom system, use a DNS server that the system shares DNS zone information with the Lync Server edge server.
5 Click Update.

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

To configure the 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 Microsoft Lync Server section of the Directory Servers page, configure these settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Contacts</td>
<td>Specifies whether to display your contacts on the contact list home screen and in the directory.</td>
</tr>
<tr>
<td>Show My Offline Contacts</td>
<td>Specifies whether to include offline contacts on the contact list home screen or in the directory.</td>
</tr>
</tbody>
</table>

4 Click Update.
Task 4: Configure AES Encryption

The Polycom HDX system supports AES (media) encryption. You need to set your HDX system encryption settings to be compatible with your Office Communications Server settings.

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

• If both components have encryption turned off, calls connect without encryption.
• If one component 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.
Deployment Process for Polycom Immersive Telepresence Systems

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.

This section contains the following topics:

- “Configure Office Communications Server for Use with an ITP System” on page 108
- “Deployment Process for Polycom HDX Systems” on page 101
- “Support for High-Quality (RTV) Video” on page 122

Configure Office Communications Server for Use with an ITP System

When configuring your Microsoft environment, you must:

- “Configure Authentication on the Office Communications Server” on page 108
- “Enable HD Video on the Office Communications Server” on page 109
- “Add a Conference Room User for each Codec within your ITP System” on page 110
- “Hiding the Secondary Codecs in the Directory” on page 112
- “Enable Conference Rooms for Remote Access and Federation” on page 97

Task 1: Configure Authentication on the Office Communications Server

Your Microsoft Lync or Office Communications Server must have NTLM enabled in order for an HDX system or ITP system to participate in your Microsoft environment. 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, not Kerberos.

Task 2: Using 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 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 video (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 box, select the Video tab.
5. In the **Client video settings** area of the **Video** tab, 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

Each ITP system in your deployment must have a set of conference room user accounts in Active Directory.

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 Office Communications Server. If needed, you should then enable HDX users for remote access and federation.

The names used for the user accounts must follow the ITP naming convention. 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><a href="mailto:vineyarditp4@abc.com">vineyarditp4@abc.com</a></td>
</tr>
<tr>
<td>Secondary codec</td>
<td>~&lt;name&gt;&lt;codec_number&gt;@&lt;domain&gt;</td>
<td>~<a href="mailto:vineyard2@abc.com">vineyard2@abc.com</a></td>
</tr>
<tr>
<td>Right codec</td>
<td>~&lt;name&gt;&lt;codec_number&gt;@&lt;domain&gt;</td>
<td>~<a href="mailto:vineyard3@abc.com">vineyard3@abc.com</a></td>
</tr>
<tr>
<td>Left codec</td>
<td>~&lt;name&gt;&lt;codec_number&gt;@&lt;domain&gt;</td>
<td>~<a href="mailto:vineyard4@abc.com">vineyard4@abc.com</a></td>
</tr>
</tbody>
</table>

You can use a script, the Active Directory Users and Computers management console, or custom software for this purpose. The procedure below describes adding a conference room user manually in the Active Directory Users and Computers management console.

If your deployment will also include Polycom Conferencing for Outlook, there are additional considerations when creating this user account. See “Configure Mailboxes for Room-based HDX Systems” on page 164.

Note

If these conference room users have an expiring password, you must 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:
   
   \texttt{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:
   
   \texttt{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 box, select the format used to generate the conference room’s SIP URI and click **Next**.

5. In the **Enable Operation Status** dialog box, 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 Office Communications Server directory in either of these ways:

- 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 ADSI Edit tool on the Office Communications 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.

5. Click OK.

Figure 8-3 Exchange User Properties General Tab.
Hiding the Secondary Codecs in the Directory Using the ADSI Edit Tool


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.

**Figure 8-4** ADSI Edit Screen.

4. Select the attribute named `msExchHideFromAddressLists`, and click Edit.
5. On the Boolean Attribute Editor dialog box, select True in the Value field.
Click OK.

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

If you need to support remote users and federated users, you need to configure your Lync Server edge server for that purpose. The following instructions assume you have configured a Lync Server edge server.

In order to support external users, you need to do both of the following:

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

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

Configure Your Polycom ITP System for the Microsoft Environment

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:

- “Register All Codecs with the Office Communications Server” on page 115
- “Configure the LAN Properties for each Codec” on page 120
- “Configure Display Options for the ITP System Contact List” on page 120
- “Configure AES Encryption” on page 121

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

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

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. For guidance, see the below table.

**Note** If registering a remote ITP system with an Office Communications Server edge server, use the fully qualified domain name of the access edge server role.
**Figure 8-6** Polycom system settings when an RTV option key is installed.

**Figure 8-7** Polycom system settings without the RTV option key installed.
### Table 8-3  
SIP Settings fields and their descriptions

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Mark this check box to enable the HDX system to receive and make SIP calls.</td>
</tr>
<tr>
<td>SIP Server Configuration</td>
<td>Select <strong>Auto</strong> if your Microsoft server (Lync or Office Communications Server) configuration is set up for automatic discovery.</td>
</tr>
<tr>
<td></td>
<td>If Microsoft server (Lync or Office Communications Server) is not configured for automatic discover, you need to select <strong>Specify</strong>.</td>
</tr>
<tr>
<td>Server Name or IP Address</td>
<td>If you selected <strong>Specify</strong> in the <strong>SIP Server Configuration</strong> field, you need to specify the IP address or DNS name of the SIP Registrar Server.</td>
</tr>
<tr>
<td></td>
<td>• In an Lync Server environment, specify the DNS name of the Lync Server server. The default port is 5061.</td>
</tr>
<tr>
<td></td>
<td>• If registering a remote HDX system with an 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.</td>
</tr>
<tr>
<td></td>
<td>• 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:</td>
</tr>
<tr>
<td></td>
<td>&lt;DNS_NAME&gt;::&lt;TCP_Port&gt;::&lt;TLS_Port&gt;</td>
</tr>
<tr>
<td></td>
<td>Syntax Examples:</td>
</tr>
<tr>
<td></td>
<td>• To use the default port for the protocol you have selected:</td>
</tr>
<tr>
<td></td>
<td>lyncserver.corp.local</td>
</tr>
<tr>
<td></td>
<td>• To specify a different TLS port (and use the default TCP port):</td>
</tr>
<tr>
<td></td>
<td>lyncserver.corp.local::443</td>
</tr>
<tr>
<td><strong>Note</strong>:</td>
<td>If you have not installed the RTV option key, this setting is named <strong>Registrar Server</strong>.</td>
</tr>
</tbody>
</table>
### 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**.
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 “Configure the Polycom HDX System LAN Properties” on page 105.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Specifies the name to use for authentication when registering with a SIP Registrar Server—for example, <a href="mailto:jsmith@company.com">jsmith@company.com</a>. Polycom supports the User Principal Name format (<a href="mailto:username@domain.com">username@domain.com</a>) as well as the legacy Microsoft DOMAIN\username format. If the SIP server requires authentication, this field and the password cannot be blank. <strong>Note:</strong> If you have not installed the RTV option key, this setting is named <strong>Domain User Name</strong>.</td>
</tr>
<tr>
<td>Password</td>
<td>When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP Server.</td>
</tr>
<tr>
<td>Directory: Microsoft Lync Server</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Contacts</td>
<td>Specifies whether to display your contacts on the contact list home screen and in the directory.</td>
</tr>
<tr>
<td>Show My Offline Contacts</td>
<td>Specifies whether to include offline contacts on the contact list home screen or in the directory.</td>
</tr>
</tbody>
</table>

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 is set to require 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.
Support for High-Quality (RTV) Video

Polycom supports using high-quality video among Microsoft components, Polycom ITP, Polycom HDX endpoints and the Polycom RMX system.

Microsoft clients (both Office Communicator and Lync client) use the RTV (Real-time Video) protocol by default which provides VGA and HD (720p) video. Polycom components support the RTV protocol when participating on calls with Microsoft clients.

Without RTV support, Microsoft clients receive lesser quality video.

Note: RTV video is only supported when Polycom endpoints are registered to Lync Server or an Office Communications Server.

RTV Requirements

Polycom supports the RTV protocol with the following products:

- 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.

- 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 are hosted on the HDX system's internal MCU and use RTV video. If a non-RTV HDX system joins the call, the entire call will be conducted on CIF instead of RTV.
- 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 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.
- For Polycom ITP systems, RTV is used only on point-to-point calls with a Lync client. For point-to-point calls with a Lync client, the Polycom ITP system connects with only the primary codec.
Deployment Process for Polycom RMX Systems

The RMX 2000/4000 system can host multiple video endpoints in a single conference, as well as host multiple conferences simultaneously. For these reasons, the RMX 2000/4000 system is configured as a trusted application rather than 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, see “Setting up Dialing Plans” on page 129.

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 configuring DNS.

Using Multiple Computer Application Pools

As a best practice, you should create a multiple trusted application pool and include your DMA system or RMX system SIP signaling domains as nodes under this pool. See Figure 8-8 for an example.

This method simplifies your Microsoft unified communications environment and also allows you to add additional RMX systems or DMA systems at a later time.

Figure 8-8  Using a multiple-computer Trusted application server pool.
In Figure 8-8, video.corp.local is the pool name. 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. This can be done by 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 then Polycom recommends placing the DNS host record for the RMX Signaling Host IP Address or DMA system in the Active Directory domain (e.g. 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 tables provide examples of different Microsoft environments. **Table 8-4** provides example values for an environment that has different namespaces for SIP and Active Directory domains.

**Table 8-4  Different 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></td>
</tr>
<tr>
<td>DMA system FQDN</td>
<td>dmacorp.local</td>
<td>DMA virtual signaling IP address. FQDN must match security certificate</td>
</tr>
</tbody>
</table>
Table 8-4  Different 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>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>

### Configuring the Polycom RMX System

See Appendix H of the *Polycom RMX 2000/4000 Administrator’s Guide* for detailed steps on how to deploy a Polycom RMX 2000/4000 system for use with the video conferencing solution.
Deployment Process for Polycom DMA System

The DMA system can host multiple video endpoints in a single conference, as well as host multiple conferences simultaneously. For these reasons, the DMA system is configured as a trusted application rather than a single user in the Office Communications Server.

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

Perform the following procedure 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 box, select the Host Authorization tab and click Add.

   The Add Authorized Host dialog box is displayed.

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

5. Select the Throttle As Server and Treat As Authenticated check boxes. Then click OK.

6. In the Front End Properties dialog box, select the Routing tab and click Add.

   The Add Static Route dialog box appears.

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: Always refer to the system by the fully qualified domain name of its virtual interface. The system’s IP addresses should be available only on the DNS server.
The Polycom DMA 7000 system is now set as a trusted host, and calls from an Office Communicator client to a SIP address in the Polycom DMA system’s domain will be routed through that system.

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

If your solution includes a Polycom DMA 7000 system and you elected to use TLS transport, you must install a security certificate on the Polycom DMA 7000 system so that Office Communications Server trusts it. This can be accomplished in 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 DMA system’s online help 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 your organization permits the submission of certificate requests directly to the enterprise’s CA server, use the Office Communications Server Certificate Wizard. From it, you can then download an export file of the certificate to your PC for later installation on the Polycom DMA system. This procedure is described below.
  - 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.

Before you proceed, make certain that:

- You have all the fully qualified domain names (FQDNs) of the system for which you’re creating a certificate. A two-node system has three: one virtual and two physical; a single-node system has two: one virtual and one physical.
- These host names 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.
To request a security certificate for the Polycom DMA system 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 and the server pools list, right-click the pool front end entry, and select Certificate.

The Office Communications Server Certificate Wizard appears.

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 appears.

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. Be sure to record what it is.
   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

Within an Office Communications Server environment, you can include several dialing plans, depending on your environment.

You can use all dialing methods concurrently.

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

- **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 also required to use connect links included in meeting invitations generated from the Polycom Conferencing for Outlook add-in.

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

**Numeric Dialing**

Numeric dialing is where meeting rooms and entry queues are assigned numeric values and routes that allow users to dial a number instead of a URI.

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

- Enable HDX system users or Office Communicator users to dial a number to call into a meeting room rather than a full SIP URI. This greatly simplifies dialing, especially with the HDX remote.

- Enable a common dialing plan for VMRs across Office Communications Server and H.323 infrastructures. This means that a single number can be inserted into a calendar invitation and it will be valid for Office Communications Server endpoints and H.323 endpoints.

**Note**

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 steps to set up numeric dialing into VMRs in the Office Communications Server infrastructure:

- “Configure the RMX/DMA as a Routable Gateway” on page 130
“Configure an Office Communications Server Voice Route to the RMX/DMA” on page 131

You can remove numeric dialing capability at any time and return to enabling Office Communicator or HDX users to dial to meeting rooms using a matching URI, see “Remove Numeric Dialing” on page 132.

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

The RMX system (or the DMA system) must be set as a routable voice gateway in the Office Communications Server infrastructure. This does not restrict the RMX system to just voice operation, rather it means that the RMX system or the DMA system can be set as a destination for a voice route in the Office Communications Server infrastructure.

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, but in this case, the RMX or DMA is set 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 accomplish this.

To set up the RMX/DMA as a Voice Gateway

1. If you have not already, download and install the Office Communications Server 2007 R2 Resource Kit Tools from the following URL:

2. Open a command prompt and navigate to where 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 RMX or DMA system.

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

   Your RMX system (or DMA system) is now established as a trusted gateway by all Office Communications Server pools in the domain. It appears in the list of voice gateways when you establish a voice route.
Ensure that your DMA or RMX is not in the **Authorized Hosts** list for your Office Communications Server.

The **TrustedService** object that you just created needs to be the only trusted entry for this particular RMX/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 RMX system or DMA system for which you created an **TrustedService** instance is not also in the list of authorized hosts. If it is, you MUST delete it. It is necessary to completely remove the entry from the list.

---

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

The Voice Route to the RMX system (or DMA system) must be configured in the Office Communications Server.

The Office Communications Server infrastructure enables the establishment of a voice route to a voice gateway. Typically, this means that all SIP INVITEs to phone numbers which match a particular pattern will be routed to a specific gateway. In this example, all INVITEs to numbers which start 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 information in the **Add Route** dialog. In this example, the regex expression `^73` causes this route to be applied to all numbers starting with 73.
In the Add Route dialog, choose Add to set the destination gateway. The RMX gateway set up in Step 1 above, appears in the drop down list of gateways.

7 In 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 RMX which has been set up as the gateway, create meeting rooms which start with 73 (e.g., 73111). On the Office Communicator or HDX, dial 73111 and verify that the Office Communicator or HDX 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 RMX/DMA which have been defined.

2 Remove the trusted service definition which you created in “To set up the RMX/DMA as a Voice Gateway” on page 130.

   a Open a command prompt and navigate to where 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:

```powershell
cscript 0CSTrustEntry.vbs /action:list /type:trustedservice
```

An example of a returned TrustEntry is shown in Table 8-5.
Table 8-5  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=polycom,DC=com

objectClass:
top
container
msRTCSIP-TrustedService
 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=westminster,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-TrustedService,CN=Schema,CN=Configuration,DC=ocs2,DC=eng,DC=westminster,DC=polycom,DC=com
dSCorePropagationData: 1/1/1601
msRTCSIP-TrustedServicePort: 5073 (0x13D1)
msRTCSIP-TrustedServerFQDN: QAOCS.ocs2.eng.westminster.polycom.com
msRTCSIP-TrustedServiceType: Microsoft.Rtc.Applications.Cas
msRTCSIP-TrustedServerVersion: 4 (0x4)
msRTCSIP-Routable: True
msRTCSIP-ExtensionData:
TlsTarget=QAOCS.ocs2.eng.westminster.polycom.com

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

b  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.

3  Add a Matched URI route to the RMX/DMA by right-clicking the Office
Communications Server Pool, selecting Properties > Front End
Properties > Route.

4  Add a host authorization for the RMX/DMA by right-clicking the OCS
5 Wait about five minutes for Office Communicator to replicate Active Directory settings to its repository so that changes will take effect.

**Set up Simultaneous Numeric and Matched URI Routing**

You can simultaneously set up an RMX system or DMA system for both 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 also required to use connect links included in meeting invitations generated from the Polycom Conferencing for Outlook add-in.

You complete this task on the Office Communications Server.

**To Set Up Simultaneous Numerical and Matched URI Routing:**

1 Set the RMX/DMA as a trusted service (MediationServer) using the instructions in “To set up the RMX/DMA as a Voice Gateway” on page 130.

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

3 Also set up a voice route to the same RMX/DMA using instructions in “To establish a Voice Route to the RMX/DMA Voice Gateway” on page 131.

**Note**

You cannot also add this DMA/ROMX as an authorized host using the Front End Properties > Host Authorization tab. There can only be one trusted service entry for the RMX/DMA even though there are two different routes to the RMX/DMA (i.e., Matched URI and voice route). Only TLS connections to the DMA/ROMX system will work. TCP connections will not work.

**Registered RMX User Name Dialing**

The Office Communications Server Edge server enables remote and federation 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]@[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.
Supporting Remote and Federated Users for 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 which allows 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 in both the Microsoft Office Communications Server, the Polycom video infrastructure, and Polycom HDX systems.

This configuration supports both remote and federated users.

- **Remote users** are users who are outside of an organization’s firewall. When a remote user is registered to an enterprise’s Office Communication Server edge server, it can make and receive calls to/from 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 network boundaries as federated partners.

  **Federated users** are users from another enterprise (registered to a different Office Communications Server on a different network) that are able to make and receive calls to endpoints and video infrastructure on an external network that is behind one or more firewalls.

*Figure 9-1* illustrates a possible Edge Server deployment 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 who is behind more than one firewall. The user in the Branch Office can also place and receive calls from other enterprises and remote users.
Users in both enterprises 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 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

**Task Overview**

Complete the following tasks to ensure support for remote and federated users.

- “Deployment Process Microsoft Office Communications Edge Server” on page 138
- “Deployment Process for RMX Systems with Office Communications Server Edge Server” on page 142
- “Deployment Process for Remote HDX Systems” on page 149

**Deployment Process Microsoft Office Communications Edge Server**

The following section provides details related to deploying Polycom devices in your Office Communications Server edge server.
Related Microsoft Documentation

Consult your Microsoft Communications Server documentation for full instructions on how to include a Microsoft Communications Server Edge Server to your environment.

For more information, see the Edge Configuration Guide which is available at: http://www.microsoft.com/downloads/details.aspx?familyid=E9F86F96-4DCA-9088-F64B4F01C703&displaylang=en

Microsoft also provides an Edge Server Planning Tool which is available at: http://www.microsoft.com/downloads/details.aspx?FamilyID=149e5dd5-ee-46b6-afba-01c31e88a275&displaylang=en
Deployment Considerations:

• TLS is required for both federated environments and for remote users.
• Polycom devices use the Access Edge Server IP address to register to a Office Communications Server edge server.
• Numeric dialing is not supported between federated environments.

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

Note: The following instructions should be performed on the Office Communications Server on the network where the RMX system or DMA system resides. Note this needs to be configured on the internal Office Communications Server, not the edge server.

The RMX system (or the DMA system) must be set as a routable voice gateway in the Office Communications Server infrastructure. This does not restrict the system to just voice operation, rather it means that the RMX system or the DMA system can be set as a destination for a voice route in the Office Communications Server infrastructure.

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, but in this case, the RMX or DMA is set 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 accomplish this.

To set up the RMX/DMA as a Voice Gateway

1. If you have not already, download and install the Office Communications Server 2007 R2 Resource Kit Tools from the following URL:

2. Open a command prompt and navigate to where 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:

cscript OCSTrustEntry.vbs /action:add /type:trustedservice
/fqdn:<your FQDN> /service:MediationServer /port:5061
/version:4 /routable:TRUE

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

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

Your RMX system (or DMA system) is now established as a trusted
gateway by all Office Communications Server pools in the domain. It
appears 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.

The TrustedService object that you just created needs to be the only
trusted entry for this particular RMX/DMA system. 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 RMX system or DMA system for which you
created an TrustedService instance is not also in the list of
authorized hosts. If it is, you MUST delete it. It is necessary to
completely remove the entry from the list.

**Note**

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

**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 both 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 companyB wants to connect to calls managed by a DMA
system or RMX system on companyA, companyB must add the companyA
domains to its list of allowed SIP domains in the Office Communications
Server edge server.

Likewise if companyA wants to connect to calls managed by a DMA system or
RMX system on companyB, companyB’s SIP domains must be on the allowed
SIP domain list of companyA’s 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: area, click Add Domain.

5. In the Add SIP Domain dialog box, 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

- Office Communications Server edge server with which you want to federate. For example, OCS.companyB.com.

- The SIP signaling domain of the DMA system or RMX system. For example, DMA.OCS.companyB.com if your companyB deployment includes a DMA system. If the companyB deployment includes only an RMX system, use the FQDN of the RMX system.

Note that the FQDN of the SIP signaling domain is in the following format: RMX_DMA_NAME.OCS_EDGE_SERVER_NAME.DOMAIN.COM

Deployment Process for RMX Systems with Office Communications Server Edge Server

To enable remote and federated connections with the Polycom RMX system, do the following:

- Create an Active Directory account for the RMX system to use for registering and operating in the Office Communications Server Edge Server environment.

- Enable the RMX User Account for Office Communication Server.

- Configure the RMX for ICE dialing.

- Ensure that the RMX system SIP signaling domain has been allowed on the Office Communications Server edge server to which you are federating (if your deployment does not include a DMA system).
Edge Server Considerations for the Polycom RMX

- 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.

Task 3: Creating 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 password is not important. 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 User** wizard, enter the required user information.

![New Object - User](image)

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 4: Enabling the RMX User Account for Office Communication Server Edge Server

You must 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 box, 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) as entered in the New User dialog box.
4. Select the Server or Pool from the list.
5. Click Apply and then click OK.

Task 5: 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.
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 6: Configuring the RMX for ICE Dialing**

The **Default IP Network Service** for the RMX system must be configured to work with the Office Communication Server edge server as the SIP Server and the RMX user defined in the Active Directory must also be defined in the RMX ICE environment parameters.

The procedure described here assumes that the RMX is configured to work in Microsoft environment; the **MS_ENVIRONMENT** flag is set to YES, the IP Network Service is set to work with Office Communications Server as the SIP Server and the TLS certificate is installed. For a detailed description of these settings, see the *RMX Administrator's Guide, Appendix H*.

**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 box opens.

3 Click the **SIP Servers** tab.

4 Make sure that the **Registration** options (**Ongoing Conferences**, **Meeting Rooms**, **Gateway Profiles**, **Entry Queues** and **SIP factories**) are not selected (check boxes are cleared).

5 Make sure that the IP address of the Office Communications Server 2007 edge server is specified and the **Server Domain Name** is the same as 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 defined in the Active Directory. For example, enter `rmx1234567890`.

8 In the **ICE Environment** field, select **MS** (for 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 7: Add the SIP Signaling Domain to 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 to which you are federating, see “Ensure SIP Signaling Domains are Allowed” on page 141.

**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 box.

**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 to which it is connected and the connection status.

In addition, the system indicates the status of the firewall detection in the RMX.
Deployment Process for Remote HDX Systems

Remote HDX system users (those outside of the corporate network) are supported through an Office Communications Server edge server. Remote HDX systems need to register with this server in order to make and receive calls to/from endpoints behind the corporate firewall.

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

Edge Server Considerations for the Polycom HDX

- 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 they are made behind the same firewall, i.e., the same side of the network.
- When traversing firewalls with ICE, the Polycom HDX supports a Single Video Stream (either People Video or Content Video). People + Content (H.239 / Dual Streams) is not supported. In such scenarios 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 “Deployment Process for Polycom HDX Systems” on page 101 with the following consideration:
   - If registering a remote HDX system with an Office Communications Server edge server, use the fully qualified domain name of the access edge server role.
Polycom® Conferencing for Microsoft® Outlook®

Polycom Conferencing for Microsoft Outlook offers an integrated and enhanced calendaring experience for all of those involved in video conferencing.

This chapter includes the following sections:

- “Polycom Products that Enable Polycom Conferencing for Outlook” on page 152
- “Microsoft Products that Enable Polycom Conferencing for Outlook” on page 154
- “Deploying Polycom Conferencing for Outlook” on page 155
Polycom Solution Support Services

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. UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations.

Please see [http://www.polycom.com/services/professional_services/index.html](http://www.polycom.com/services/professional_services/index.html) or contact your local Polycom representative for more information.

Polycom Products that Enable Polycom 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>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>
</tbody>
</table>

  
  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.
<table>
<thead>
<tr>
<th>System</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 that Enable Polycom Conferencing for Outlook

The following table shows the minimum version of Microsoft products required for the Polycom-enabled Unified Communications user experience.

<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 Exchange</td>
<td>2007 with SP2 and 2010</td>
<td>Hosts mailboxes and calendars. SP1 is required for the 'Manage Full Access Permissions' function. Exchange Web Services must be enabled.</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td>2007 with SP2 and 2010</td>
<td></td>
</tr>
<tr>
<td>Microsoft Lync Server</td>
<td>2010 and 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 and 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

Complete the following tasks to deploy Polycom Conferencing for Outlook:

- “Configure DNS Entries for Polycom Devices” on page 155
- “Considerations for Remote Users” on page 157
- “Configure the Polycom the Infrastructure Mailbox and Devices” on page 158
- “Configure Mailboxes for Room-based HDX Systems” on page 164
- “Configure Mailboxes for Polycom HDX Desktop Systems” on page 171
- “Configure HDX Mailboxes to Prevent Meeting Conflicts” on page 171
- “Configure Polycom HDX System Calendaring Settings” on page 172
- “(Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX systems” on page 176
- “Configure and Install the Polycom Conferencing Add-In” on page 176
- “Test Polycom Conferencing for Outlook Deployment” on page 177

Configure DNS Entries for Polycom Devices

For a Polycom devices to work correctly in a Polycom Conferencing for Outlook deployment, they must subscribe to the Exchange Server for notifications when meeting invitations are sent to the Polycom Conferencing Mailbox it is monitoring. This registration will only succeed if the DNS server used by Exchange (usually, the nearest Active Directory Domain Controller provides DNS services for an Exchange Server) has an A record that resolves the Fully Qualified Domain Name of the Polycom system’s virtual IP address.
For example, Company A’s DMA has a Virtual IP address of 10.1.1.222 and Virtual System name PolycomDMAVirtual.companya.local.

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.
Considerations for Remote Users

Polycom Conferencing for Outlook supports both H.323 clients (Polycom HDX systems) and Microsoft unified communications clients (see “Polycom-enabled Unified Communications for Microsoft Office Communications Server” on page 89 or “Polycom-enabled Unified Communications for Microsoft Lync Server” on page 7).

Remote users (users who are not directly connected to the enterprise network) are supported with the following caveats and requirements.

- Polycom HDX system H.323 calls are only supported if the remote user of a Polycom HDX system is registered to a Polycom VBP-S or VBP-S/T device which 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, see “Polycom-enabled Unified Communications for Microsoft Office Communications Server” on page 89 or “Polycom-enabled Unified Communications for Microsoft Lync Server” on page 7.

- Polycom supports calendar access for remote users through Outlook Anywhere. In addition, Polycom HDX systems require access to Exchange Web Services. You need to ensure they have access the /ews/* paths provided by the Exchange Client Access Server role. If your organization has already enabled Outlook Anywhere then no additional configuration should be necessary. Please follow the Microsoft documentation to enable access to the /ews/* paths: http://technet.microsoft.com/en-us/library/aa998934(EXCHG.80).aspx.

- For security purposes, only users from within an organization can set up video meetings that use that organization’s infrastructure. Federated and remote users (outside the organization’s network) can always be included on meeting invitations, but cannot create meeting invitations.
Configure the Polycom the Infrastructure Mailbox and Devices

Polycom infrastructure devices (Polycom RMX system, Polycom DMA system, and Polycom RSS) monitor a single Exchange mailbox that is automatically scheduled into Polycom Conferencing for Outlook meetings.

Polycom infrastructure devices respond to meeting invitations sent to this address and provide accept/decline feedback to the meeting organizer.

The Polycom infrastructure account will always accept meeting invitations except when a conflict in Virtual Meeting Room (VMRs) numbers exists. These numbers are randomly generated by the Polycom Conferencing Add-in for Outlook and are unlikely to collide. If this occurs, 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, please see the administrator guides for those products.

Notes
- The Polycom infrastructure account’s acceptance of a meeting is not capacity-aware. It is possible to schedule more participants into conferences than the infrastructure can support, so the administrator must carefully plan a deployment to ensure appropriate resources are in place.
- The Polycom Conferencing Add-in for Outlook generates random Virtual Meeting Room (VMR) identification numbers for calendared conferences. It does not permit calendaring of static meeting rooms that use the same VMR numbers concurrently. For more information see the System Administrator Guide for the Polycom Conferencing for Outlook Add-in.

Complete the following tasks to set up your Polycom Infrastructure Integration
- “Create the Polycom Infrastructure Account and Mailbox” on page 159
- “Configure Microsoft Exchange Integration with Polycom RMX Systems” on page 160
- “Configure Calendaring Settings for Polycom DMA System” on page 162
- “Configure Calendaring Settings for Polycom RSS System” on page 163
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. Polycom infrastructure devices (Polycom RMX system, Polycom DMA system, and RSS) will monitor this account.

Polycom Infrastructure Mailbox Requirements:

- **A standard user mailbox that is dedicated to Polycom use.**
  
  You **cannot** use a room mailbox for the Polycom infrastructure mailbox. A dedicated mailbox is important because the Polycom DMA system deletes all messages from the Inbox when it checks this mailbox for meeting invitations.

- **A password that is set 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.

This e-mail account is automatically included in meetings created Polycom Conferencing for Outlook, see Figure 10-1 for an example of configuring a Polycom infrastructure mailbox.

*Figure 10-1 Example of a Polycom infrastructure account.*
Task 2: Configure Microsoft Exchange Integration with Polycom RMX Systems

The Polycom RMX system monitors the Exchange account you configured in “Configure the Polycom the Infrastructure Mailbox and Devices” on page 158. 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 fields listed in Table 10-1.

Table 10-1 Configure Exchange integration in the RMX system.

<table>
<thead>
<tr>
<th>Exchange Web Services Url</th>
<th>Specify the full URL path to the Exchange Web Service, including the Exchange.asmx service on the Exchange server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>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 could enter either COMPANYA.local or COMPANYA.</td>
</tr>
<tr>
<td>User Name</td>
<td>This is the Active Directory account’s user name only, with no domain information included.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user account.</td>
</tr>
<tr>
<td>Primary SMTP Mailbox</td>
<td>This must match the Primary SMTP Address for the account in Exchange (one account may have multiple associated SMTP addresses). This is displayed as the Mail field in Active Directory.</td>
</tr>
</tbody>
</table>

5. Mark the Accept Appointments check box, if your deployment does not include a DMA system, shown in Figure 10-2.

If your deployment includes a DMA system, leave the Accept Appointments check box unchecked, shown in Figure 10-3. When a DMA system is present, it accepts appointments on behalf of the RMX.
**Figure 10-2** Example Polycom RMX system and Microsoft Exchange Integration without a DMA system.

Tip

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 type:

`get-WebServicesVirtualDirectory | fl`

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

**Figure 10-3** RMX configuration with Exchange when using a DMA system.
Task 3: Configure Calendaring Settings for Polycom DMA System

The DMA system needs to subscribe to the Exchange Server to receive notifications when meeting invitations are sent. It monitors the Polycom infrastructure account you created, see “Configure the Polycom the Infrastructure Mailbox and Devices” on page 158.

Be sure you have properly configured DNS before continuing, see “Configure DNS Entries for Polycom Devices” on page 155 for more information.

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.
3. Check the Enable Calendaring Service check box.
4. Specify the login credentials for the system on the Exchange server. Use the Polycom infrastructure account you configured, see “Configure the Polycom the Infrastructure Mailbox and Devices” on page 158.
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 individual Exchange server.
6. Click Update.
   A dialog box informs you that the configuration has been updated.
7. Click OK.

Figure 10-4 Example Polycom DMA system and Microsoft Exchange integration.
**Task 4: Configure Calendaring Settings for Polycom RSS System**

The Polycom RSS system needs to subscribe to the Exchange server to receive notifications of which meeting invitations have requested that the meeting be recorded.

It monitors the Polycom infrastructure account you created, see “Configure the Polycom the Infrastructure Mailbox and Devices” on page 158.

**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.
3. Check the **Enable Calendar Integration** check box.
4. Complete the provided fields, see the RSS documentation for more details.

**Figure 10-5 Example Polycom RSS system and Microsoft Exchange integration.**

**Task 5: Configure 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 and uploaded to the Polycom VMC 1000. It provides scalable and reliable content access by means of streaming protocols to end users across the entire enterprise.

Configuring calendaring settings for a Polycom VMC involves two steps:

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

For complete details, see the *Polycom Video Media Center (VMC) 1000 Administrator Guide*. 
Configure Mailboxes for Room-based HDX Systems

You need to configure an Exchange room mailbox and an Active Directory account (used to authenticate with Exchange) for each room-based HDX in your deployment.

**Note** In many environments, User and Room accounts are likely to already be configured. However, room mailboxes and accounts associated with a room-based HDX need additional configuration.

Scheduling a video-enabled Polycom Conferencing for Outlook conference uses the same workflows as reserving a conference room for a meeting without video. The room mailbox (sometimes referred to as the resource mailbox) is scheduled via the Outlook client when users wish to hold a meeting in the room. The Polycom HDX system located in the conference room monitors the Exchange calendar of this room mailbox to view the meetings scheduled for the conference room, both video-enabled and not.

You can configure mailboxes for HDX room systems in three ways, see Table 10-2.

1. **Enable the user account associated with the room mailbox.**
   The enabled Active Directory account can be used to authenticate with Polycom CMA system for automatic provisioning if the same credentials are used for both the Provisioning Service and Calendaring Service configurations in the Polycom HDX system.

2. **Associate a service account to a single mailbox and grant that account full manage permissions.**

3. **Associate a service account to multiple mailboxes and grant that account full manage permissions.**

By default, room mailboxes are linked to disabled Active Directory accounts. If your company’s policy prohibits enabling the Active Directory accounts linked to room mailboxes, see “Option 2: Use a Service Account with a Single Room Mailbox” on page 168 or “Option 3: Use a Single Service Account for Multiple Room Mailboxes” on page 170.
Table 10-2  Available features with different HDX room mailbox configurations.

<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>
<tr>
<td>Presence</td>
<td>✓ (either with CMA or Office Communications Server)</td>
<td>✓ (only with Office Communications Server)</td>
<td>X</td>
</tr>
<tr>
<td>CMA Automatic Provisioning</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>CMA Softupdate</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

Note: If your environment includes both a Polycom CMA system and Office Communications Server, presence and directory are provided by Office Communications Server.

Option 1: Enable the user account for the room mailbox

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

The Subject and Description information needs to be included in the meeting invitation (some default Exchange configurations hide this information). The Polycom HDX system uses this data to display information and complete calls. Optionally, you can also add the organizer's name to the meeting invitation.

You can modify these settings using Microsoft Exchange Powershell or Microsoft Office Outlook Web Access.


To use Microsoft Exchange Powershell to modify the mailbox settings:

1. View the settings for the room mailbox.
   
   Get-MailboxCalendarSettings <ExchangeMailbox> | fl
   
   For example: Get-MailboxCalendarSettings zeusroom | fl
   
   — By default, the DeleteSubject value is set to True. This setting must be set to False.
   
   — By default, the DeleteComments value is set to True. This setting must be set to False.
   
   — By default, the AddOrganizerToSubject value is set to True and will add the organizer's name to the subject line. Changing this setting is optional.

2. Set the room mailbox properties:
   
   Set-MailboxCalendarSettings -id <ExchangeMailbox> -DeleteComments$false -DeleteSubject$false -AddOrganizerToSubject$false

To use Outlook Web Access to Configure 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.

The two settings highlighted in red correspond to the required Exchange Powershell commands above - the blue setting corresponds to the optional setting.
Option 2: Use a Service Account with a Single Room Mailbox

This section assumes you have already created the room mailbox.

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

This configuration results in two accounts in the Microsoft deployment:

- One primary account that is disabled in Active Directory with an associated Exchange Mailbox.
- One service account that is enabled in Active Directory without a directly assigned Exchange Mailbox.

Task 1: Create the service account

This Active Directory account may be named starting with SRV-, or another naming scheme fitting with your organization’s deployment. The configuration is similar to any standard user account, and no Exchange mailbox is directly associated.

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: Grant the service account the permission to manage the Room Mailbox

You can do this either with the Exchange Management Console of the Exchange Management Shell.

To Use the Exchange Management Console to grant permission:

1. Navigate to the resource mailbox to which you want to grant permissions.
2. Right-click the mailbox and select Manage Full Access Permission.
In the **Manage Full Access Permission** dialog box, click **Add** and add the Active Directory service account to the list.

In **Figure 10-7**, the SRV-\apolloroom is a service account that has no directly assigned Exchange mailbox, but it is given permission to manage the room mailbox assigned to the apolloroom user.
To Use the Exchange Management Shell to Grant Permissions:

- 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: Use a Single Service Account for Multiple Room Mailboxes

You can use one service account for all Polycom HDX systems in the Polycom Conferencing for Outlook deployment.

Note: If you create one service account for multiple room mailboxes, you will not be able to take advantage of presence information, see “Available features with different HDX room mailbox configurations.” on page 165.

The steps for this approach are the same as mentioned in “Option 2: Use a Service Account with a Single Room Mailbox” on page 168, with the exception that you can grant the same service account permission to manage multiple mailboxes.

In Figure 10-8, the SRV-AllHDX-CompanyA service account is being used to manage multiple conference rooms. Only the association between Aphrodite and SRV-AllHDX-CompanyA is shown, but this same association could be duplicated for other rooms. For example, SRV-AllHDX-CompanyA could manage dozens of conference rooms within Company A, such as the Poseidon Room, the Hestia Room, and more.

**Figure 10-8 Using a service account for all HDX conference rooms.**
Configure Mailboxes for Polycom HDX Desktop Systems

Each HDX desktop system in your deployment needs to be configured to use an individual user’s Active Directory account and Exchange Mailbox for authentication with Exchange.

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

There is no additional Exchange configuration necessary to for user accounts to be integrated with an HDX system.

Configure HDX Mailboxes to Prevent Meeting Conflicts

Microsoft Outlook allows users and mailboxes to schedule conflicting meetings. 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. You can use either Microsoft Outlook or Outlook Web Access.
   a. In Microsoft Outlook, select Tools > Options to view the Options dialog box.
   b. Click Calendar Options to view the Calendar Options dialog box.
   c. In the Advanced Options section, click Resource Scheduling.
   d. In Resource Scheduling, ensure that the Automatically accept meeting requests and process cancellations and the Automatically decline conflicting meeting requests check boxes are both marked.

   OR

   a. In Outlook Web Access, select Options.
   b. Click Resource Settings.
   c. In the Resource Scheduling, ensure that the Automatically process meeting requests and cancellations and the Allow conflicts check boxes are both marked.
Configure 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.

If you are using a Polycom CMA system, these settings can be dynamically managed, see “(Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX systems” on page 176 instead.

To configure the calendar 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 the Enable Calendaring Service check box.
4. Complete the fields listed in Table 10-3.

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

<table>
<thead>
<tr>
<th>Table 10-3 Calendar Settings in the Polycom HDX system.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Address</strong></td>
</tr>
<tr>
<td>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 would be the FQDN of the Client Access Servers’ Virtual IP Address. An IP address can be used in place of an FQDN but Polycom recommends using the same FQDN that is used for Outlook clients.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
</tr>
<tr>
<td>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 could enter either companya.local or COMPANYA.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
</tr>
<tr>
<td>This is the Active Directory account’s user name only, with no domain information included</td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td>The password for the user account.</td>
</tr>
<tr>
<td><strong>Mailbox (Primary SMTP)</strong></td>
</tr>
<tr>
<td>This must match the Primary SMTP Address for the account in Exchange (one account may have multiple associated SMTP addresses). This is displayed as the Mail field in Active Directory.</td>
</tr>
</tbody>
</table>

5. Click Update.
Example Calendar Settings

Figure 10-9 shows the configuration using the method described in “Option 1: Enable the user account for the room mailbox” on page 165. The zeusroom Active Directory account is enabled and no service accounts are required. As a User, Dwight’s Active Directory account is enabled as well.

Figure 10-9  Using an enabled user account assigned to a room mailbox.
Figure 10-10 shows the ‘individual service accounts’ strategy discussed in “Option 2: Use a Service Account with a Single Room Mailbox” on page 168. The integration between the apolloroom mailbox and the SRV-apolloroom service account is reflected in the HDX as below.

**Figure 10-10 Using a service account to manage a single mailbox.**

![Using a service account to manage a single mailbox.](image)

Figure 10-11 shows, the ‘shared service account for all HDXs’ strategy discussed in “Option 3: Use a Single Service Account for Multiple Room Mailboxes” on page 170. The integration between the Aphrodite Room and the SRV-AllHDX-Company A service account is shown. Remember that this service account may also be managing other room mailboxes simultaneously.

**Figure 10-11**

![Using a service account to manage multiple mailboxes.](image)
Figure 10-12 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 10-12 User-based Calendar Settings in the Polycom HDX System**

![Calendar configuration for a SOHO user](image)

Figure 10-13 shows the configuration for a SOHO user. When configuring a remote HDX user, be sure to use a publicly-routable Exchange server address, see Figure 10-13. Microsoft Outlook Anywhere must be enabled, see “Considerations for Remote Users” on page 157.

**Figure 10-13 Calendar configuration for a SOHO User**

![Calendar configuration for a SOHO user](image)
(Optional) Configure CMA System Automatic Provisioning of Calendaring Service Settings on HDX systems

You can use the Polycom CMA system to automatically provision a Polycom HDX system when using dynamic management mode, see “Deploying Dynamic Device Management” on page 7.

To use the Polycom CMA system to automatically provision a Polycom endpoint system, the endpoint system must use the same credentials (username and password) to access both the Exchange server and the Polycom CMA system. Only then can the Polycom CMA system automatically provision a calendaring service-enabled endpoint system.

See the Polycom CMA System Operations Guide for more information.

Note: You must use an enabled resource account (room mailbox) in order to take advantage of CMA Automatic Provisioning, see “Configure Mailboxes for Room-based HDX Systems” on page 164.

Configure and Install the Polycom Conferencing Add-In

The Polycom Conferencing Add-In software and its templates must be installed on each Microsoft Outlook client.

For complete documentation, see the System Administrator Guide for the Polycom Conferencing Add-in for Microsoft Outlook.

Complete the following tasks:

- “Configure Polycom Conferencing Add-in Preferences For Installation to Client PCs” on page 176
- “Install Polycom Conferencing Add-in for Outlook to Client PCs” on page 177
- “Deploy Customization Files” on page 177
- “Test Polycom Conferencing for Outlook Deployment” on page 177

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

Administrators 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 the System Administrator Guide for the Polycom Conferencing Add-in for Microsoft Outlook.
Task 2: Install Polycom Conferencing Add-in for Outlook to Client PCs

The Conferencing Add-in can be installed in a number of ways, depending on the administrator’s preference. After customizing preferences as described in Task 1, the administrator can provide the file to users via existing software deployment processes, using a link to a network location where the file resides, by using a software installation program like Microsoft SMS, or by using a Group Policy Object. For specific information regarding your environment’s preferred software delivery method, consult the documentation for your software delivery product.

For an example deployment method using Microsoft Active Directory and Global Policy, refer to the System Administrator Guide for the Polycom Conferencing Add-in for Microsoft Outlook.

Task 3: Deploy Customization Files

After the installation described in Task 2, the customization files created in Task 1 can be deployed to the appropriate 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 one possible deployment method using Microsoft Active Directory and Global Policy, refer to the System Administrator Guide for the Polycom Conferencing Add-in for Microsoft Outlook.

Test Polycom Conferencing for Outlook Deployment

• Walk through scheduling and joining a meeting.
• For more details on the on-screen experience with an Polycom HDX system, please see the Polycom HDX system documentation.
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 either 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>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 authentication</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>vlanid</td>
<td>VLAN ID</td>
<td>Integer in [2,4094]</td>
<td>100</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>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 system</td>
<td>Text string</td>
<td>hdx334</td>
</tr>
<tr>
<td>userdomain</td>
<td>Domain of the user account used to log into the provisioning server</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 provisioned</td>
<td>Text string</td>
<td></td>
</tr>
<tr>
<td>ipaddress</td>
<td>IP address of the Polycom HDX system</td>
<td>IP address</td>
<td>172.18.1.222</td>
</tr>
<tr>
<td>subnetmask</td>
<td>Subnet mask of the Polycom HDX system</td>
<td></td>
<td>255.255.255.192</td>
</tr>
<tr>
<td>defaultgateway</td>
<td>IP address of the default router</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 server</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>
Exchange Calendar Polling Information

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

No longer able to access the Polycom Conferencing Add-In

It is possible for the Polycom Conferencing Add-In to 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

Most likely, the Exchange Powershell commands to change the default Exchange behavior of deleting meeting information after acceptance have not been completed. Review the Exchange Powershell commands in “Modify the room mailbox settings” on page 166 and verify that they have been performed correctly.

Unable to complete a call to a federated or remote HDX system

In an Office Communications Server deployment, the HDX system user must be enabled for remote access and federation, see “Enable Conference Rooms for Remote Access and Federation” on page 97.

Cannot import PFX file into the RMX system

PFX files are container files with contents that may vary. Because of this variance, the RMX system sometimes fails to import a PFX file.

The workaround is to use OpenSSL to extract the files you need from the PFX file.
Use OpenSSL to extract the certificate onto the RMX system

Once the *.pfx file is on your PC, you can upload it to the Polycom RMX system and install it. These instructions show how to accomplish this using OpenSSL.


2. Use OpenSSL to extract the root CA certificate. For example,
   ```bash
   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,
   ```bash
   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,
   ```bash
   C:\Program Files\OpenSSL-Win64\bin\openssl" pkcs12 -in rmxcert.pfx -clcerts -out pkey.pem -nodes
   ```

5. Manually create your password file.
   ```
   create 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.