



SOLUTION DEPLOYMENT GUIDE

September 2015 | 3725-06675-006A

Polycom® Unified Communications for Microsoft® Environments



Copyright© 2015, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks



Polycom®, the Polycom logo and the names and marks associated with Polycom 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 property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

End User License Agreement

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

Patent Information

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

Open Source Software Used in this Product

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

Disclaimer

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

Limitation of Liability

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

Customer Feedback

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



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

Contents

Conventions Used in Polycom Guides.....	7
Information Elements	7
Typographic Conventions	7
Before You Begin.....	9
Required Skills	9
Hardware and Software Dependencies	10
What's New?	10
Get Help	11
<i>Polycom Resources.....</i>	<i>11</i>
<i>The Polycom Community.....</i>	<i>11</i>
Use Polycom-Enabled Unified Communications with Microsoft Lync and Skype for Business Server.....	12
Features of the Polycom-Enabled Microsoft Solutions	12
<i>Polycom ContentConnect Software</i>	<i>12</i>
<i>Continuous Presence</i>	<i>13</i>
<i>Viewing Content.....</i>	<i>14</i>
<i>Polycom RealConnect for Microsoft Lync and Skype for Business.....</i>	<i>14</i>
<i>Dial Plans for a Lync Server Environment</i>	<i>14</i>
<i>Support Remote and Federated Users in Lync Server Environments</i>	<i>15</i>
<i>Microsoft Domains and Application Pools Best Practices.....</i>	<i>16</i>
Deploy Polycom RealPresence Group Series Systems	20
Configure Lync Server for use with a RealPresence Group Series System	20
<i>Configure Authentication in Lync Server.....</i>	<i>20</i>
<i>Use Microsoft Call Admission Control.....</i>	<i>21</i>
<i>Enable RTV on the Lync Server</i>	<i>21</i>
<i>Add Calendar and Scheduling Features to Polycom RealPresence Group Series Systems</i>	<i>21</i>
<i>Enable Conference Rooms for Lync Server</i>	<i>22</i>
<i>Enable Conference Room Access for Remote and Federated Users.....</i>	<i>22</i>
<i>Enable Conference Room Accounts for Lync or Skype for Business Server.....</i>	<i>22</i>
<i>Add Lync Contacts to Conference Room Local Address Book.....</i>	<i>23</i>
Configure Polycom RealPresence Group Series System for Lync or Skype for Business Server.....	24
<i>Install the Skype for Business Interoperability License on your RealPresence Group Series System.....</i>	<i>24</i>
<i>Register a Polycom RealPresence Group Series System with Lync Server.....</i>	<i>24</i>
<i>Understand SIP Settings</i>	<i>26</i>
<i>Configure the Polycom RealPresence Group Series System LAN Properties.....</i>	<i>28</i>
<i>Configure Display Options for the RealPresence Group Series System Contact List.....</i>	<i>28</i>
<i>Configure AES Encryption</i>	<i>29</i>
<i>Configure Encryption Settings for Skype for Business 2015 and Microsoft Lync 2013.....</i>	<i>29</i>

<i>Support Lync-hosted Video Conferencing Lync Server 2013 and Skype for Business</i>	30
Polycom Support for Microsoft Real-Time Video (RTV) and H.264 SVC	32
<i>Call Quality Scenarios for RTV Video</i>	32
Enable Native Polycom RealConnect Click-to-Join Functionality.....	33
Deploy Polycom HDX Systems	35
Configure Lync Server for use with a Polycom HDX System	35
<i>Configure Authentication in Lync Server</i>	36
<i>Use Microsoft Call Admission Control</i>	36
<i>Enable RTV on the Lync Server</i>	36
<i>Add Calendar and Scheduling Features to Polycom HDX Systems</i>	36
<i>Enable Conference Rooms for the Lync Server</i>	37
<i>Enable Conference Room Access for Remote and Federated Users</i>	37
<i>Add Lync Contacts to Conference Room Local Address Book</i>	38
Configure Your Polycom HDX System for Lync Server.....	38
<i>Install the RTV Option Key on your Polycom HDX System</i>	38
<i>Register Polycom HDX System with the Lync Server</i>	39
<i>Understand SIP Settings</i>	40
<i>Configure the Polycom HDX System LAN Properties</i>	42
<i>Configure Display Options for the Polycom HDX System Contact List</i>	43
<i>Configure AES Encryption</i>	43
<i>Support Lync-hosted Video Conferencing and Lync Server 2013</i>	44
Support Microsoft Real-Time Video (RTV)	45
<i>Call Quality Scenarios for RTV</i>	46
Deploy Polycom RealPresence Collaboration Server (RMX) Solution	47
Configure Polycom RealPresence Collaboration Server (RMX) System for Lync Server.....	47
<i>Set Up the RealPresence Collaboration Server (RMX) System for Security and SIP</i>	47
<i>Create and Install a Security Certificate for the Polycom RealPresence Collaboration Server (RMX) System</i>	49
<i>Install the Certificate on your RealPresence Collaboration Server (RMX) solution</i>	53
<i>Configure Encryption</i>	53
<i>Configure Lync Server for use with a Polycom RealPresence Collaboration Server (RMX) System</i>	54
Enable Microsoft Presence for Lync Server 2013	58
Enable Edge Server Integration with Polycom RealPresence Collaboration Server (RMX) System ...	58
<i>Required Ports</i>	59
<i>Set Up a Microsoft Edge Server for the Polycom RealPresence Collaboration Server (RMX) System</i>	59
Configure RealPresence Collaboration Server (RMX) for Polycom ContentConnect Software.....	62
Deploy Polycom RealPresence DMA Systems	64
Configure Lync Server for Use with a RealPresence DMA System	64
<i>Set the Routing for the RealPresence DMA System</i>	64
<i>Enable Federation in your Lync Environment</i>	66
Configure RealPresence DMA System for Lync Server	68
<i>Ensure DNS is Configured Properly</i>	68
<i>Create a Security Certificate for the RealPresence DMA 7000 System</i>	68
<i>Enable RealPresence DMA System for Lync 2013 and Polycom RealConnect</i>	72
<i>Configure the RealPresence DMA System Lync Dial Rule</i>	81

Configure the RealPresence DMA System Polycom ContentConnect Dial Rule	82
<i>Enable RealPresence DMA System for Presence Publishing</i>	84
Configure RealPresence DMA System for Polycom ContentConnect Software	92
Deploy Polycom ContentConnect Software.....	95
Required Components	95
Optional Components	96
Access and Use the Polycom ContentConnect Server Web Configuration Tool	97
<i>Configure the Content Sharing Server Using the Content Sharing Server Web Configuration Tool</i>	98
<i>(Optional) Configure your Polycom ContentConnect Software Provisioning Profile</i>	101
Appendix A: Polycom HDX System Configuration Files	103
Appendix B: Exchange Calendar Polling Information	105
Polycom HDX and RealPresence Group Series System	105
Polycom RealPresence DMA System	105
Polycom RealPresence Collaboration Server (RMX) System	105
Polycom RSS Solution	105
Appendix C: Lync Client and Server Support	106
Appendix D: Polycom RealConnect Technology Resources and Licenses	107
Appendix E: Configure Static Routes in Skype for Business	108
Trusted Application Pool	108
TLS Security	109
Configure a Certificate	110
Appendix F: Polycom RealConnect for Service Providers	116
Prerequisites for Service Providers	116
RealPresence System and Lync 2013 for Polycom RealConnect.....	117
Deploy Lync Dial-in Conferencing	118
Deploy Polycom RealPresence Collaboration Server (RMX) Solution.....	123
<i>Configure Polycom RealPresence Collaboration Server (RMX) System for Lync Server</i>	123
<i>Enable Edge Server Integration with Polycom RealPresence Collaboration Server (RMX) System</i>	132
<i>Required Ports</i>	132
Deploy Polycom ContentConnect Software.....	135
<i>Required Components</i>	136
<i>Optional Components</i>	137
<i>Access and Use the Polycom ContentConnect Server Web Configuration Tool</i>	137
Configure Your RealPresence DMA System for Lync Server	141
<i>Ensure DNS is Configured Properly</i>	141
<i>Create a Security Certificate for the RealPresence DMA 7000 System</i>	142
<i>Configure a RealPresence DMA System SIP Peer for Lync Server</i>	146
<i>Specify a Domain and Time on the RealPresence DMA System</i>	148
<i>Configure the RealPresence DMA System Lync Dial Rule</i>	148
<i>Configure the Directory Server and Domain</i>	149

Troubleshoot	156
---------------------------	------------


Conventions Used in Polycom Guides

Polycom guides contains graphical elements and a few typographic conventions. Familiarizing yourself with these elements and conventions will help you successfully perform tasks.

Information Elements

Polycom guides may include any of the following icons to alert you to important information.

Icons Used in Polycom Guides

Name	Icon	Description
Note		The Note icon highlights information of interest or important information needed to successfully complete a procedure or understand a concept.
User Tip		The User Tip icon highlights techniques, shortcuts, or productivity related tips for users.
Administrator Tip		The Administrator Tip icon highlights techniques, shortcuts, or productivity-related tips.
Caution		The Caution icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.
Warning		The Warning icon highlights an action you must perform or avoid to prevent information loss, damage your configuration setup, and/or affect component or network performance.
Web Info		The Web Info icon highlights online information such as documents or downloads.
Troubleshooting		The Troubleshooting icon highlights information that can help you solve a problem or refer you to troubleshooting resources.
Settings		The Settings icon highlights settings you might need to choose or access.

Typographic Conventions

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

Typographic Conventions

<i>Convention</i>	<i>Description</i>
Bold	Highlights interface items such as menus, menu selections, window and dialog names, soft keys, file names, and directory names when they are involved in a procedure or user action. Also used to highlight text to be entered or typed.
<i>Italics</i>	Used to emphasize text, to show example values or inputs (in this form: <i><example></i>), and to show titles of reference documents available from the Polycom Support Web site and other reference sites.
Blue Text	Used for cross references to other sections within this document and for hyperlinks to non-Polycom web sites and documents such as third-party web sites and documentation.
<code>Courier</code>	Used for code fragments and parameter names.

Before You Begin

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

The Polycom UC solution for Microsoft is a suite of Polycom hardware devices and Session Initiation Protocol (SIP) software applications that enable you to integrate high-quality video and audio conferencing across Microsoft platforms, such as Microsoft Lync Server 2010 and 2013, SharePoint, Exchange Server, Skype for Business, and Office 365. The Microsoft Lync Server manages presence for each registered Polycom endpoint or component. The Microsoft UC infrastructure provides full-featured video calls between Lync clients and Polycom components, including point-to-point and video conferencing calls, high-quality video, content sharing, and direct calling from a contact list.

Required Skills

Deploying Polycom UC solution in a Microsoft environment requires planning and knowledge of SIP video conferencing and video conferencing administration. Note that this guide does not provide full administration or maintenance procedures for Microsoft Lync Server 2010 or 2013 and Skype for Business 2015. For full administrative procedures, see [Microsoft documentation](#).

This document assumes administrators have knowledge of the following systems, that these systems are already deployed, and that Microsoft administrators are available to assist administrators of the Polycom UC solution:

- Microsoft Active Directory
- Microsoft Exchange Server
- Domain name servers
- Microsoft Domain accounts
 - To participate in calls with Microsoft components, including Lync clients and Lync-hosted multipoint calls, your Polycom devices must have an account in a Windows domain accessible by the Lync or Skype for Business Server environment. You can create a new Lync or Skype for Business accounts for your Polycom device, or you can set up your Polycom device with an existing Lync or Skype for Business accounts. This Windows domain can be an Active Directory domain or a SIP domain. You need to configure the proper capabilities and settings at the account level, and at the domain level, with policies.
- Lync or Skype for Business Server.
 - For help with Lync Server 2013, see [Microsoft Lync Server 2013](#)
 - For help with Skype for Business 2015, see [Skype for Business 2015](#)
- Lync Server components. In particular, you should be familiar with [Lync Server Management Shell](#).

- Depending on which components of the Polycom UC solution you are using, Polycom® ContentConnect™ software, Polycom® RealPresence® Collaboration Server (RMX®) solution, Polycom® HDX® system, Polycom® RealPresence® Group Series system, and Polycom® RealPresence® Distributed Media Application™ (DMA®) system. You can access Polycom product documentation and software at [Polycom Support](#).

Hardware and Software Dependencies

Polycom products for use with this solution require at least one of the following Microsoft systems:

- Lync Server 2013 May 2015 Cumulative Update (5.0.8308.887)
- Skype for Business Server 2015 RTM

What's New?

New features for Microsoft Lync Server 2013 and support for Skype for Business Server 2015 vary by Polycom product and for this release include the following:

- Polycom RealPresence Collaboration Server (RMX)
 - Skype for Business support for MPMx-based hardware platforms
 - Version 8.5.4 of Collaboration Server (RMX) 1500, 2000 and 4000 (with MPMx media cards) supports on-premise Skype for Business deployments



Note: Collaboration Server (RMX) version 8.5.4

Version 8.5.4 of Collaboration Server (RMX) 1500 supports Skype for Business and is the last version that supports MPMx cards. Collaboration Server (RMX) 1500 will not be able to run MPMx cards or run version 8.6.

- RealPresence Group Series system
 - Receive native Lync and Skype for Business content through desktop and application sharing
 - Exchange Online
 - Native support for Polycom® RealConnect™ technology click-to-join functionality
 - Additional Lync and Skype for Business Presence state (Idle/Away)
- Polycom HDX systems do not currently support Skype for Business
- Federated Lync conference join for Polycom® ContentConnect™ gateway
- Polycom® RealPresence® Platform support for Lync Front End and Edge Server Failover
- Enhancements for RealPresence® Collaboration Server (RMX®) solution:
 - Polycom® RealConnect™ technology for service providers
 - Ability to allocate Collaboration Server (RMX) to the nearest standard endpoint joining the conference
 - Polycom RealConnect enhanced resiliency:
 - ◆ Automatic VMR re-establishment during Polycom RealConnect technology network loss

- ♦ Automatic VMR re-allocation during multipoint control unit (MCU) failure with Polycom RealConnect technology



Web Info: Release Notes for Polycom Unified Communications for Microsoft environments

For more information on what's new in this release and products tested for use with this solution, see the latest release notes at [Polycom Unified Communications Solution for Microsoft Environments](#).

Get Help

For more information about installing, configuring, and administrating Polycom products, refer to Documents and Downloads at [Polycom Support](#).

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

- [Lync Server Management Shell](#)
- [Microsoft's Lync Server 2013 Planning Tool](#) and [Skype for Business 2015 documentation](#) on the [Microsoft TechNet Library](#).

Polycom Resources

All Polycom documentation for Microsoft Lync solutions is available at [Polycom Unified Communications Solution for Microsoft Environments](#).

Polycom provides support for Polycom solution components only. Additional services for supported third-party UC environments integrated with Polycom solutions are available from Polycom Global Services. These services are intended to help customers successfully design, deploy, optimize, and manage Polycom visual communication within their third-party UC environments. If you want to deploy Polycom Conferencing for Outlook or Microsoft Lync Server, you need to contact [Polycom Services](#) or contact your local Polycom representative for more information.

The Polycom Community

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

Use Polycom-Enabled Unified Communications with Microsoft Lync and Skype for Business Server

This section provides an overview of the Polycom UC solution for Microsoft Lync Server 2010, 2013, and Skype for Business environments, including information on available features.

Features of the Polycom-Enabled Microsoft Solutions

Integrating Polycom products with Microsoft Lync 2013 and Skype for Business Server 2015 enables the following:

- Support for Exchange Online (Group Series only) and Microsoft Skype for Business
- Support for Polycom ContentConnect software
- Support for Microsoft Real-Time Video (RTV) and H.264 SVC
- Support for Native Polycom RealConnect technology Click-to-Join functionality
- Point-to-point calls among Polycom HDX systems, RealPresence Group Series systems, and Microsoft Lync clients
- Real-time presence information between Polycom devices and Microsoft Lync clients
- Support for remote and federated endpoints to participate in point-to-point calls and video conference calls
- High-quality video (720p for RTV and 1080p for SVC) between Lync clients and Polycom endpoints
- Participation in Lync Server-hosted multipoint conferences using Polycom endpoints
- Optional use of Microsoft Lync clients to view the presence status of Polycom RealPresence meeting rooms and to start one-click conferences

Polycom ContentConnect Software

Polycom ContentConnect software is a conference content sharing solution for Microsoft Lync clients and standard-based video endpoints. This solution enables you to receive and send content between different types of endpoints. You can enable Polycom ContentConnect software in two modes: Add-on Mode and Gateway Mode. This guide focuses on the new Gateway Mode, which enables client-less bi-directional content sharing between Lync and standards-based video room systems.



Note: Using Gateway Mode

Gateway Mode is supported only with Polycom ContentConnect for Microsoft Lync® and Lync Server 2013.

Gateway Mode

Polycom ContentConnect software Gateway Mode enables a Lync client or standards-based video room system to share content within a Polycom RealConnect technology meeting. This new mode was introduced in Polycom ContentConnect software and supports Microsoft Lync 2013 and Skype for Business clients that are participating within a Lync 2013 meeting. For previous versions of Polycom ContentConnect and Polycom ContentConnect software and documentation, see [Polycom RealPresence Content Sharing Suite](#).

In Gateway mode, the Polycom ContentConnect software works as a Remote Desktop Protocol (RDP) - Binary Floor Control Protocol (BFCP) content gateway that fully transcodes RDP and BFCP H.264 content streams. Client-side Lync software is no longer required as both signaling and content media conversion is performed infrastructure-side.



Note: Using Gateway Mode

Gateway Mode facilitates content sharing only between standards-based video room systems and Lync for Polycom RealConnect conferences. Note that you must set Polycom ContentConnect to Gateway Mode if you are using Polycom RealConnect technology. If you are direct dialing to RealPresence Platform, you must set Polycom ContentConnect to Add-On Mode.

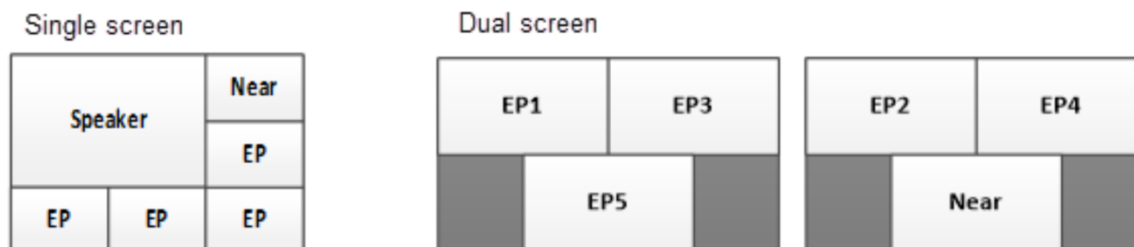
H.264 SVC

This solution supports Microsoft H.264 SVC. Previous releases for RealPresence Group Series system, RealPresence DMA system, and RealPresence Collaboration Server (RMX) solution delivered backward compatibility with Lync Server 2013. Now, RealPresence Group Series system, RealPresence DMA system, and RealPresence Collaboration Server (RMX) solution offer native support for Microsoft Real-time Video (RTV) and Microsoft H.264 SVC.

Continuous Presence

Polycom's native support for Microsoft SVC technology means that you can use Lync Server 2013 to host multipoint conferences with up to five active participants with continuous presence video. The new SVC layouts enable RealPresence Group Series systems to host up to five active speakers in a multipoint conference call using a single-screen or dual-screen layout that optimizes participant screen space. Two primary use cases are illustrated in the following figure.

Single and dual screen layouts on RealPresence Group Series systems



Viewing Content

RealPresence Group Series systems can view content from Microsoft Lync and Skype for Business desktop clients in active calls when a Lync or Skype for Business desktop client initiates the content-sharing request. RealPresence Group Series can view the following content types from Lync clients:

- **All Monitors** Displays content from all monitors connected to the system with the Lync client.
- **Primary Monitor** Displays content from the primary monitor connected to the system with the Lync client.
- **Secondary Monitor** Displays content from the secondary monitor connected to the system with the Lync client.
- **Program** Displays content from a particular program connected to the system with the Lync client.

For more information, refer to Microsoft Lync or Skype for Business documentation.

Polycom RealConnect for Microsoft Lync and Skype for Business

RealPresence DMA system and RealPresence Collaboration Server (RMX) solution feature Polycom RealConnect technology for Microsoft Lync and Skype for Business. Polycom RealConnect technology gives you the ability to send a Microsoft-compatible SVC stream from Polycom RealPresence platform products to an audio/video multipoint control unit (AVMCU) and receive up to five Lync or Skype for Business participants. Polycom RealConnect also enables you to join traditional standards-based video room systems to Lync or Skype for Business-hosted conferences, and to use Microsoft Outlook scheduling without the need for additional plug-in applications. Note that Polycom RealConnect technology still enables you to join Microsoft UC desktop clients and traditional video endpoints to a VMR, and offers standards-based systems you can use to add non-Lync or Skype for Business-capable, H.323, or standard SIP-registered endpoints. For more information on configuring RealPresence DMA systems, refer to the section [Enable RealPresence DMA system for Lync 2013 and Polycom RealConnect](#).

Dial Plans for a Lync Server Environment

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

MatchURI Dialing

Match uniform resource identifier (URI) dialing enables federated users to dial the full SIP URI of the conference room or endpoint, and is required to use links included in meeting invitations generated from Polycom Conferencing for Outlook.

MatchURI dialing is enabled as part of the process of creating a static route for the RealPresence Collaboration Server (RMX) solution or for the RealPresence DMA system you are using. Refer to the sections [Deploy Polycom RealPresence Collaboration Server Systems](#) or [Set the Routing for the RealPresence DMA System](#), respectively.



Note: Creating static routes in Skype for Business

For instructions on creating a MatchURI and provisioning a certificate, refer to [Appendix E: Configuring Static Routes in Skype for Business](#).

Support Remote and Federated Users in Lync Server Environments

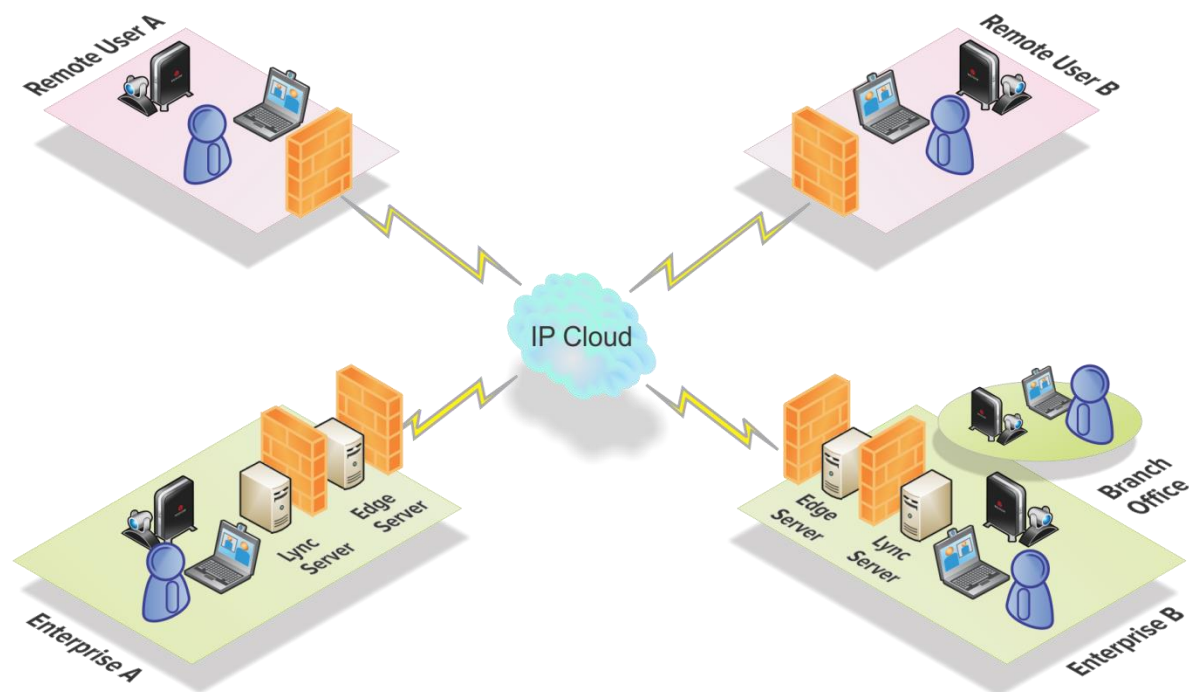
You can support remote and federated users by including a Lync Edge Server in your environment.

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

Installing an Edge Server to your Lync Server environment enables you to support the Interactive Connectivity Establishment (ICE) protocol. The ICE protocol enables devices outside an organization's network to call other devices that are also part of the Polycom-enabled unified communications solution. This functionality is supported with Lync Server 2013 and Skype for Business Server 2015, the Polycom video infrastructure, and Polycom video systems.

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

Lync Server environment with a Lync Edge Server



Users in enterprise A and B can place calls to remote user A and B. The remote users can call each other as well as users in both enterprises.

Lync Server 2013 Edge Server or Skype for Business Server 2015 environments support calls to the following devices:

- Polycom HDX and RealPresence Group Series systems
- Lync 2013 clients and Skype for Business 2015 clients
- Polycom RealPresence Collaboration Server (RMX) solutions
- Polycom RealPresence DMA systems

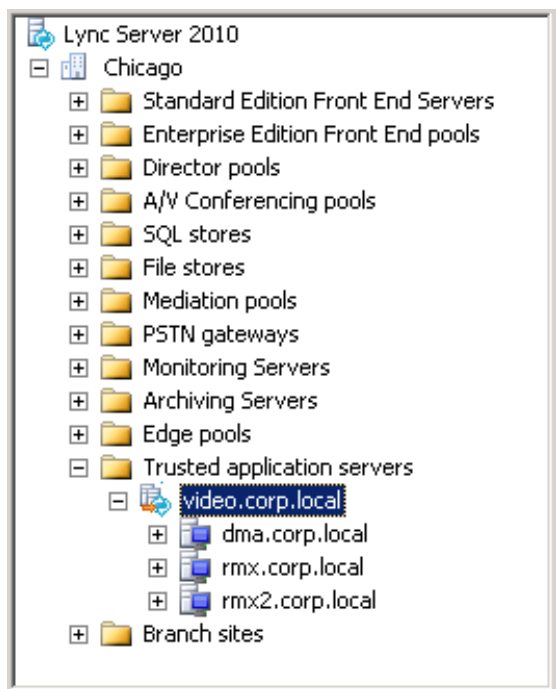
Microsoft Domains and Application Pools Best Practices

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

Use Multiple Computer Application Pools

As a best practice, create a multiple computer-trusted application server pool and include your RealPresence DMA system or RealPresence Collaboration Server (RMX) system SIP signaling domains as nodes under this pool, as shown next.

Using a multiple computer trusted application server pool



In this example, `video.corp.local` is the pool name. This method simplifies your Microsoft unified communications environment and also allows you to add additional RealPresence Collaboration Server systems or RealPresence DMA systems at a later time.

The fully qualified domain name (FQDN) of the DMA SIP signaling interface (`dma.corp.local`) and the two RealPresence Collaboration Server (RMX) SIP signaling domains (`rmx.corp.local` and `rmx2.corp.local`) are used as destination routes.

SIP Domain and MatchURI Configuration

When you configure a RealPresence Collaboration Server (RMX) solution or RealPresence DMA system for integration with Microsoft unified communications, you can create a Lync Server MatchURI.

- To configure for RealPresence Collaboration Server (RMX) solution see the section [Task 4: Use Lync PowerShell to Define a Static Route for the Polycom RealPresence Collaboration Server System](#).
- To configure for RealPresence DMA system see the section [Task 2: Use Lync PowerShell to Set the RealPresence DMA System as a Trusted Host with a Static Route](#).

For example, you can dial VMR <12345@*sipdomain.com*> to route to a VMR on RealPresence Collaboration Server (RMX) solution or RealPresence DMA system.

**Note: Creating static routes in Skype for Business**

For instructions on creating a MatchURI and provisioning a certificate in Skype for Business, refer to [Appendix E: Configuring Static Routes in Skype for Business](#).

This configuration is not required for deployments of Polycom RealConnect technology or RealPresence DMA VMRs with Lync Presence enabled. If, however, your deployment is created with RealPresence DMA VMRs that are not Lync presence-enabled, you need to create a MatchURI.

**Note: Trusted application pool or server destination address**

The destination address for the trusted application pool or server do not need to share the same domain extension as the SIP domain and the MatchURI can be different.

Consider the use of domains adopted for the MatchURI. Using the default Lync SIP domain is not recommended. There are two reasons why using an alternate domain is preferred:

- In larger enterprises, Lync generates an excessive number of SIP client subscriptions. Much of this traffic is not relevant to DMA and can create unnecessary stress on your RealPresence DMA system.
- Office 365 split-domain deployments are unable to route from Lync on-premises to Lync Online when you use the default SIP domain as a MatchURI.

When federation is required in your deployment, and you are adding an alternate domain as a MatchURI, for example, if sipdomain.com is the default domain and video.sipdomain.com is dedicated to the MatchURI, add the video.sipdomain.com as an alternate domain to Lync. Once this domain is published within your Lync Topology you must then publish

`_sipfederationtls._tcp.video.sipdomain.com` in public DNS and add this additional domain to your public Subject Alternative Name (SAN) certificates.

If the default SIP domain is already used in your deployment, Polycom recommends adding the preliminary script shown next to the 'Dial by Conference ID' dial rule and giving the dial rule a high order preference to ensure that SIP subscribe messages are ignored for subsequent rules:

```
//println(" Debug DIAL_STRING=" + DIAL_STRING);
var cseq = getHeader("CSeq");
//println("Debug cseq=" + cseq);
var pattern = new RegExp("subscribe");

if (DIAL_STRING != null
&& DIAL_STRING.toLowerCase().match(/^sip:[^@]*@sipdomain\.com*/)
&& cseq != null
&& pattern.test(cseq.toLowerCase()))
{
    println("Block SUBSCRIBE request via DMA to sipdomain.com");
    return BLOCK;
}
```

}

Microsoft Domains and DNS Entries

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

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

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

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

Microsoft Environments with Different SIP and Active Directory Domain Namespaces

<i>Domain</i>	<i>Example</i>	<i>Usage Notes</i>
Primary SIP domain for Lync	sipdomain.com	This domain should be used as the MatchURI in federated environments.
RealPresence DMA system FQDN	dma.corp.local	RealPresence DMA virtual signaling IP address. The FQDN must match the security certificate.
RealPresence Collaboration Server (RMX) solution FQDN	rmx.corp.local	RealPresence Collaboration Server (RMX) SIP signaling IP address. The FQDN used for DNS must match the security certificate.
Additional RealPresence Collaboration Server (RMX) solution FQDN	rmx2.corp.local	RealPresence Collaboration Server (RMX) SIP signaling IP address. The FQDN used for DNS must match the security certificate.
Application Pool	video.corp.local	Make this domain a user-friendly name to use to dial into conferences. This value does not need DNS representation.

Deploy Polycom RealPresence Group Series Systems

When deploying a Polycom RealPresence Group Series system for use with the solution, you must complete tasks in Lync Server 2013 or Skype for Business Server 2015 and the RealPresence Group Series system.

This section contains the following major tasks:

- [Configure Lync Server for use with a RealPresence Group Series System](#)
- [Configure Your Polycom RealPresence Group Series System for Lync Server](#)
- [Support Microsoft Real-Time Video \(RTV\) and H.264 SVC](#)

Configure Lync Server for use with a RealPresence Group Series System

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

- 1 [Configure Authentication in Lync Server](#)
- 2 [Use Microsoft Call Admission Control](#)
- 3 [Enable RTV on the Lync Server](#)
- 4 [Add Calendar and Scheduling Features to Polycom RealPresence Group Series Systems](#)
- 5 [Enable Conference Rooms for Lync Server](#)
- 6 [Enable Conference Room Access for Remote and Federated Users](#)
- 7 [Add Lync Contacts to Conference Room Local Address Book](#)



Note: Configure Lync client users in Microsoft Active Directory

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

Configure Authentication in Lync Server

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

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

Use Microsoft Call Admission Control

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

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

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

Enable RTV on the Lync Server

If you want to support high-quality RTV, you need to change the default video settings on Lync Server. Lync Server 2013 is by default enabled for full HD 1080p only on endpoints that support the Microsoft H.264 SVC codec. Polycom RealPresence Group Series and RealPresence Collaboration Server (RMX) support the Microsoft H.264 SVC codec; Polycom HDX systems do not.

To change the default video settings for your Lync Server:

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

Add Calendar and Scheduling Features to Polycom RealPresence Group Series Systems

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



Note: Set passwords to never expire

If conference room users have an expiring password, system administrators need to keep track of the users and passwords and update the accounts as required. Polycom recommends setting the passwords to never expire. For information on default user names and passwords, see the *Polycom RealPresence Group Series System Administrator Guide* for your product at [Telepresence and Video](#) on Polycom Support.

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 enable **Password never expires**.
- 5 Click **Next** and **Finish**.
- 6 Repeat for each conference room that has a Polycom RealPresence Group Series system.

Enable Conference Rooms for Lync Server

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

Polycom recommends using Lync PowerShell to do this. For more information, see [Windows PowerShell and Lync Server Management Tools](#).

To enable a conference room user for the Lync Server:

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

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

Enable Conference Room Access for Remote and Federated Users

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

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

After you have configured the Lync Edge Server, you can enable Lync Server to support remote and federated user access to a conference room. To enable remote and federated user access to a conference room, see [Microsoft Configuring Support for External User Access](#) for detailed instructions.

Enable Conference Room Accounts for Lync or Skype for Business Server

RealPresence Group Series system 5.0 enables you to use Remote Desktop Protocol (RDP) with Lync 2013 and Skype for Business 2015 clients. Using RDP with Microsoft clients enables both application and desktop sharing without additional infrastructure.

To maximize the benefits of RDP content sharing, Polycom recommends deploying a Skype Room System or `CsMeetingRoom` account to allow sharing from in-room clients. When you use this approach, the Skype Room System prompts content presenters to mute the microphone and speaker to avoid audio feedback.

To create a Skype Room System account, complete the following procedure and update your account name and server details on your Exchange Server Management Shell.

To create a Skype Room System account:

- 1 Within your Exchange Management Shell, set the following:

```
New-Mailbox -Name 'Group Series01' -Alias 'Group.Series01' -
UserPrincipalName 'Group.Series01@domain.com' -SamAccountName
'Group.Series01' -FirstName 'Group' -Initials '' -LastName 'Series01' -
Room
```

- 2

```
Set-CalendarProcessing -Identity Group.Series01 -AutomateProcessing
AutoAccept -AddOrganizerToSubject $false -RemovePrivateProperty $false -
DeleteSubject $false
```
- 3

```
Set-Mailbox -Identity Group.Series01@domain.com -MailTip "This room is
equipped with a Polycom Group Series, please make it a Skype Meeting to
take advantage of the enhanced meeting experience from Group Series"
```
- 4

```
Set-ADAccountPassword -Identity Group.Series01
```
- 5

```
Enable-ADAccount -Identity Group.Series01
```
- 6 Within your Lync or Skype for Business Management Shell, set:

```
Enable-CsMeetingRoom -SipAddress "sip:Group.Series01@domain" -
domaincontroller dc.domain.local -RegistrarPool pool01.domain.local -
Identity Group.Series01
```

Add Lync Contacts to Conference Room Local Address Book

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

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

For more information about displaying contacts on your RealPresence Group Series system, see [Configure Display Options for the RealPresence Group Series System Contact List](#).



Note: Configure a maximum of 200 personal contacts per RealPresence Group Series system user

Polycom recommends that you configure the Lync Server to allow no more than 200 contacts per user. Though the Lync Server and Skype for Business default setting is 250, the RealPresence Group Series system displays a maximum of 200 contacts per user.

Configure Polycom RealPresence Group Series System for Lync or Skype for Business Server

Before you begin configuring your Polycom RealPresence Group Series system for a Microsoft environment, you should ensure that the RealPresence Group Series system is installed according to standard installation procedures. To identify the installation required for your RealPresence Group Series system, see the *Polycom RealPresence Group Series Administrator Guide* for your model at [Group Series](#) on Polycom Support. You must complete the following tasks to configure your RealPresence Group Series system for a Microsoft environment:

- [Install the Skype for Business Interoperability License on your RealPresence Group Series System](#)
- [Register a Polycom RealPresence Group Series System with the Lync Server](#)
- [Understand SIP Settings](#)
- [Configure the Polycom RealPresence Group Series System LAN Properties](#)
- [Configure Display Options for the RealPresence Group Series System Contact List](#)
- [Configure AES Encryption](#)
- [Support Lync-hosted Video Conferencing and or Lync Server 2013](#)
- [Support Microsoft Real-Time Video \(RTV\)](#)

Install the Skype for Business Interoperability License on your RealPresence Group Series System

When using Lync 2013 or Skype for Business 2015, support for RTV and H.264 SVC is mandatory for point-to-point and multiparty calls and you must install the Skype for Business Interoperability License.



Note: Register Polycom endpoints to Lync Server for RTV and H.264 SVC video and conferencing

RTV and H.264 SVC video and Lync-hosted conferencing are supported only when you directly register Polycom endpoints to Lync Server.

Register a Polycom RealPresence Group Series System with Lync Server

When you register a RealPresence Group Series system with a Lync Server, the Polycom RealPresence Group Series system user can see a list of Lync 2013 or Skype for Business 2015 contacts and whether contacts are online or offline. Contacts display in the directory and users can choose to display up to five contacts on the home screen or call a contact. You can find descriptions of all SIP settings shown in this procedure in the section [Understand SIP Settings](#).

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

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

After the RealPresence Group Series system registers with Lync Server, continue to the section [Configure the Polycom RealPresence Group Series System LAN Properties](#).



Note: H.263 codec deprecated and Skype for Business Interoperability License required with Lync Server 2013

The H.263 codec has been deprecated and a Skype for Business Interoperability License is required for integration with Lync Server 2013.

Understand SIP Settings

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

RealPresence Group Series system SIP settings

The screenshot shows the Polycom Group Series RealPresence Group 500 web interface. The top header includes the Polycom logo, the system name 'Group Series RealPresence Group 500', the current IP address '10.218.48.109', a language dropdown set to 'American English', and links for 'Home' and 'System'. The left sidebar contains navigation links: 'Manage Favorites', 'Admin Settings' (with sub-links for General Settings, Network, LAN Properties, IP Network, Dialing Preference, Audio / Video, Security, and Servers), 'Diagnostics', 'Utilities', and 'Site Map'. The main content area is titled 'Network Quality' and 'H.323'. Under the 'SIP' section, the following settings are visible: 'Enable SIP' (checked), 'Enable AS-SIP' (unchecked), 'SIP Server Configuration' (set to 'Auto'), 'Transport Protocol' (set to 'Auto'), 'Sign-in Address' (user@sipdomain.com), 'User Name' (user@windowsdomain.local), 'Password' (masked with a blue square), 'Registrar Server' (empty), 'Proxy Server' (empty), and 'Registrar Server Type' (set to 'Microsoft'). At the bottom right of the settings area are 'Revert' and 'Save' buttons. Below the SIP settings, there are expandable sections for 'AS-SIP', 'Quality of Service', and 'Firewall'.

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

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

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

Syntax Examples:

- To use the default port for the protocol you have selected: `lyncserver.corp.local`
- To specify a different Transport Layer Security (TLS) port and use the default Transmission Control Protocol (TCP) port: `lyncserver.corp.local:443`
- **Proxy Server** Specify the DNS name or IP address of the SIP Proxy Server. If you leave this field blank, the Registrar Server is used. If you selected Auto for your SIP Server Configuration and leave the Proxy Server field blank, no Proxy Server is used.

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

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

**Note: The Proxy server and Registrar server are the same.**

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

- **Transport Protocol** The SIP network infrastructure in which your Polycom RealPresence Group Series system is operating determines which protocol is required.
 - **Auto** enables an automatic negotiation of protocols in the following order: TLS, TCP, User Datagram Protocol (UDP). This is the recommended setting for Microsoft environments.
 - **TLS** provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060. TLS is required when connecting to Microsoft Lync.
 - **TCP** provides transport via TCP for SIP signaling and is not applicable for Lync. Signaling encryption is mandatory.
 - **UDP** provides transport via UDP for SIP signaling.
- **Sign-in Address** Specify the system's SIP name. This is the SIP URI or Lync sign-in address. Specify the address for the conference room or user account created for the Polycom system.
- **User Name** Specifies the name and Windows Domain to use for authentication when registering with a SIP Registrar Server, for example, `<user@windowsdomain.local>`.
Polycom RealPresence Group Series systems supports the User Principal Name format `<username@domain.com>` as well as the legacy Microsoft DOMAIN\username format. If the SIP server requires authentication, this field and the password cannot be blank.
- **Password** When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP Server.
- **Registrar Server Type** For Lync Server this must be set to Microsoft.

**Note: Default user name and password**

For information on default user names and passwords, see the *Polycom RealPresence Group Series System Administrator Guide* for your model at [Group Series](#) on Polycom Support.

Configure the Polycom RealPresence Group Series System LAN Properties

To register with Lync Server, the RealPresence Group Series system must be able to access a DNS server and the name for the Lync Pool or Lync Edge Server must have a valid domain name resolution.

To configure the Polycom system LAN properties:

- 1 Open a browser window and in the **Address** field enter the Polycom system IP address or host name.
- 2 Go to **Admin Settings > Network > LAN Properties**.
- 3 If needed, enter the **Domain Name** for the domain to which the Polycom system belongs.
- 4 In the **DNS Servers** field, verify that the correct DNS server addresses are populated if you are using DHCP to assign addresses. If the DNS server addresses are not correctly populated, enter the IP addresses for DNS servers that share DNS zone information with the Lync Server. If you are registering a remote Polycom system, use a public DNS server that shares DNS zone information with the Lync Edge Server.
- 5 Click **Update**.

Configure Display Options for the RealPresence Group Series System Contact List

You can configure display options for your Microsoft contacts in your RealPresence Group Series system contact list.

To configure display options for the contact list:

- 1 Open a browser window and in the **Address** field enter the Polycom RealPresence Group Series system IP address or host name.
- 2 Go to **Admin Settings > Servers > Directory Servers**.
- 3 In the **Lync Server** section of the Directory Servers page, configure these settings:
 - **Server Type** Specifies whether the SIP Registrar Server is a Lync Server. Enabling this setting activates integration features such as the Microsoft global directory and Lync contact sharing with presence.
 - **Registration Status** Upon successful authentication this field displays as Registered, as shown in the next figure.
 - **Domain Name** Specifies the Windows Domain to use for Directory lookup, for example, `windowsdomain.local`.
 - Polycom RealPresence Group Series systems supports the User Principal Name format `<windowsdomain.local>` as well as the legacy Microsoft NETBIOS domain format.
- 4 Click **Save**.

Directory Servers	
Server Type:	Microsoft
Registration Status:	Registered
Domain Name:	windowsdomain.local
Domain User Name:	user@windowsdomain.local
User Name:	user@sipdomain.com



Note: Personal Lync contacts do not display until you complete Directory Services configuration

If you don't complete the Directory Services configuration, the Lync Directory search, personal favorites, and contacts list do not display in the Contacts menu.

Configure AES Encryption

Polycom endpoint systems support AES media encryption. Your system encryption settings must be compatible with your Lync Server settings. For more information on Lync Server encryption, refer to the section [Configure Encryption](#).

Each codec within Polycom systems must have the same settings.

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

To configure AES encryption:

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

Configure Encryption Settings for Skype for Business 2015 and Microsoft Lync 2013

Polycom RealPresence Group systems support media encryption in calls with Skype for Business 2015 and Microsoft Lync 2013. Skype for Business 2015, Microsoft Lync 2013 Server pool, and the Polycom RealPresence Group system must be configured to support encryption so that calls can connect with encryption. If 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.

Before you use Microsoft Lync 2013 or Skype for Business 2015 in video conferences with RealPresence Group systems, you must enable AES encryption in the web interface.

To enable encryption for Microsoft Lync 2013 and Skype for Business 2015:

- 1 Go to **Admin Settings > Security > Global Security > Encryption > Require AES Encryption for Calls** and select **When Available**.
- 2 On the Skype for Business Server go to `Get-CsMediaConfiguration` and change the encryption setting to:
`Set-CsMediaConfiguration -EncryptionLevel supportencryption`.
(The default setting is:
`Set-CsMediaConfiguration -EncryptionLevel requireencryption`)

Support Lync-hosted Video Conferencing Lync Server 2013 and Skype for Business

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

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

- When in a Lync-hosted call, the Polycom RealPresence Group Series system displays a Busy presence state and rejects any incoming calls.
- When in a Lync-hosted call, other multipoint calling methods, such as internal multipoint hosting, RealPresence Collaboration Server (RMX)/RealPresence DMA hosted conferencing, and Conference on Demand, are disabled.
- You need to install the Skype for Business Interoperability License on your RealPresence Group Series system to support Lync-hosted conference calls and to use up to 1080p high-definition video between a RealPresence Group Series system and Lync client.
- You need the Skype for Business Interoperability License to enable support for Lync Server 2013.
- In SVC multipoint calls hosted on Microsoft Lync Server 2013, you can view multiple far-end sites in layouts. Note that when using Polycom RealPresence Group Series systems, layouts vary by model. On RealPresence Group Series 300, 500, and 700 systems you can view a maximum of five far-end sites as shown in the figure [Single and Dual Screen Layouts on RealPresence Group Series Systems](#).

In conferences hosted on Lync and Skype for Business, RealPresence Group Series systems require a Polycom Touch Control to:

- View the conference participants
- Add participants to the conference
- Organize and initiate conferences with Polycom RealPresence Group Series and Microsoft Lync clients and groups

Use the Polycom Touch Control with Lync Conferencing

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

To initiate a Lync-hosted call:

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

The conference call is initiated.

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

- 4 To view all participants in a call, touch **Participants** from the call screen.

Understand Roles in Lync-hosted Calls

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

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

Managing Participants in a Lync-hosted Call

<i>Role</i>	<i>Add a Participant</i>	<i>View Participants</i>
Organizer	Y	Y
Presenter	Y	Y
Attendee	N	Y

Managing a Lync-Hosted Call

<i>Role</i>	<i>Remove a Participant</i>	<i>End a Conference</i>	<i>Leave a Conference</i>	<i>Mute a Participant</i>	<i>Mute a Conference</i>	<i>Mute Self</i>
Organizer	Y	Y	Y	Y	Y	Y
Presenter	N	N	Y	Y	Y	Y
Attendee	N	N	Y	N	N	Y

Polycom Support for Microsoft Real-Time Video (RTV) and H.264 SVC

The Microsoft Lync 2013 and Skype for Business 2015 clients use both the RTV protocol and H.264 SVC. Polycom supports the RTV protocol for both Lync 2013 and Skype for Business 2015, and includes support for the Microsoft H.264 SVC codec for RealPresence Group Series and Polycom Collaboration Server (RMX) solution. You must install the Skype for Business Interoperability License to enable the RTV and H.264 SVC protocols for RealPresence Group Series and to register endpoints with Lync Server 2013.

The following Polycom systems support the Microsoft RTV and H.264 SVC protocols:

- Polycom RealPresence Group Series systems with the Skype for Business Interoperability License
- Polycom Collaboration Server (RMX) solutions with the MPMx or MPMrx cards
- Software-based Polycom Collaboration Server 800s and RealPresence One

Call Quality Scenarios for RTV Video

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

- RTV and H.264 SVC video require a minimum call rate of 128 kbps. Calls below this rate connect with audio only.
- Multipoint calls initiated by a Microsoft Lync client are hosted on the Microsoft AVMCU. You must install the Skype for Business Interoperability License to connect RealPresence Group Series systems. Multipoint calls initiated by a RealPresence Group Series system with the Skype for Business Interoperability License installed are also hosted on the Microsoft AVMCU.
- Multipoint calls initiated by a RealPresence Group Series system that does not have the Skype for Business Interoperability License are hosted on the RealPresence Group Series system's internal multipoint control unit (MCU) and do not use RTV or H.264 SVC. If a Lync client joins the call, the entire call will be conducted on H.263/CIF.
- On point-to-point calls with Microsoft clients, the RealPresence Group Series system uses RTV or H.264 SVC with Lync 2013 and Skype for Business when the Skype for Business Interoperability License is installed. You must install the Skype for Business Interoperability License to make point-to-point calls and multi-point calls with Lync 2013 and Skype for Business.

- When you call into a RealPresence Collaboration Server conference that includes participants using a RealPresence Group Series system, Polycom HDX system, or Polycom ITP system, Polycom systems can use H.264 while Lync uses either RTV or H.264 SVC.
- Polycom ITP systems only use RTV on point-to-point calls with a Lync client and connect only with the primary codec.
- When calling from RealPresence Group Series and RealPresence Collaboration Server to Lync 2013 H.264 SVC is prioritized higher than RTV. H.264 SVC also delivers higher resolution video 1080p vs a maximum of 720p (for point-to-point) with RTV it also reduces the need for Lync 2013 clients to send additional video streams comprised of RTV.

Enable Native Polycom RealConnect Click-to-Join Functionality

Polycom RealPresence Group Series 5.0 includes the ability to directly join room systems to Polycom RealConnect meetings without manually typing the Lync Conference ID. This feature is available for H.323 and SIP-registered RealPresence Group Series systems, as well as for dual-registered Lync and H.323 endpoints.

RealPresence Group Series deployments running versions earlier than 5.0. Non-Polycom VTCs and Polycom HDX systems supported by this solution still require the RealPresence Calendar Proxy.

To enable Polycom RealConnect click-to-join functionality:

- » To enable click-to-join functionality, add the following metadata to the meeting invitation sent to the mailbox associated with the RealPresence Group Series system.

```
Admin BeginAdmin::Prefix::<Prefix #>Admin::Domain::<SIP or H.323  
Domain>Admin End
```

With the exception of the Lync Conference ID, which is supplied by the Lync Server, this metadata is static. For this reason, Polycom recommends that you update your Lync Server Meeting Configuration with custom footer text indicating the appropriate dial string.

The metadata can be used for two purposes:

- **Prefix field.** To automatically prepend a prefix number prior to the Lync Conference ID.
This is useful when deploying Polycom RealConnect for Service Providers and a tenant-specific prefix is required to route to the correct Conference Auto Attendant.
- **Domain field:** To route the call outside of your organization to a neighbored organization.
This is useful for invitations sent from other parties or when deploying an instance of RealPresence Platform hosted by a service provider.

The following is an example configuration showing how you can configure your invitation to route the call to the domain Polycom.com with the prefix 76.

Lync Server 2013 Administrator | [Sign out](#)
5.0.8308.556 | [Privacy statement](#)

Navigation: Home, Users, Topology, IM and Presence, Persistent Chat, Voice Routing, Voice Features, Response Groups, **Conferencing**, Clients, Federation and External Access, Monitoring and Archiving, Security, Network Configuration

Configuration Tabs: Conferencing Policy, **Meeting Configuration**, Dial-in Access Number, PIN Policy

Meeting Configuration Form:

- Commit** **Cancel**
- Scope:** Global
- Name:** *
Global
- ☒ **PSTN callers bypass lobby**
- Designate as presenter:**
Company
- ☒ **Assigned conference type by default**
- ☐ **Admit anonymous users by default**
- Logo URL:**
<https://webext.polycom.com/logo.jpg>
- Help URL:**
<https://webext.polycom.com/help.txt>
- Legal text URL:**
<https://webext.polycom.com/legal.txt>
- Custom footer text:**
To join this meeting from a traditional video conferencing system you can utilize the numeric 'Conference ID' provided in this invitation.
H.323 and SIP systems can dial ID@polycom.com (for example 12345@polycom.com)
Admin BeginAdmin::Prefix:76Admin::Domain:polycom.comAdmin End

Deploy Polycom HDX Systems

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



Note: Polycom HDX systems do not support Skype for Business

At this time, the Polycom HDX system does not support Skype for Business.

This section contains the following major tasks:

- [Configure Lync Server for use with a Polycom HDX System](#)
- [Configure Your Polycom HDX System for Lync Server](#)
- [Support Microsoft Real-Time Video \(RTV\)](#)

Configure Lync Server for use with a Polycom HDX System

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

- 1 [Configure Authentication in Lync Server](#)
- 2 [Use Microsoft Call Admission Control](#)
- 3 [Enable RTV on the Lync Server](#)
- 4 [Add Calendar and Scheduling Features to Polycom HDX Systems](#)
- 5 [Enable Conference Rooms for the Lync Server](#)
- 6 [Enable Conference Room Access for Remote and Federated Users](#)
- 7 [Add Lync Contacts to Conference Room Local Address Book](#)



Note: Configure Lync client users in Microsoft Active Directory

Before completing tasks in this section, you must configure Lync client users in Microsoft Active Directory and enable Lync Server. Talk to your Microsoft Active Directory and Lync Server administrators or visit [Preparing Active Directory Domain Services for Lync Server 2013](#).

Configure Authentication in Lync Server

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

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

Use Microsoft Call Admission Control

Microsoft CAC policies are supported and enforced when your HDX system is registered to a Microsoft Lync Edge Server.

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

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

Enable RTV on the Lync Server

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

To change the default video settings for your Lync Server:

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

Add Calendar and Scheduling Features to Polycom HDX Systems

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

**Note: Set passwords to never expire**

If these conference room users have an expiring password, you will need to keep track of the users and passwords and make sure to update the accounts as required. Polycom recommends setting the passwords to never expire. For information on default user names and passwords, see the *Polycom HDX Systems Administrator Guide* for your model at [Telepresence and Video](#) on Polycom Support.

To add a conference room user to the Active Directory:

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

Enable Conference Rooms for the Lync Server

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

Polycom recommends using Lync PowerShell to do this. For more information, see [Windows PowerShell and Lync Server Management Tools](#).

To enable a conference room user for the Lync Server:

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

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

Enable Conference Room Access for Remote and Federated Users

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

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

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

For detailed instructions on configuring support for external users in Lync Server, see [Configuring Support for External User Access](#) on Microsoft TechNet.

Add Lync Contacts to Conference Room Local Address Book

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

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

For more information about displaying contacts in your Polycom HDX system, refer to the section [Configure Display Options for the Polycom HDX System Contact List](#).



Note: Configure a maximum of 200 contacts per Polycom HDX system user

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

Configure Your Polycom HDX System for Lync Server

Before you begin configuring your Polycom HDX system for a Microsoft environment, you should ensure that the Polycom HDX system is installed according to standard installation procedures. To identify the installation required for your Polycom HDX system, see the *Polycom HDX Systems Administrator Guide* for your model at [HDX Series](#) on Polycom Support. Configuring your Polycom HDX system for a Microsoft environment requires the following tasks:

- [Install the RTV Option Key on your Polycom HDX System](#)
- [Register Polycom HDX System with the Lync Server](#)
- [Understand SIP Settings](#)
- [Configure the Polycom HDX System LAN Properties](#)
- [Configure Display Options for the Polycom HDX System Contact List](#)
- [Configure AES Encryption](#)
- [Support Lync-hosted Video Conferencing and Lync Server 2013](#)
- [Support Microsoft Real-Time Video \(RTV\)](#)

Install the RTV Option Key on your Polycom HDX System

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


Note: Register Polycom endpoints to Lync Server for RTV video and conferencing

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

Register Polycom HDX System with the Lync Server

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

To configure a Polycom HDX system to register with Lync Server:

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

Configure the system so that users can place and receive calls using IP on your LAN or WAN.

<ul style="list-style-type: none"> General Settings <ul style="list-style-type: none"> System Settings Home Screen Settings Security Location Date and Time Serial Port Options Software Update Network <ul style="list-style-type: none"> IP Network Telephony Call Preference Network Dialing Call Speeds Monitors Cameras Audio Settings LAN Properties Global Services Tools 	IP Network Update SIP Settings Enable SIP: <input checked="" type="checkbox"/> SIP Server: Auto Configuration: Server Name or IP: Address: Transport Protocol: Auto Sign-in Address: user1@sipdomain.com User Name: user1 Password: <input type="checkbox"/> Directory: Microsoft Lync Server 2010: <input checked="" type="checkbox"/> Domain Name: corp.local Quality of Service Type of Service: IP Precedence Type of Service Value:
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



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

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

Configure the system so that users can place and receive calls using IP on your LAN or WAN.

<ul style="list-style-type: none"> General Settings <ul style="list-style-type: none"> System Settings Home Screen Settings Security Location Date and Time Serial Port Options Software Update Network <ul style="list-style-type: none"> IP Network Telephony Call Preference Network Dialing Call Speeds Monitors Cameras Audio Settings LAN Properties Global Services Tools 	<p>IP Network Update</p> <p>SIP Settings</p> <p>Enable SIP: <input checked="" type="checkbox"/></p> <p>SIP Server: Auto</p> <p>Configuration: Auto</p> <p>Registrar Server: <input type="text"/></p> <p>Proxy Server: <input type="text"/></p> <p>Transport Protocol: Auto</p> <p>User Name: <input type="text" value="user1@sipdomain.com"/></p> <p>Domain User Name: <input type="text" value="user1"/></p> <p>Password: <input type="checkbox"/></p> <p>Directory:</p> <p>Microsoft Lync Server 2010: <input checked="" type="checkbox"/></p> <p>Domain Name: <input type="text" value="corp.local"/></p> <p>Quality of Service</p> <p>Type of Service: IP Precedence</p> <p>Type of Service Value: <input type="text"/></p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4 Click Update.

After the Polycom HDX system registers with Lync Server, continue to the section [Configure the Polycom HDX System LAN Properties](#).

Understand SIP Settings

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

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

- If registering a remote Polycom HDX system with a Lync Edge Server, use the FQDN 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: Setting name change if you have not installed the RTV option key

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: Setting hidden if you install the RTV option key

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

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

- **Sign-in Address** Specify the system's SIP name. This is the SIP URI. Specify the user name for the conference room or user account created for the Polycom system.



Note: Setting name change if you have not installed the RTV option key

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

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

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



Note: Setting name change if you have not installed the RTV option key

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

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



Note: Default user name and password

For information on default user names and passwords, see the *Polycom HDX Systems Administrator Guide* for your model at [HDX Series](#) on Polycom Support.

Configure the Polycom HDX System LAN Properties

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

To configure the Polycom system LAN properties:

- 1 Open a browser window and in the **Address** field enter the Polycom system IP address or host name.
- 2 Go to **Admin Settings > LAN Properties**.
- 3 If needed, enter the **Domain Name** for the domain to which the Polycom system belongs.

- 4 In the **DNS Servers** field enter the IP address for a DNS server that shares DNS zone information with the Lync Server. If you are registering a remote Polycom system, use a public DNS server that shares DNS zone information with the Lync Edge Server.
- 5 Click **Update**.

Configure Display Options for the Polycom HDX System Contact List

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

To configure display options for contact list information:

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

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.

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

Each codec within Polycom systems must have the same settings.

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

To configure AES encryption:

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

Support Lync-hosted Video Conferencing and Lync Server 2013

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

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

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

A Polycom Touch Control is required for the following Polycom 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 system and Microsoft Lync clients and groups.

Use the Polycom Touch Control with Lync Conferencing

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

To initiate a Lync-hosted call:

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

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

- 4 To view all participants in a call, touch **Participants** from the call screen.

Understand Roles in Lync-hosted Calls

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

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

Managing Participants in a Lync-Hosted Call

<i>Role</i>	<i>Add a Participant</i>	<i>View Participants</i>
Organizer	Y	Y
Presenter	Y	Y
Attendee	N	Y

Managing a Lync-Hosted Call

<i>Role</i>	<i>Remove a Participant</i>	<i>End a Conference</i>	<i>Leave a Conference</i>	<i>Mute a Participant</i>	<i>Mute a Conference</i>	<i>Mute Self</i>
Organizer	Y	Y	Y	Y	Y	Y
Presenter	N	N	Y	Y	Y	Y
Attendee	N	N	Y	N	N	Y

Support Microsoft Real-Time Video (RTV)

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

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

The following Polycom systems support the RTV protocol:

- Polycom HDX systems with the RTV option key
- Polycom ITP systems

Call Quality Scenarios for RTV

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

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

Deploy Polycom RealPresence Collaboration Server (RMX) Solution

To integrate your Polycom RealPresence Collaboration Server (RMX) solution with Lync Server 2013, you must add a DNS entry, and create and install a security certificate. You also need to add a static route on the Lync Server for the RealPresence Collaboration Server (RMX) solution to use, and enable Lync presence for each RealPresence Collaboration Server (RMX) solution's virtual meeting room that you use.

If you need to support remote or federated users, your deployment must include a 2013 Edge Server. For more information, see [Support Remote and Federated Users in Lync Server Environments](#).

This section outlines the following tasks required to configure Polycom RealPresence Collaboration Server (RMX) solution Lync Server 2013.

You need to complete these tasks in the following order:

- 1 [Configure Polycom RealPresence Collaboration Server \(RMX\) System for Lync Server](#)
- 2 [Enable Microsoft Presence for Lync Server 2013](#)
- 3 [Enable Edge Server Integration with Polycom RealPresence Collaboration Server \(RMX\) System](#)
- 4 [Configure RealPresence Collaboration Server \(RMX\) for Polycom ContentConnect Software](#)

Configure Polycom RealPresence Collaboration Server (RMX) System for Lync Server

To begin, you must configure your RealPresence Collaboration Server (RMX) solution for use in a Lync Server environment. This includes setting up your RealPresence Collaboration Server (RMX) solution for SIP, creating security certificates, and ensuring encryption settings.

Complete the following steps:

- [Set up the RealPresence Collaboration Server \(RMX\) System for Security and SIP](#)
- [Create and Install a Security Certificate for the Polycom RealPresence Collaboration Server \(RMX\) System](#)
- [Install the certificate on your RealPresence Collaboration Server \(RMX\) solution](#)
- [Configure Encryption](#)
- [Configure Lync Server for use with a Polycom RealPresence Collaboration Server \(RMX\) System](#)

Set Up the RealPresence Collaboration Server (RMX) System for Security and SIP

Your RealPresence Collaboration Server (RMX) solution must be accessible via DNS and must be configured for SIP calls.

In this section, complete the following two tasks:

- [Task 1: Configure the RealPresence Collaboration Server \(RMX\) IP Network Service](#)
- [Task 2: Add the RealPresence Collaboration Server \(RMX\) FQDN \(SIP signaling IP address\) in DNS](#)

Task 1: Configure the RealPresence Collaboration Server (RMX) IP Network Service

You must configure the IP network services to include SIP.

To configure the RealPresence Collaboration Server (RMX) IP Network Service:

- 1 Using a web browser, connect to the RealPresence Collaboration Server (RMX).
- 2 In the **RealPresence Collaboration Server (RMX) Management** pane, expand the **Rarely Used** list and click **IP Network Services**.
- 3 In the **IP Network Services** pane, double-click the **Default IP Service** entry.
The Default IP Service - Networking IP dialog opens.
- 4 Make sure the **IP Network Type** is set to **H.323 & SIP** even though SIP will be the only call setup you use with the Lync Server.
- 5 Make sure that the correct parameters are defined for the Signaling Host IP Address, Media Card 1 IP Address, Media Card 2 IP Address (RealPresence Collaboration Server 2000/4000 if necessary), Media Card 3 IP Address (RealPresence Collaboration Server 4000 if necessary), Media Card 4 IP Address (RealPresence Collaboration Server 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 Lync Front End server or Pool name and the server domain name.
- 10 If not selected by default, change the **Transport Type** to **TLS**.

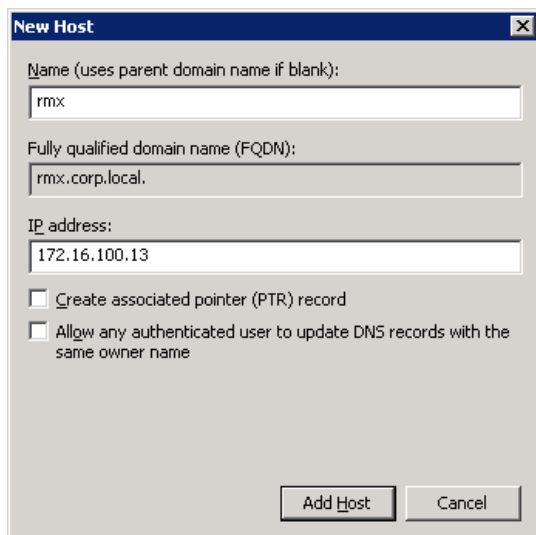
Task 2: Add the RealPresence Collaboration Server (RMX) FQDN (SIP Signaling IP address) in DNS

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

The RealPresence Collaboration Server (RMX) solution and the Lync Server must both resolve the RealPresence Collaboration Server (RMX) host record identically, regardless of the domain you select to store the DNS Host record.

To create a DNS record:

- 1 On the computer where the DNS manager is installed, open the **DNS Manager** and expand the **Forward Lookup Zone**.
- 2 Right-click the appropriate domain zone and select **New Host (A or AAAA)**.
The New Host dialog opens.
- 3 Define the new record. The following figure defines a record using `rmx.corp.local` for the FQDN for the RealPresence Collaboration Server (RMX) SIP signaling domain and 172.16.100.13 as the IP address of the RealPresence Collaboration Server (RMX) signaling host.



- 4 Click **Add Host**.
- 5 Click **OK** to confirm and then click **Done**.

Create and Install a Security Certificate for the Polycom RealPresence Collaboration Server (RMX) System

You must install a security certificate on the RealPresence Collaboration Server (RMX) solution so that Lync Server trusts it.

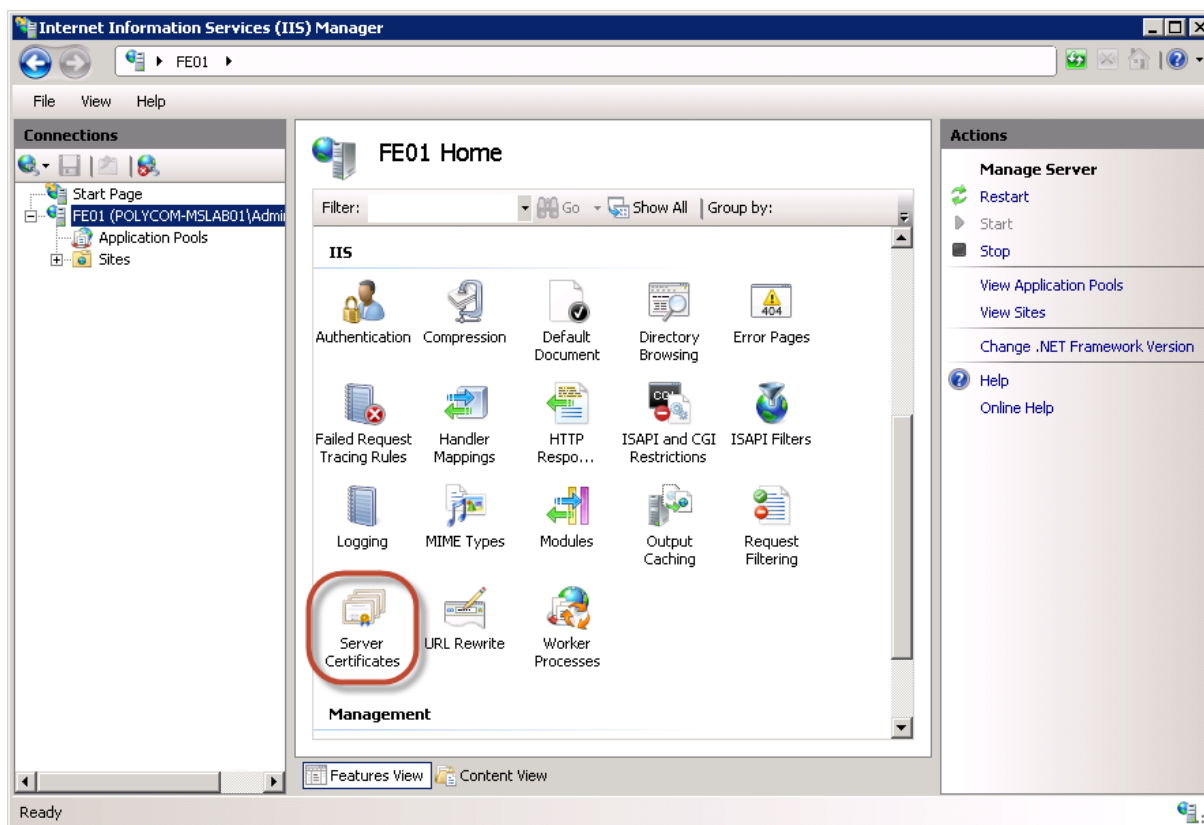
You can install a security certificate using one of the following two ways:

- Purchase and install a certificate from a commercial Trusted Root certificate authority (CA) such as VeriSign or Thawte. Use the procedures in the Polycom RealPresence Collaboration Server (RMX) solution'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 one of three ways:
 - If you must submit certificate requests through the enterprise's CA team or group, use the procedures in the *Polycom RealPresence Collaboration Server (RMX) Administrator Guide* to create a Certificate Signing Request and to install the certificate(s) received from the CA team or group.

- If your organization permits the submission of certificate requests directly to the enterprise's CA server, you can use the Internet Information Services (IIS) Manager on the Lync Server to download an export file of the certificate to your computer for later installation on the Polycom RealPresence Collaboration Server (RMX) solution. This procedure is described next.
- If your organization requires that all certificates be generated externally, then follow those procedures to generate the certificates and install them on your system using the procedures outlined in *Polycom RealPresence Collaboration Server (RMX) Administrator Guide* for your model at [Collaboration & Conferencing Platforms](#) on Polycom Support.

To request a security certificate for the Polycom RealPresence Collaboration Server (RMX) solution using IIS Manager 7:

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



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



The Create Certificate wizard displays.

- 5 In the **Distinguished Name Properties** panel, shown next, complete all fields. Do not leave any fields blank.
- In the **Common Name** field, enter the FQDN of RealPresence Collaboration Server (RMX) SIP signaling interface.

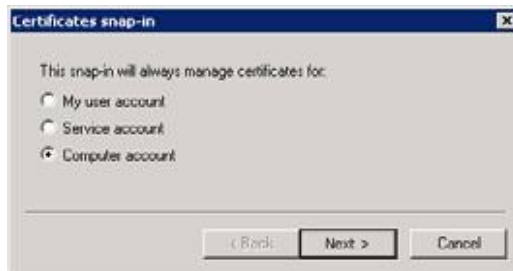
A screenshot of a 'Create Certificate' wizard window. The title bar says 'Create Certificate'. The main panel is titled 'Distinguished Name Properties'. Below the title, there is a small icon of a certificate and a text instruction: 'Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.' Below this instruction are several input fields: 'Common name:' with the value 'rmx.corp.local', 'Organization:' with the value 'Video Infrastructure', 'Organizational unit:' with the value 'IT', 'City/locality' with the value 'London', 'State/province:' with the value 'London', and 'Country/region:' with a dropdown menu showing 'UK'. At the bottom of the panel are four buttons: 'Previous', 'Next' (which is highlighted with a dashed border), 'Finish', and 'Cancel'.

- 6 Click **Next**.
- 7 In the **Online Certification Authority** panel, select a certificate authority from the list and enter a name.
- 8 Click **Finish**.
- Your certificate is created.

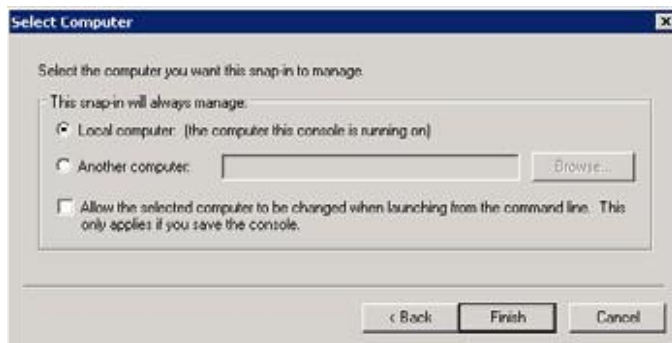
To use the Microsoft Management Console to export the created certificate:

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

- a Choose **File > Add/Remove Snap-in**.
- b Select **Certificates** from the Available Snap-ins area and click **Add**.
- c On the **Certificates snap-in** dialog, select **Computer Account** and click **Next**, as shown next.

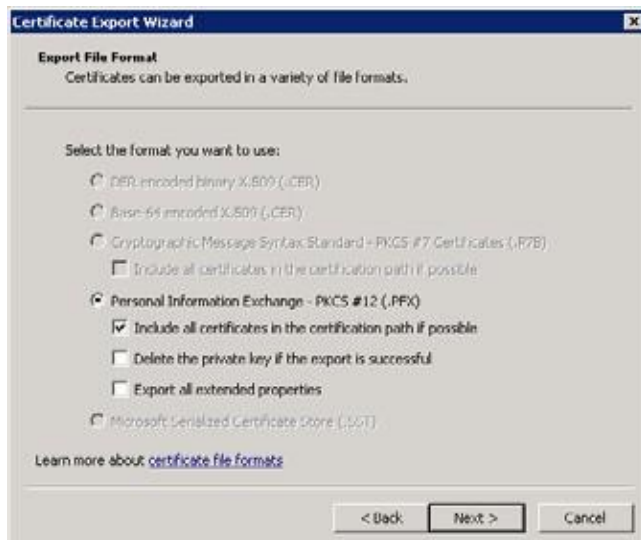


- d On the Select Computer page, select **Local Computer** and click **Finish**.



- 2 Click **OK**.
- 3 Browse to **Certificates (Local Computer) > Personal > Certificates**.
- 4 Right-click the created certificate and select **All Tasks > Export** to view the Certificate Export wizard.
- 5 In the Certificate Export wizard, do the following:
 - a In the **Export Private Key** panel, select **Yes, export the private key**.
 - b Click **Next**.

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



- d Click **Next**.
- e In the **Password** panel, enter a password. This password cannot include special characters or numbers.
- f Click **Next**.
- 6 In the **File to Export** panel, enter a path where you want to save the new file, for example, `c:\temp\rmxcert.pfx`.

Install the Certificate on your RealPresence Collaboration Server (RMX) solution

To install the Certificate on Your RealPresence Collaboration Server (RMX) System

- » After the `.pfx` file is on your computer, you can upload it to the Polycom RealPresence Collaboration Server (RMX) solution and install it, using the procedures in the Polycom RealPresence Collaboration Server (RMX) solution documentation.

Configure Encryption

The Microsoft Lync Server requires encryption by default. Polycom recommends that you enable a minimum settings of 'Support Encryption'.



Note: Integration with Skype for Business requires media encryption

You must enable encrypted media when integrating RealPresence Platform with Skype for Business Server.

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

To change the Lync Server encryption setting:

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

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

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

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

- 3 Verify your encryption settings:

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

Configure Lync Server for use with a Polycom RealPresence Collaboration Server (RMX) System

The Polycom RealPresence RealPresence Collaboration Server 1800/2000/4000/VE systems can host multiple video endpoints in a single conference and host multiple conferences simultaneously. To accommodate these features, you must configure your RealPresence Collaboration Server (RMX) solution as a trusted application and not as a single user in Lync Server 2013.

Polycom recommends using Lync PowerShell commands to perform the following tasks. For detailed documentation on using Lync PowerShell, see [Microsoft Lync Server Management Shell](#).



Note: Using domain names

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

Complete the following tasks to set the Lync routing for the Polycom RealPresence Collaboration Server (RMX) solution:

- [Task 1: Use Lync Topology Builder to Define Your Trusted Application Pool](#)

- [Task 2: Use Lync PowerShell to Create the Trusted Application](#)
- [Task 3: Use Lync PowerShell to Update the Topology](#)
- [\(Optional\) Task 4: Use Lync PowerShell to Define a Static Route for the Polycom RealPresence Collaboration Server \(RMX\) System](#)

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

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

To define your trusted application pool:

- 1 Navigate to **Start > All Programs > Microsoft Lync Server 2013 > Lync Server Topology Builder** to open the Lync Server Topology Builder.
- 2 When prompted, save a copy of the topology.
- 3 Expand the appropriate site container, right-click the **Trusted Application Servers** folder, and select **New Trusted Application Pool**.
- 4 In the **Define the Trusted Application Pool FQDN**, enter the name of the FQDN of the application pool you want to create, for example, `video.sipdomain.com`.
As a best practice, Polycom recommends configuring this pool to be a multiple computer pool. See [Use Multiple Computer Application Pools](#) for more information.
- 5 Click **Next** to add computers to this pool.
- 6 In **Define the computers in this pool**, enter the FQDN for the RealPresence Collaboration Server (RMX) SIP signaling domain and click **Add**.
- 7 When finished adding computers, click **Next**.
- 8 Select the appropriate next hop pool and click **Finish**.
- 9 Select **Action > Topology > Publish** to verify and publish your topology changes.

Task 2: Use Lync PowerShell to Create the Trusted Application

This step creates the trusted application using the Lync PowerShell.

To create the trusted application:

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

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

The parameters are defined as follows:

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

-trustedApplicationPoolFQDN The FQDN of the application pool, in this example, `video.sipdomain.com`.

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

For more information about the `New-CsTrustedApplication` command see Microsoft Lync [New-CsTrustedApplication](#).

- 3 Use the `New-CsTrustedApplicationEndpoint` command to set up a trusted application endpoint for the RealPresence Collaboration Server (RMX) solution.

```
New-CsTrustedApplicationEndpoint -SipAddress sip:video@sipdomain.com -
ApplicationId video -TrustedApplicationPoolFqdn video.sipdomain.com
```

The parameters are defined as follows:

-SipAddress An internal SIP address used by RealPresence Collaboration Server (RMX) for ICE.

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

For more information about the `New-CsTrustedApplicationEndpoint` command see Microsoft Lync [New-CsTrustedApplication](#).



Settings: Creating the trusted application

When creating your trusted application:

- Add all RealPresence Platform Trusted Servers within the same Trusted Application Pool
- Ensure that the Trusted Application Pool FQDN and Trusted Application Endpoint URI share the same name
- Ensure that the Trusted Application '-applicationId' uses the same suffix, shown as 'video' is the example in step 2

Task 3: Use Lync PowerShell to Update the Topology

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

To update the topology:

- 1 Navigate to **Start > All Programs > Microsoft Lync Server2013 > Lync Server Management Shell** to open the Lync PowerShell terminal.
- 2 Use the `Enable-CsTopology` command to update the Lync topology.
`Enable-CsTopology`

(Optional) Task 4: Use Lync PowerShell to Define a Static Route for the Polycom RealPresence Collaboration Server (RMX) System

This step explains how to define a static route for your Polycom RealPresence Collaboration Server (RMX) solution using Lync PowerShell. Route changes you make take effect immediately.

To define a static route:

- 1 Navigate to **Start > All Programs > Microsoft Lync Server2013> Lync Server Management Shell** to open the Lync PowerShell terminal.

- 2 Use the `New-CsStaticRoute` command to set up a static route for the RealPresence Collaboration Server (RMX) solution.

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

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

For more information about the `New-CsStaticRoute` command see Microsoft Lync [New-CsStaticRoute](#).

- 3 Set the routing configuration. By configuring the static route, matched URI dialing is enabled.

The following example sets the route to be global:

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

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

```
Get-CsStaticRoutingConfiguration.
```

Static routes are not required for presence-enabled VMRs or for Polycom RealConnect-enabled conferences.

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



Note: Creating VMRs

You must create a static route within Lync for Collaboration Server (RMX) or RealPresence DMA only for RealPresence Platform VMRs without RealPresence DMA presence and/or Polycom RealConnect technology.

Polycom recommends creating VMRs on RealPresence DMA system to leverage additional high-availability capabilities, such as clustering, and to scale up to 25,000 presence-enabled VMRs. Polycom does not recommend creating presence-enabled VMRs on RealPresence Collaboration Server (RMX).

Enable Microsoft Presence for Lync Server 2013

If you are using a RealPresence Collaboration Server (RMX) system to enable presence in Lync clients, you must manually create and register each meeting room, entry queue, and SIP factory with Lync Server.



Note: RealPresence DMA automatically creates VMR for Polycom RealConnect

You do not need to manually enable presence for each meeting room for Polycom RealConnect. The RealPresence DMA system automatically creates the VMR and does not require presence.

For this reason, Polycom recommends that you enable presence using DMA VMRs as DMA registers VMRs automatically. You can configure RealPresence DMA system version 6.1 or higher to create a corresponding Polycom conference contact in Active Directory whenever users create a new VMR. You can configure up to 25,000 presence-enabled VMRs on RealPresence DMA systems, and Lync clients display a status of Available, Busy, or Offline for the conference contact in the client's contact list. Note that you can configure Microsoft Presence on RealPresence DMA system only with Lync Server 2013. If you are deploying both RealPresence Collaboration Server (RMX) and RealPresence DMA system, Polycom recommends following the steps in [Enable RealPresence DMA Systems for Presence Publishing](#).

If you do not want to delegate remote PowerShell access to RealPresence DMA system, you can also manually create accounts and assign the accounts to a RealPresence DMA system for VMR Presence.

Enable Edge Server Integration with Polycom RealPresence Collaboration Server (RMX) System

Before enabling Edge Server integration with your RealPresence Collaboration Server (RMX) solution, you must configure the RealPresence Collaboration Server (RMX) SIP signaling domain as a trusted application.

When your RealPresence Collaboration Server (RMX) solution is configured with a Microsoft Edge Server, the following Microsoft features are available for your RealPresence Collaboration Server (RMX) solution:

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

**Note: Federation and CAC require Lync Server or Edge Server support**

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

Required Ports

This section lists RealPresence Collaboration Server (RMX) firewall port requirements when deployed with Lync Server. Signaling is as follows:

- **Call Signaling** External Lync participant <> Firewall <> Lync Edge <> Lync Front-end <> DMA <> RMX Signalling IP <> DMA <> Lync Front-end <> Lync Edge <> Firewall <> External Lync Participant.
- **Media** External Lync participant <> Firewall <> Lync Edge <> RMX Media IP <> Lync Edge <> Firewall <> External Lync Participant.

The following table lists port requirements for Lync to Collaboration Server (RMX).

Microsoft Required Ports

Connection type	Collaboration Server (RMX) Ports	Lync Server	Lync Ports	Protocol	Use
ICE	49152 – 65535; 20000 – 35000	Lync Edge Server Internal network interface controller (NIC)	3478	STUN/TURN over UDP	ICE
ICE	49152 – 65535; 20000 – 35000	Lync Edge Server Internal network interface controller (NIC)	443	STUN/TURN Over TCP	ICE

Set Up a Microsoft Edge Server for the Polycom RealPresence Collaboration Server (RMX) System

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

- Enable the firewall for UDP.
- Provide the RealPresence Collaboration Server (RMX) solution with a unique account when you create the Trusted Application Endpoint and register it with Edge Server.
- Set up a TLS connection.

- Ensure that the RealPresence Collaboration Server (RMX) solution SIP signaling domain has been allowed on the Edge Server you are federating to (if your deployment does not include a RealPresence DMA system).

To set up a Microsoft Edge Server with the Polycom RealPresence Collaboration Server (RMX) solution and support Microsoft CAC policies, complete the following tasks:

- [Task 1: Obtain the Trusted Application Service GRUU Identification](#)
- [Task 2: Configure RealPresence Collaboration Server \(RMX\) System Flags](#)
- [Task 3: Configure the RealPresence Collaboration Server \(RMX\) System for Edge Server Support](#)
- [Task 4: Monitor the Connection to the Session Traversal Utilities for NAT \(STUN\) and Relay Servers in the ICE Environment](#)

Task 1: Obtain the Trusted Application Service GRUU Identification

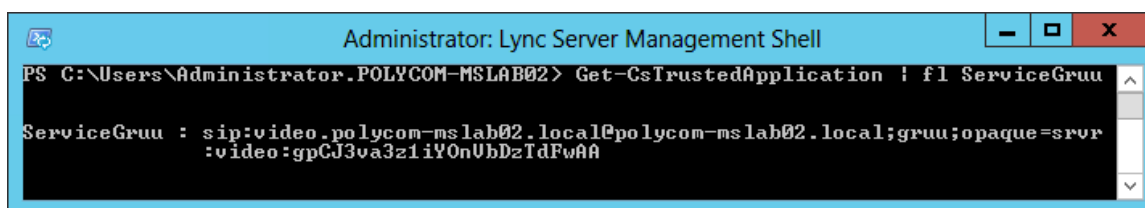
This task shows you how to use Lync PowerShell to obtain the service GRUU for your Polycom RealPresence Collaboration Server (RMX) solution.

If you are deploying multiple RealPresence Collaboration Servers, the Globally Routable User Agent URI (GRUU) information can be shared as long as the existing Trusted Application Pool and Application ID are used.

To obtain the service GRUU identification:

- 1 Navigate to **Start > All Programs > Microsoft Lync Server2013 > Lync Server Management Shell** to open the Lync PowerShell terminal.
- 2 Use the `Get-CsTrustedApplication` command to display the service GRUU information for the RealPresence Collaboration Server (RMX) solution, and make note of the information.

```
Get-CsTrustedApplication | fl ServiceGruu
```



```
Administrator: Lync Server Management Shell
PS C:\Users\Administrator\POLYCOM-MSLAB02> Get-CsTrustedApplication | fl ServiceGruu

ServiceGruu : sip:video.polycom-mslab02.local@polycom-mslab02.local;gruu;opaque=srvr
              :video:gpGJ3va3z1iY0nUbDzIdFwAA
```



Note: You must enable Interactive Connectivity Establishment (ICE)

Prior to this release, creating an account in Active Directory was necessary only for Lync deployments with an Edge Server deployed to facilitate federated or remote worker calling. As of this release, you must enable ICE with or without Edge Server deployments.

Task 2: Configure RealPresence Collaboration Server (RMX) System Flags

This section shows you how to configure system flags for the RealPresence Collaboration Server (RMX).

To configure system flags:

- 1 Enable the following system flags on the RealPresence Collaboration Server (RMX) solution:
`MS_ENVIRONMENT=YES`
- 2 Create a new flag named:
`SIP_CONTACT_OVERRIDE_STR`
- 3 Configure the service GRUU information obtained in Task 1 without the prefix *sip*:. For example, use:
`video.polycom-mslab02.local@polycom-mslab02.local;gruu;opaque=svr:video:gpCJ3va3z1iYOnVbDzTdFwAA`

For more information about configuring RealPresence Collaboration Server (RMX) solution flags, see the *Polycom RealPresence Collaboration Server (RMX) Administrator Guide* for your model at [Collaboration & Conferencing Platforms](#) on Polycom Support.

Task 3: Configure the RealPresence Collaboration Server (RMX) System for Edge Server Support

This section shows you how to configure the RealPresence Collaboration Server (RMX) for Lync Edge Server.

To configure the RealPresence Collaboration Server (RMX) for Edge Server support:

- 1 In the **RealPresence Collaboration Server (RMX)** web browser, in the **RealPresence Collaboration Server Management** pane, expand the **Rarely Used** list and click **IP Network Services**.
- 2 In the **IP Network Services** pane, double-click the **Default IP Network Service** entry.
The Default IP Service - Networking IP dialog opens.
- 3 Click the **SIP Advanced** tab.

- 4 In the **Server User Name** field, enter the SIP URI that you defined for the TrustedApplicationEndpoint, for example, `video`, as shown next.



- 5 In the **ICE Environment** field, select **MS** for Microsoft ICE implementation.
- 6 Click **OK**.

Task 4: Monitor the Connection to the Session Traversal Utilities for NAT (STUN) and Relay Servers in the ICE Environment

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

To monitor the ICE connection:

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

The system lists the ICE servers it is connected to, the connection status, and the status of the firewall detection in the RealPresence Collaboration Server (RMX) solution.

Configure RealPresence Collaboration Server (RMX) for Polycom ContentConnect Software

RealPresence Collaboration Server (RMX) version 8.5 is the minimum version required to use Gateway Mode.

Configuring RealPresence Collaboration Server (RMX) for Polycom ContentConnect software enables the following:

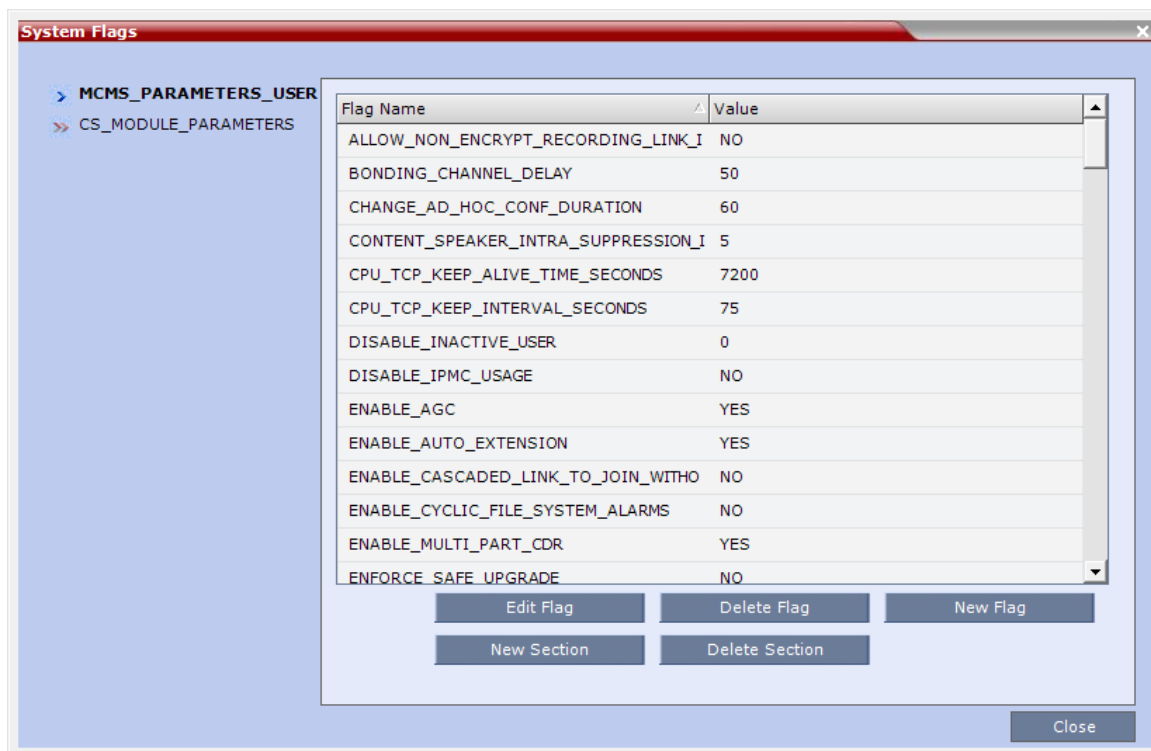
- Enables RealPresence Collaboration Server (RMX) to send content to legacy endpoints.

- Enables endpoints from outside the company firewall to share content with endpoints within the firewall.

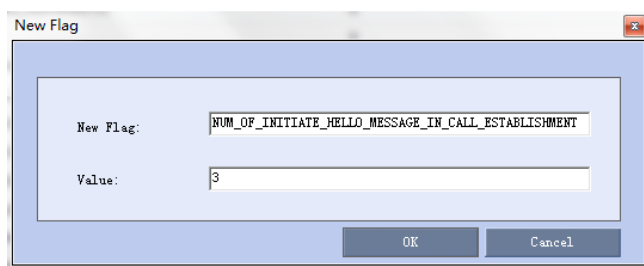
Complete the following three procedures to configure RealPresence Collaboration Server (RMX) for Polycom ContentConnect software.

To configure RMX to so that endpoints from outside the company firewall can share content (optional; complete only if endpoints traverse the firewall):

- 1 On the RealPresence Collaboration Server (RMX) menu, click **Setup > System Configuration**.
- 2 From the **System Flags** dialog box (shown next), click **New Flag**.



- 3 In the **New Flag** box (shown next), enter NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT.
 - a In the **Value** field, enter either 3 or 5.
 - b Click **OK**.



Deploy Polycom RealPresence DMA Systems

When you incorporate Polycom DMA RealPresence systems in a Microsoft Lync environment, you can do the following:

- Use the Polycom RealPresence DMA system to manage conferences on your Polycom RealPresence Collaboration Server (RMX) solutions.
- Route outgoing calls from Lync Server to Virtual Meeting Rooms (VMRs) provisioned on the RealPresence DMA system. This applies to manually created VMRs or automatically created VMRs using Active Directory Integration.
- Publish Lync Presence for Virtual Meeting Rooms.
- Integrate with Lync 2013 Online Meetings using Polycom RealConnect technology.
- You can use the RealPresence DMA system for calls between endpoints registered to a DMA system and a Lync Server that is SIP peered. Video is supported for calls with Lync 2010 clients; Lync 2013 clients supports audio-only calls.

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

- [Configure Lync Server for use with a RealPresence DMA System](#)
- [Configure Your RealPresence DMA System for Lync Server](#)

Configure Lync Server for Use with a RealPresence DMA System

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

- [Set the Routing for the RealPresence DMA System](#)
- [Enable Federation in your Lync Environment](#)

Set the Routing for the RealPresence DMA System

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

Complete the following two tasks to set the Lync routing for the RealPresence DMA system:

- [Task 1: Use Lync Topology Builder to Define Your Trusted Application Pool](#)
- [\(Optional\) Task 2: Use Lync PowerShell to Define a Static Route for the RealPresence DMA System](#)

**Note: Creating static routes in Skype for Business**

For instructions on creating a MatchURI and provisioning a certificate in Skype for Business, refer to [Appendix E: Configuring Static Routes in Skype for Business](#).

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

Before completing this RealPresence DMA task, you must integrate RealPresence Collaboration Server (RMX) with Lync by creating your Trusted Application Pool and Trusted Application Endpoint commands as shown in the section [Task 2: Use Lync PowerShell to Create the Trusted Application](#).

To define your trusted application pool:

- 1 Add RealPresence DMA system to your Trusted Application Pool and enter the FQDN for the DMA virtual host, for example, `dma.corp.local`. If you have a superclustered configuration, complete this for each RealPresence DMA system within the cluster that you want to integrate with Lync.
- 2 Select the appropriate next hop pool and click **Finish**.
- 3 Select **Action > Topology > Publish** to verify and publish your topology changes.
- 4 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 **Missing Machine** warning, shown next.



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

(Optional) Task 2: Use Lync PowerShell to Define a Static Route for the RealPresence DMA system

Set the RealPresence DMA system as a trusted host with a static route.

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

- 1 Navigate to **Start > All Programs > Microsoft Lync Server2013 > Lync Server Management Shell** to open the Lync PowerShell terminal.

- 2 Use the `New-CsStaticRoute` command to set up a static route for the RealPresence DMA system.

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

where `dma.corp.local` is the FQDN of the DMA virtual host and `sipdomain.com` is the SIP routing domain (matched URI). For information about choosing a MatchURI, refer to the section [MatchURI Dialing](#).

In a superclustered configuration, run this command for each cluster in the supercluster, replacing `dma.corp.local` with the FQDN of the cluster and `sipdomain.com` with the routing name of each cluster. You need to create an alternate MatchURI domain for each RealPresence DMA cluster within the supercluster.

For more information about the `New-CsStaticRoute` command see [Microsoft New-CsStaticRoute](#).

- 3 Set the routing configuration. By configuring the static route, matched URI dialing is enabled.

The following example sets the route to be global:

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

- 4 (Optional) To check that the commands were entered correctly in the PowerShell, enter:

```
Get-CsStaticRoutingConfiguration.
```

Static routes are not required for presence-enabled VMRs or for Polycom RealConnect-enabled conferences.



Note: Enable VMRs via presence publishing in a RealPresence DMA supercluster

Polycom recommends enabling VMRs via presence publishing when integrating a RealPresence DMA supercluster with Lync. This provides high-availability without the need to map distinct MatchURIs to specific DMA hosts.

Enable Federation in your Lync Environment

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

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

- [Task 1: Configure the Microsoft Lync Edge Server](#)
- [Task 2: Ensure the Primary SIP Signaling Domain is Allowed](#)

Task 1: Configure the Microsoft Lync Edge Server

To include Lync Server 2013 or Edge Server in your environment, see Microsoft's detailed instructions [Deploying External User Access in Lync Server 2013](#).

Note that Microsoft provides a [Microsoft Lync Server 2013 Planning Tool](#) you can use to plan your topology.

Microsoft Lync Edge Server Requirements

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

Task 2: Ensure the Primary SIP Signaling Domain is Allowed

When federating with another Lync Server environment, ensure that the domain in the MatchURI is allowed on the federated Lync Edge Server.

If you did not use the primary SIP domain as the MatchURI, you must add both the primary SIP domain and any RealPresence DMA system and RealPresence Collaboration Server (RMX) SIP signaling domains to the allowed domain list on the federated Lync Edge Server.

Example Primary SIP Domain Scenarios

- Primary SIP domain was used as the MatchURI when configuring the RealPresence Collaboration Server (RMX)/RealPresence DMA system static route.
 - If companyB wants to connect to calls managed by a RealPresence DMA system or RealPresence Collaboration Server (RMX) solution on companyA, companyB must add the following domain to its list of allowed SIP domains in the Lync Edge Server.
 - ♦ companyA's primary SIP domain
 - If companyA wants to connect to calls managed by a RealPresence DMA system or RealPresence Collaboration Server (RMX) solution on companyB, companyA must add the following domain to its list of allowed SIP domains on companyA's Edge Server.
 - ♦ companyB's primary SIP domain
- A domain other than the primary SIP domain was used as the MatchURI when configuring the RealPresence Collaboration Server (RMX)/RealPresence DMA system static route.
 - If companyB wants to connect to calls managed by a RealPresence DMA system or RealPresence Collaboration Server (RMX) solution on companyA, companyB must add the following domains to its list of allowed SIP domains in the Lync Edge Server.
 - ♦ companyA's primary SIP domain
 - ♦ Each RealPresence Collaboration Server (RMX)/RealPresence DMA system SIP signaling domain
 - If companyA wants to connect to calls managed by a RealPresence DMA system or RealPresence Collaboration Server (RMX) solution 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 RealPresence Collaboration Server (RMX)/RealPresence DMA system SIP signaling domain

You have successfully configured Lync Server for use with a RealPresence DMA system. The second section of this section shows you how to configure your RealPresence DMA system for Lync Server.

Configure RealPresence DMA System for Lync Server

This section outlines the following five steps that configure a RealPresence DMA system with Lync Server:

- [Ensure DNS is Configured Properly](#)
- [Create a Security Certificate for the RealPresence DMA 7000 System](#)
- [\(Optional\) Configure a RealPresence DMA System SIP Peer for Lync Server](#)
- [Enable RealPresence DMA System for Lync 2013 and Polycom RealConnect](#)
- [Enable RealPresence DMA System for Presence Publishing](#)

Ensure DNS is Configured Properly

To configure DNS properly, ensure that:

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

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

Create a Security Certificate for the RealPresence DMA 7000 System

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

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

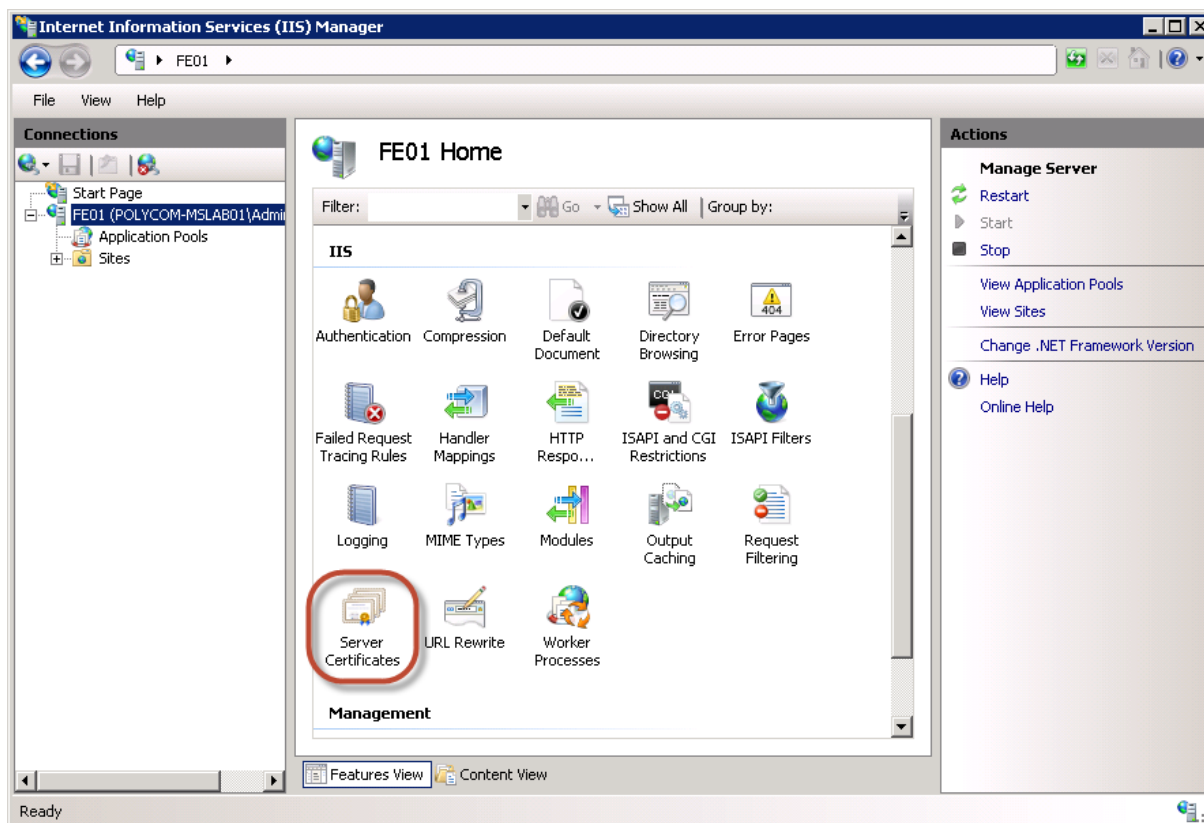
- If your organization requires that all certificates be generated externally, then follow those procedures to generate the certificates and install them on your system using the procedures outlined in *Polycom RealPresence Collaboration Server (RMX) Administrator Guide* for your model at [Collaboration & Conferencing Platforms](#) on Polycom Support.

**Note: Creating static routes in Skype for Business**

For instructions on creating a MatchURI and provisioning a certificate in Skype for Business, refer to [Appendix E: Configuring Static Routes in Skype for Business](#).

To create a security certificate for the RealPresence DMA system using IIS Manager 7:

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



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



The **Create Certificate** wizard displays.

- 5 In the **Distinguished Name Properties** panel, shown next, complete all fields. Do not leave any fields blank.
 - In the **Common Name** field, enter the FQDN of the RealPresence DMA virtual host name. This name must match what is in the DNS.

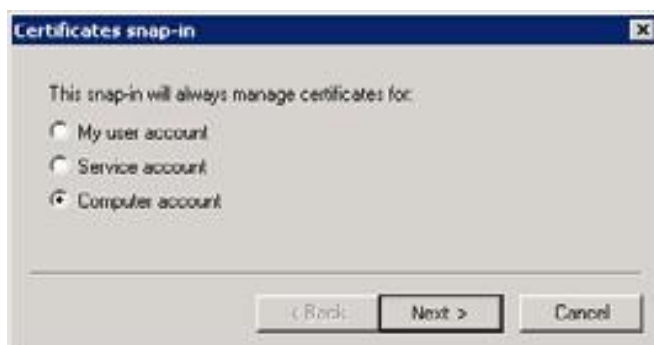
A screenshot of a 'Create Certificate' wizard window. The window has a title bar with a question mark and a close button. Below the title bar is a header area with a certificate icon and the text 'Distinguished Name Properties'. The main area contains a text box with the instruction: 'Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.' Below this are several input fields: 'Common name:' with the value 'dma.corp.local', 'Organization:' with the value 'Video Infrastructure', 'Organizational unit:' with the value 'IT', 'City/locality' with the value 'London', 'State/province:' with the value 'London', and 'Country/region:' with a dropdown menu showing 'UK'. At the bottom of the window are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

- 6 Click **Next**.
- 7 In the **Online Certification Authority** panel, select a Certificate authority from the list and enter a name that you can easily identify, for example, RealPresence DMA certificate.
- 8 Click **Finish**.

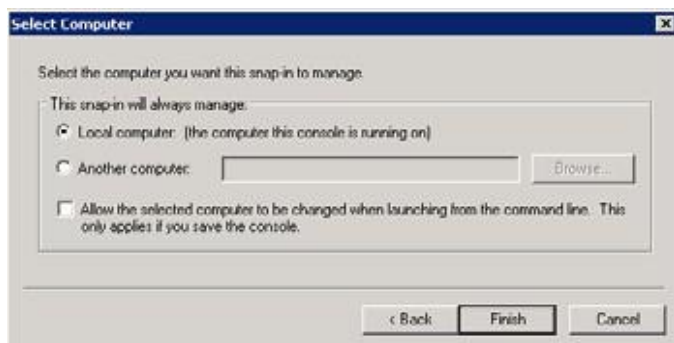
You have created the certificate.

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

- 1 Open **Microsoft Management Console**. Add the **Certificates snap-in** if it has not been added already.
 - a Choose **File > Add/Remove Snap-in**.
 - b Select **Certificates** from the **Available Snap-ins** area and click **Add**.
 - c On the **Certificates snap-in** dialog, select **Computer Account** and click **Next**.

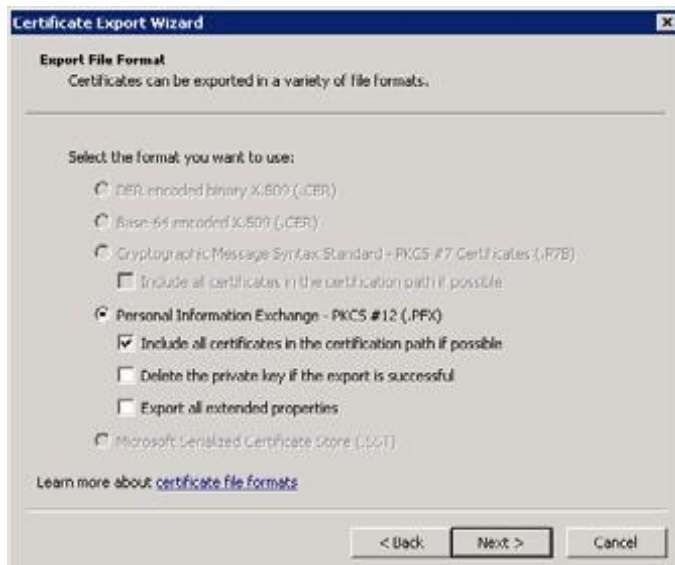


- d On the **Select Computer** dialog, select **Local Computer**.



- e Click **Finish**.
- 2 Click **OK**.
- 3 Browse to **Certificates (Local Computer) > Personal > Certificates**.
- 4 Right-click the created certificate and select **All Tasks > Export** to view the Certificate Export wizard.
- 5 In the **Certificate Export** wizard, do the following:
 - a In the **Export Private Key** panel, select **Yes, export the private key**.
 - b Click **Next**.

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



- d Click **Next**.
- e In the **Password** panel, enter a simple password.
- f Click **Next**.
- 6 In the **File to Export** panel, enter a path where you want to save the new file, for example, `c:\temp\dmacert.pfx`.
- 7 Once the `.pfx` file is on your computer, you can upload it to the RealPresence DMA system and install it, using the procedures in the RealPresence DMA system's online help for Certificate Management.

Enable RealPresence DMA System for Lync 2013 and Polycom RealConnect

Polycom RealPresence Collaboration Server (RMX) solution and RealPresence DMA system introduce Polycom RealConnect technology for Lync 2013, a new RealPresence platform function for Lync 2013 customers. Polycom RealConnect technology enables you to dial into scheduled Lync 2013 conferences using H.323 or standard SIP. Because all of the call control and media translation is handled by the RealPresence Collaboration Server (RMX) solution and RealPresence DMA system, any standards-based H.323 or SIP endpoint can use Polycom RealConnect technology even if the endpoint does not support Lync.

The figure [Lync Invitation with Conference ID](#) show a Lync invitation populated with a Conference ID, which is provided automatically by Lync Server and represents the H.323 number or SIP URI you dial on the endpoint.

For example:

17894

17894@dmadomain.net

**Note: Configure Microsoft dial-in conferencing**

Conference IDs are generated only when you deploy Lync Dial-in Conferencing and are typically enabled when PSTN dial-in conferencing capabilities are also enabled. However, you can use a dummy dial-in access number. For full Lync 2013 dial-in conference deployment steps, refer to Microsoft's [Configuring Dial-in Conferencing](#).

Lync invitation with conference ID

Start time	<input type="text" value="Tue 4/15/2014"/>	<input type="text" value="5:00 PM"/>
End time	<input type="text" value="Tue 4/15/2014"/>	<input type="text" value="5:30 PM"/>

→ [Join Lync Meeting](#)

Join by phone

[VMR-Number](#) (London, UK)

English (United Kingdom)

[Find a local number](#)

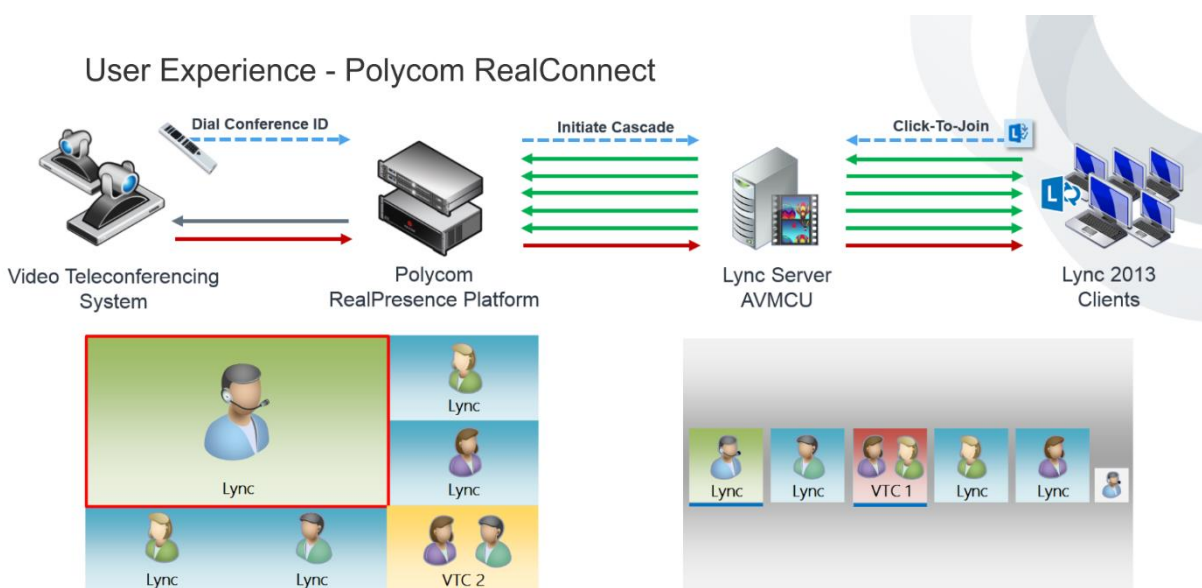
Conference ID: 17894

[Forgot your dial-in PIN?](#) | [Help](#) | [Legal](#)



Polycom RealConnect technology with Lync 2013 provides Lync clients with Microsoft's familiar Gallery View and standards-based video endpoints a Continuous Presence experience on the RealPresence Collaboration Server (RMX). Conferences on RealPresence Collaboration Server (RMX) are bridged or use Polycom RealConnect technology automatically, and up to five of the active Lync 2013 participants display as individual participants on the RealPresence Collaboration Server (RMX) layout. In addition, all participants are joined in a single virtual meeting room which displays video from participants using a standards-based endpoint. This conference scenario is illustrated next.

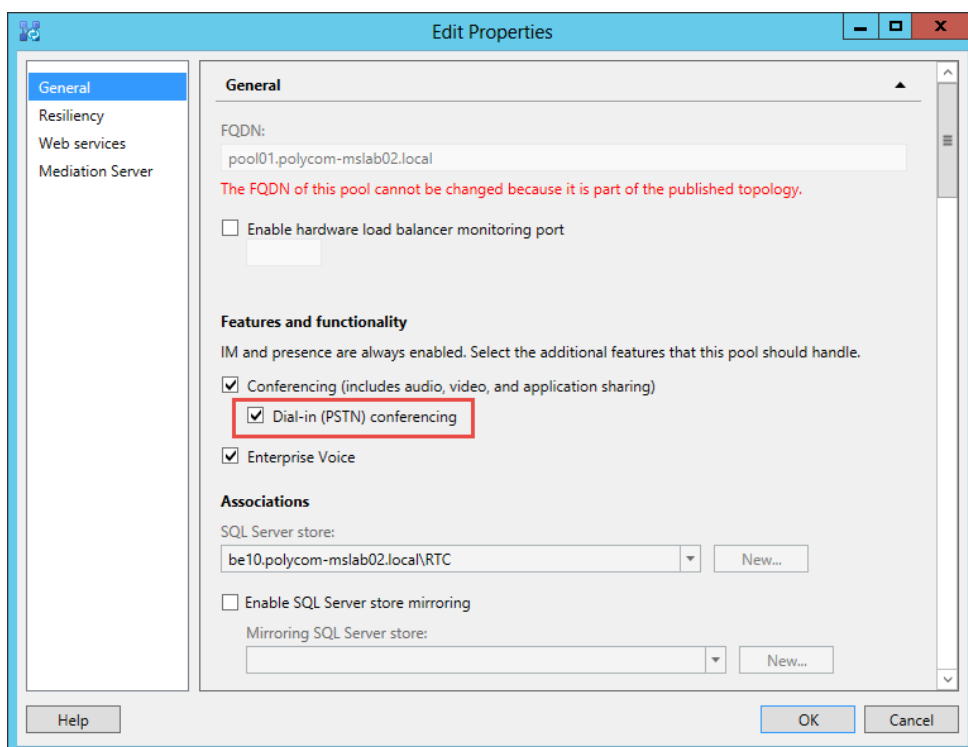
Polycom RealConnect conference scenario



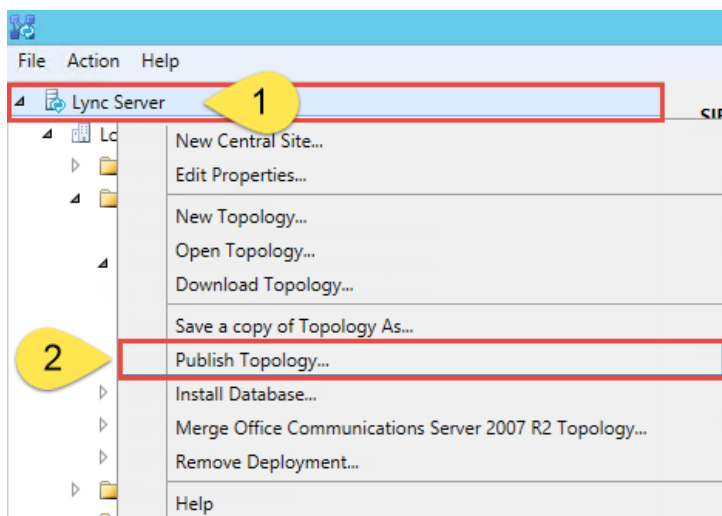
The following procedure provides the key steps that enable Dial-in Conferencing on Lync Server 2013. If you require more details, refer to [Configuring Dial-in Conferencing](#) on Microsoft TechNet.

To enable Dial-in Conferencing:

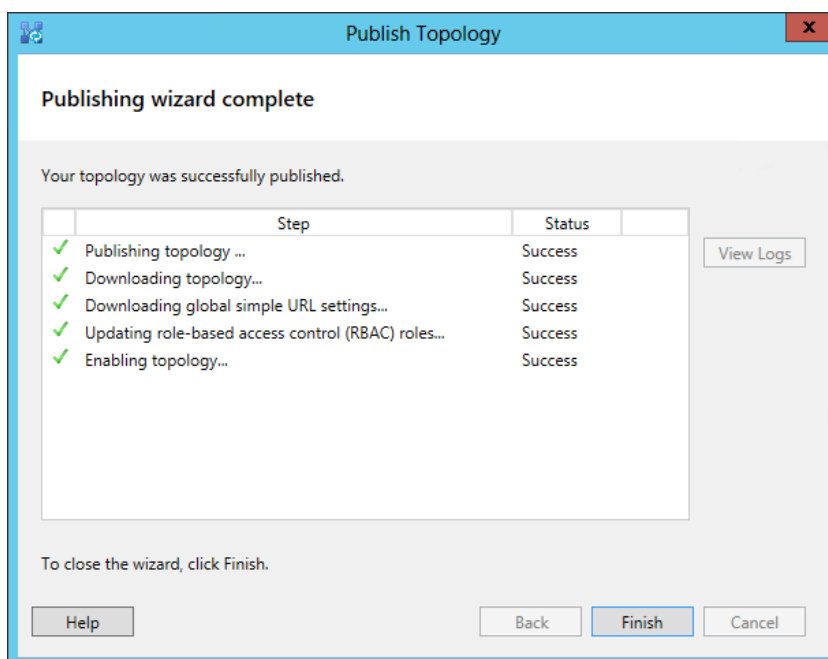
- 1 Install the dial-in (PSTN) conferencing component for the Lync front end server or pool in the Lync 2013 topology builder by going to **Edit Properties > General > Features and Functionality**.
- 2 Check **Dial-in (PSTN) conferencing** and click **OK**.



- 3 Publish the topology by right-clicking the central site name and clicking **Publish Topology > Next > Finish**.



After publication, the output displays, as shown next.



After you change the topology, deploy the application on the Lync Server by running the Lync 2013 bootstrapper process.

To deploy the application:

- 1 Open the command prompt on your Lync front end server and execute the command:
`%ProgramFiles%\Microsoft Lync Server 2013\Deployment\Bootstrapper.exe`

```

Administrator: Command Prompt

Checking prerequisite MSSpeech_SR_nb-NO_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_nl-NL_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_pl-PL_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_pt-BR_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_pt-PT_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_ru-RU_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_sv-SE_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_zh-CN_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_zh-HK_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_zh-TW_TELE...prerequisite satisfied.
Checking prerequisite UcmWorkflowRuntime...prerequisite satisfied.
Installing any collocated databases...
Executing PowerShell command: Install-CSDatabase -Confirm:$false -Verbose -Local
Databases -Report "C:\Users\Administrator.POLYCOM-MSLAB02\AppData\Local\Temp\2\I
nstall-CSDatabase-[2014_05_06]f10_34_031.html"
Enabling new roles...
This step will configure services, apply permissions, create firewall rules, etc
Executing PowerShell command: Enable-CSComputer -Confirm:$false -Verbose -Report
"C:\Users\Administrator.POLYCOM-MSLAB02\AppData\Local\Temp\2\Enable-CSComputer-
[2014_05_06]f10_34_221.html"
Complete.
Log file was: %TEMP%\Bootstrap-CsMachine-[2014_05_06]f10_33_261.html
C:\Users\Administrator.POLYCOM-MSLAB02>

```

- 2 Install the associated service by opening the Lync Server Management Shell and executing `Start-CSWindowsService`.

Next, ensure that a dial-in conferencing region is configured. Typically, you will need to configure multiple regions and assign local access numbers. In the following example, we add a default region in order to generate an H.323 or standard SIP number that users can dial into from any standards-based room system. The naming convention is not important but you must populate the dial-in conferencing region to complete the configuration.

To populate the dial-in conferencing region:

- 1 Open the **Lync 2013 Server Control Panel** and go to **Voice Routing > Edit the Global Dial Plan > Dial-in conferencing region**.

- 2 Specify a dial-in access number by going to **Lync 2013 Server Control Panel > Conferencing > Dial-in Access Number > New** and completing the following fields:
 - **Display number** This field permits alphanumeric entry. This is typically the dial-in access number. This example uses the VMR or Conference ID and is labelled here as VMR-Number.
 - **Display name** Choose a display name. Typically, this name matches the region.
 - **Line URI** The line URI will not be used as the actual dial-in conference is not being used. This example uses a dummy number tel+111.

- **SIP URI** This field allocates a SIP address to the conference number. Though this field is not used for Polycom RealConnect, you must enter a SIP URI.
- **Pool** Enter the pool you are enabling for dial-in conferencing.
- **Primary language** This field is not used for Polycom RealConnect.
- **Associated Regions** Add the region you created in step 1.

Commit Cancel

Display number: *

VMR-Number

Display name:

Conference Dial-in (London)

Line URI: *

tel:+111

SIP URI: *

sip:conf-lonuk @ polycom-mslab02.com

Pool: *

pool01.polycom-mslab02.local

Primary language: *

English (United Kingdom)

Secondary languages (maximum of four):

Add... Remove

Associated Regions *

Add... Remove

Region
London, UK

If you want to customize the meeting invitation, you can add custom footer text to allow meeting participants to join a meeting using a standards-based video endpoint.

- 3 In the **Lync 2013 Control Panel**, go to **Conferencing > Meeting Configuration**.
- 4 Edit the default global template as shown next.

Custom footer text:

For traditional video meeting participation dial the Lync conference ID from your endpoint, external participants can also join by appending the ID with video.polycom-mslab02.com.

For SIP 123456@video.polycom.com and for H.323 video.polycom.com##123456

This example shows external addresses. If you want to show external addresses, you need to enable standards-based video Firewall traversal using, for example, a RealPresence Access Director.

Your Lync environment now includes Conference IDs in Lync-enabled meeting invitations.

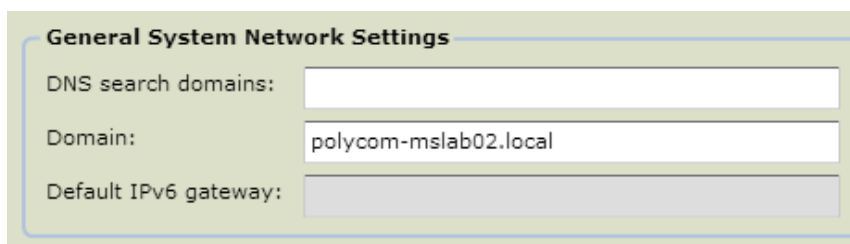
Next, complete the Lync 2013 and RealPresence DMA system integration. The following steps assume that you have created a security certificate, as shown in [Create a Security Certificate for the Polycom DMA 7000 System](#).

Configure RealPresence DMA system network settings to match the Lync Server, specifically, Time and Domain. You need to configure the domain to match the extension you gave to the RealPresence DMA system DNS name.

Next, specify domain and time on the RealPresence DMA system.

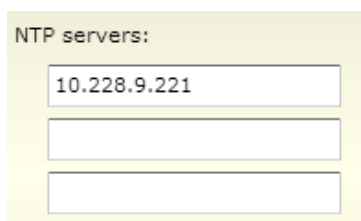
To specify domain and time on the RealPresence DMA system:

- 1 From the **DMA administrator** screen go to **Local Cluster > Network Settings > General System Network Settings**.



The screenshot shows the 'General System Network Settings' window. It contains three input fields: 'DNS search domains' (empty), 'Domain' (containing 'polycom-mslab02.local'), and 'Default IPv6 gateway' (empty).

- 2 Configure the time to synchronize with the same source as the Lync Server, typically one of your domain controllers, by going to **Local Cluster > Time Settings**. Specify an IP address for your time server, as well as a time zone.



The screenshot shows the 'NTP servers' configuration page. It has a label 'NTP servers:' followed by three input fields. The first field contains the IP address '10.228.9.221', while the other two are empty.

Next, if you have not done so yet, add the Lync Server as an external SIP peer. You must complete the additional steps in this section to enable Polycom RealConnect.

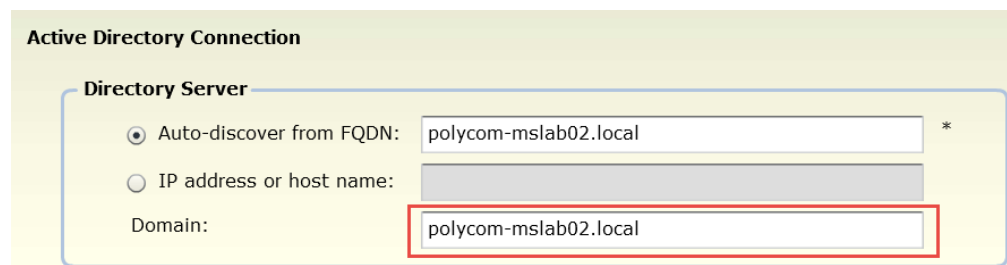
To add the Lync 2013 Server as a SIP Peer:

- 1 In the **DMA administrator** console go to **Network > External SIP Peers > Add**. Complete the following fields:
 - **Name** Enter the name you gave to this Lync Front End Server or Pool.
 - **Description** Enter a description for Name field.
 - **Type** Choose **Microsoft**.
 - **Next hop address** Enter the FQDN for your Lync Front End Server or Pool.

- **Destination network** Enter the SIP domain used for Polycom RealConnect conferences. This is not the domain extension for your Lync Front End Server or your Pool.
- **Port** Enter 5061.
- **Transport type** Enter TLS.

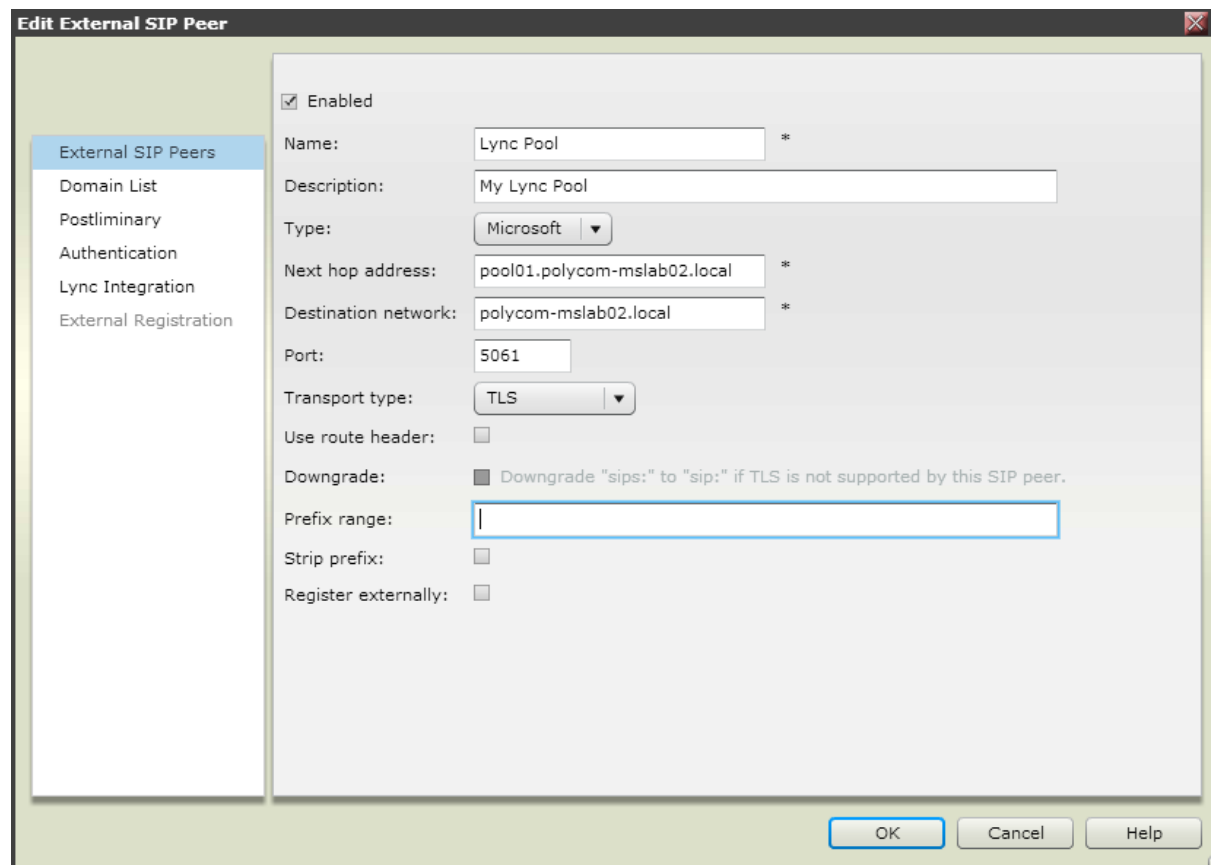
You can leave the remaining fields blank.

As of DMA 6.2, you need to enter the FQDN of your Active Directory domain in the new **Domain** field, as shown next. Complete this field during Active Directory integration.



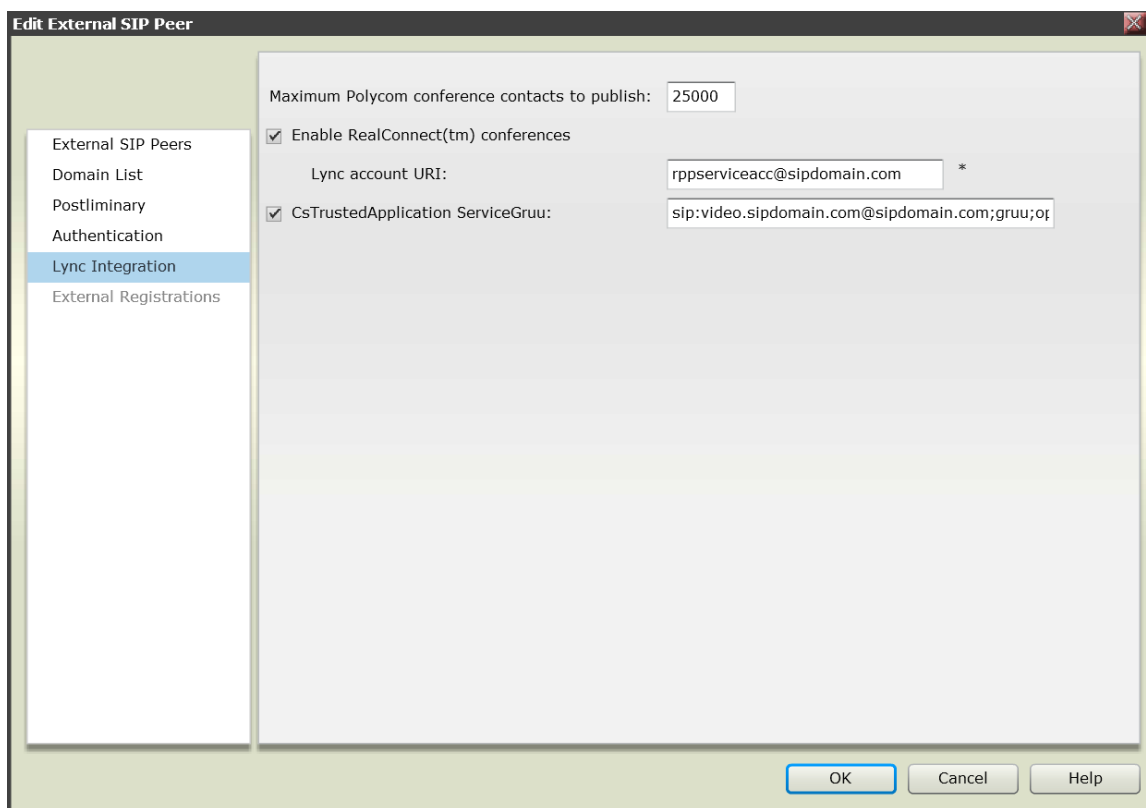
The image shows a dialog box titled "Active Directory Connection". Inside, there is a section labeled "Directory Server" with three options: "Auto-discover from FQDN:", "IP address or host name:", and "Domain:". The "Auto-discover from FQDN:" option is selected. The text "polycom-mslab02.local" is entered in the field next to it. The "Domain:" field also contains "polycom-mslab02.local" and is highlighted with a red rectangle.

Previously, you specified the Active Directory domain in the Destination Network field of Edit External SIP Peer screen, shown next.



The image shows the "Edit External SIP Peer" dialog box. On the left is a sidebar with a tree view containing "External SIP Peers", "Domain List", "Postliminary", "Authentication", "Lync Integration", and "External Registration". The main area has a list of settings: "Enabled" (checked), "Name" (Lync Pool), "Description" (My Lync Pool), "Type" (Microsoft), "Next hop address" (pool01.polycom-mslab02.local), "Destination network" (polycom-mslab02.local), "Port" (5061), "Transport type" (TLS), "Use route header" (unchecked), "Downgrade" (unchecked), "Prefix range" (empty field), "Strip prefix" (unchecked), and "Register externally" (unchecked). The "Prefix range" field is highlighted with a blue rectangle. At the bottom are "OK", "Cancel", and "Help" buttons.

2 In the left window, click **Lync Integration**.



3 In **Maximum Polycom conference contacts to publish**, enter the maximum number of VMRs you are publishing presence for. This field is not required for Polycom RealConnect. This example sets the maximum at 25,000, the recommended number.

4 Check **Enable combined RealPresence-Lync scheduled conferences**.

Next, assign a Lync account. Although this can be an existing account, Polycom recommends creating a dedicated Lync account that can be used to perform Conference ID to Lync Conference SIP URI resolution. In this case, the account can be a Lync account enabled for PC-to-PC telephony, as illustrated next.

Edit Lync Server user – RealPresence Platform service account

Commit Cancel

Display name:
RPP Service Account

☒ Enabled for Lync Server

SIP address: *
sip:rppserviceacc @ polycom-mslab02.com

Registrar pool:
pool01.polycom-mslab02.local

Telephony:
PC-to-PC only

Line URI:
tel:+123456

Configure the RealPresence DMA System Lync Dial Rule

Next, create a conference template that is assigned to Polycom RealConnect Lync conferences.

To create a conference template:

- 1 Set **Conference mode** to **AVC only**. Mixed mode is not supported.
- 2 Enable the dial rule on RealPresence DMA system by going to the **DMA administrator screen > Call Server > Dial Rules**.

The Description field displays *Dial to Polycom RealConnect Conference*.

- 3 Highlight **Dial by Lync conference ID** and select **Edit**.
- 4 Select **Enabled** to enable both the rule and the Conference template created in the previous step.
The available SIP peer(s) you assigned displays in Selected SIP peers.
- 5 Click **OK**.



Note: Define a specific MCU pool order

As of RealPresence DMA system 6.2 you have the option to define a specific MCU pool order.

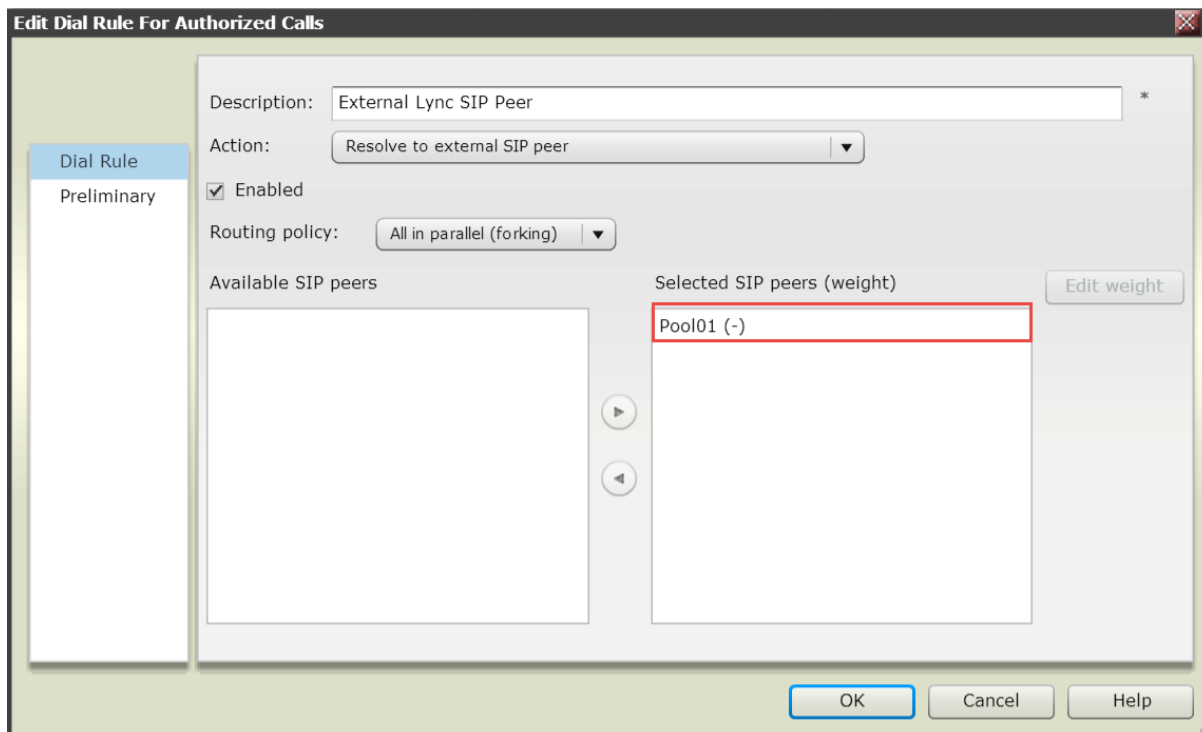
Configure the RealPresence DMA System Polycom ContentConnect Dial Rule

Next, create a dial rule assigned to Polycom RealConnect Lync conferences.

To create a dial rule:

- 1 Create a new dial rule in last position.
- 2 Create the dial rule on RealPresence DMA system by going to **Admin > Call Server > Dial Rules**.
The Add Dial Rule for Authorized Calls dialog displays.

- 3 Select **Resolve to external SIP peer** and enter a description, for example, 'External Lync SIP Peer'.



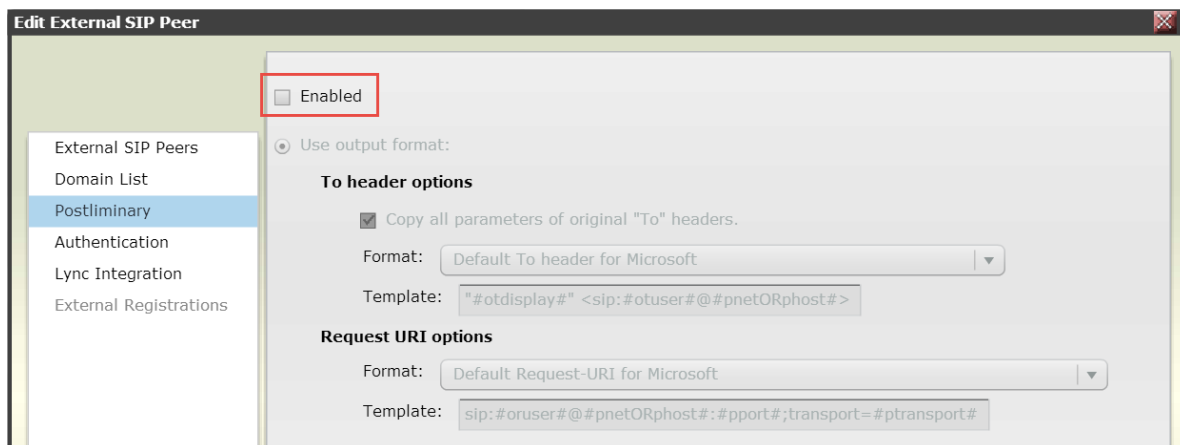
- 4 Add the SIP peer created previously.

- 5 Select **Enabled** to enable dial rule.

The available SIP peer(s) you assigned displays in Selected SIP peers.

- 6 Click **OK**.

Note that for Polycom DMA system v6.3, the postliminary configuration for the SIP peer is not the same as for Polycom DMA system v6.2. As shown in the following illustration, do not enable the postliminary.



Enable RealPresence DMA System for Presence Publishing

As of RealPresence DMA system 6.1, you can publish Lync presence for Virtual Meeting Rooms and automatically manage Active Directory contacts representing VMRs. To use this feature, complete the Microsoft Active Directory integration and configure remote PowerShell access for Active Directory and Lync as shown in the *Polycom RealPresence DMA 7000 System Operations Guide* at [Polycom RealPresence Distributed Media Application \(DMA\)](#). The RealPresence DMA system manages contacts in Active Directory that are enabled for Lync presence by creating, altering, or deleting the contact to match the VMR.

Complete the following procedure only if you want to automatically create Polycom conference contacts (refer the section [To publish presence for VMR contacts](#)). The next procedure shows you how to enable remote PowerShell on the Active Directory Domain Controller(s). You must repeat this procedure for all domain controllers and for each corresponding Lync Front End Server.



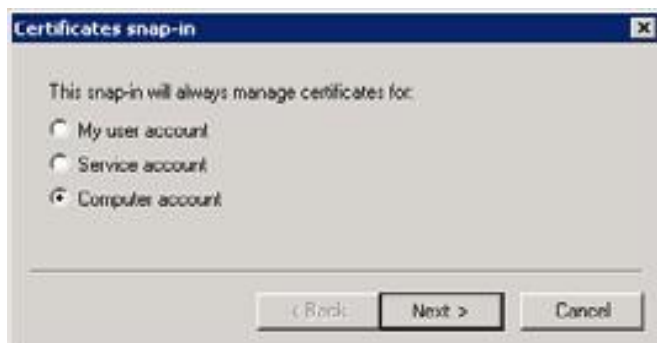
Settings: DMA Active Directory accounts

When using the same Active Directory account for both Active Directory integration and Presence Publishing, you must ensure this account has write access to both Active Directory and Lync.

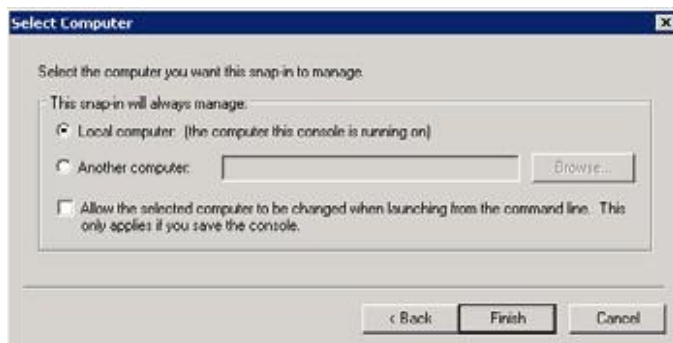
If a Server Authentication certificate is not already present within the personal certificate store on the Domain Controller, you must first enable remote PowerShell to create an SSL certificate, which is required for RealPresence DMA system and all domain controllers. To check whether or not a certificate is already present, see the following procedure.

To check for a server authentication certificate:

- 1 Open the **Microsoft Management Console**.
- 2 Choose **File > Add/Remove Snap-in**.
- 3 Select **Certificates** from the **Available Snap-ins** and click **Add**.
- 4 In the **Certificates snap-in** dialog, select **Computer Account** and click **Next**.



- 5 In the **Select Computer** dialog, select **Local Computer** and click **Finish**.



6 Click **OK**.

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

Console Root	Issued To	Issued By	Expiration Date	Intended Purposes
Certificates (Local Computer)	dc10.polycom-mslab02.local	polycom-mslab02-DC10-CA	10/29/2013	Client Authentication, Server Authentication
Personal	dc10.polycom-mslab02.local	polycom-mslab02-DC10-CA	10/29/2014	Server Authentication

- If a certificate is not available you can purchase and install a certificate from a commercial Trusted Root CA such as VeriSign or Thawte. To create a Certificate Signing Request and to install the certificate(s) you receive from the CA, follow the procedures in the section *Certificate Procedures* in the *Polycom RealPresence DMA 7000 System Operations Guide* at [Polycom RealPresence Distributed Media Application \(DMA\)](#).

If you want to request and obtain a certificate from your enterprise CA, you can do one of the following:

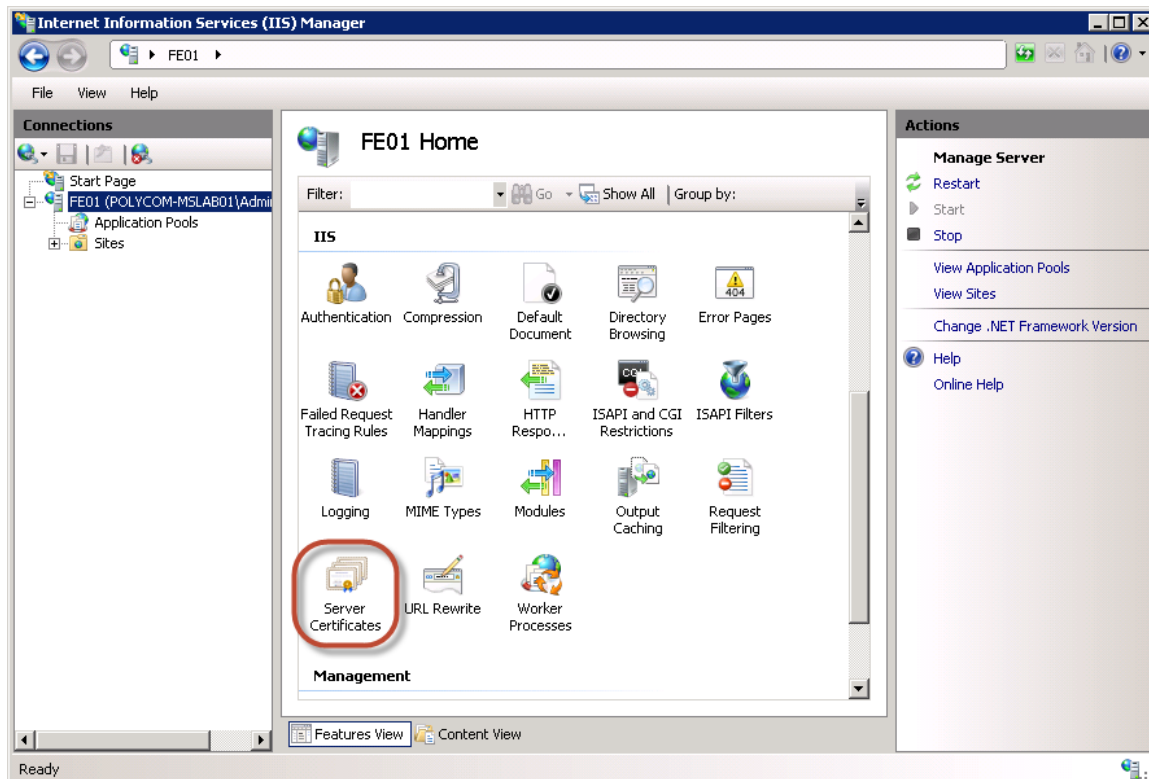
- ♦ If you must submit certificate requests through the enterprise's CA, use the procedure outlined next.
- ♦ If your organization permits, you can use the Internet Information Services (IIS) Manager on the Domain Controller to request certificates directly to the enterprise CA server.

Use the following procedure to request a security certificate for Windows Remote Management using IIS Manager 7.

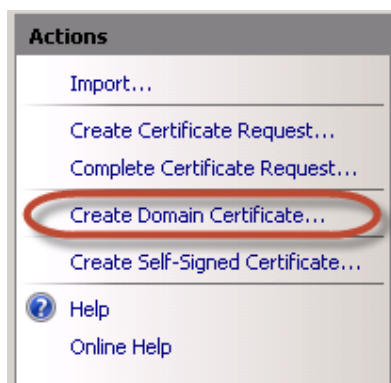
To request a security certificate using IIS Manager 7:

- 1 Open **IIS 7** on the **Domain Controller** by selecting **Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager (7.0)**.
- 2 Under **Connections**, double-click the server name.

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



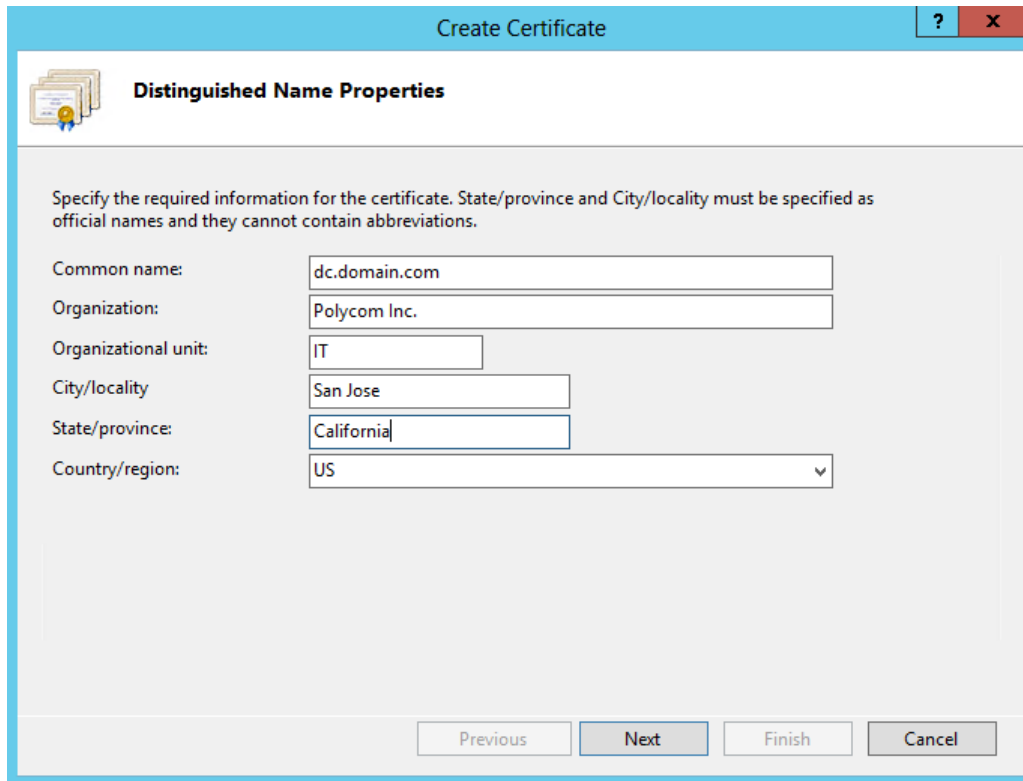
- 4 In the **Actions** pane (far right), select **Create Domain Certificate**, shown next.



The Create Certificate wizard displays.

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

- In the **Common Name** field, enter the FQDN for the Domain Controller. This name must match what displays in the DNS.



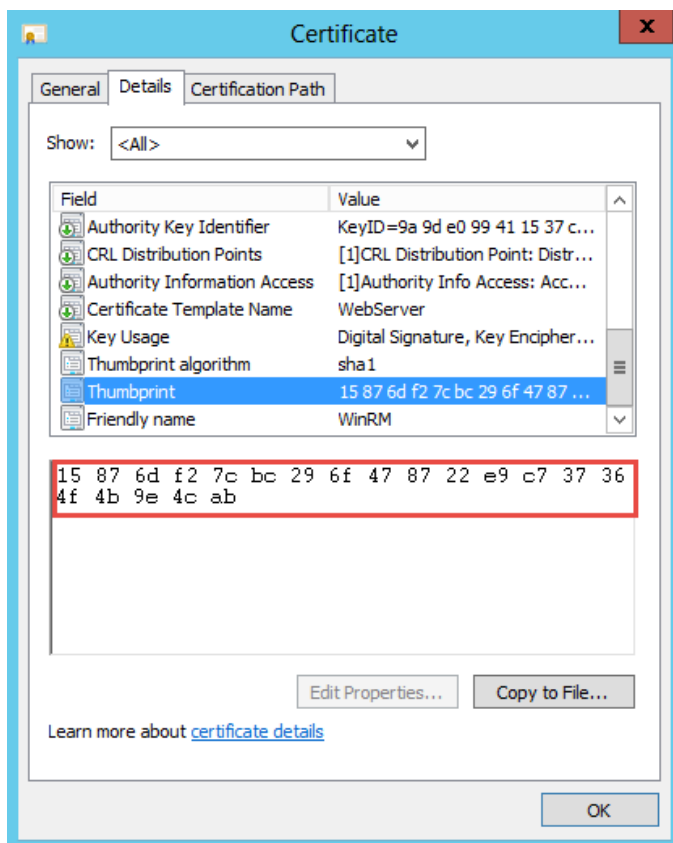
The screenshot shows a Windows-style dialog box titled "Create Certificate" with a blue header bar. Below the header, there's a section titled "Distinguished Name Properties" with a certificate icon. A text box explains: "Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations." Below this, there are six input fields: "Common name:" with "dc.domain.com", "Organization:" with "Polycom Inc.", "Organizational unit:" with "IT", "City/locality" with "San Jose", "State/province:" with "California", and "Country/region:" with a dropdown menu showing "US". At the bottom, there are four buttons: "Previous", "Next" (highlighted in blue), "Finish", and "Cancel".

6 Click **Next**.

7 In the **Online Certification Authority** panel, select a certificate authority from the list and enter a name that you can easily identify, for example, Windows Remote Management (WinRM) certificate.

8 Click **Finish**.

You have successfully created the certificate. You can verify that the certificate has been created and obtain the corresponding thumbprint. After you locate the certificate, open it to view the thumbprint, as show next.



Next, create a Windows Remote Management listener with the corresponding certificate.

To create a Windows Remote Management listener:

- 1 Enter the following into an Administrator command prompt:

```
winrm create winrm/config/Listener?Address=*&Transport=HTTPS
@{Hostname="<Domain Controller FQDN used for certificate common
name>";CertificateThumbprint="<Certificate thumbprint>"}
```

Note that you cannot execute this command via PowerShell.

- 2 Validate the Windows remote management listener by executing:

```
winrm enumerate winrm/config/listener
```

The output confirms that you created a listener on the HTTPS transport with the correct certificate applied.

- 3 Change the PowerShell execution policy to permit the local scripts to run on both the domain controller(s) and Lync Server(s). Both script execution policies should be set to **RemoteSigned**, which you can set by running the following command on Windows PowerShell: `Set-ExecutionPolicy RemoteSigned`.

After you complete these steps for all domain controllers, set the same on each Lync Front End. You must create each certificate with a common name that matches the FQDN for the respective server, for example, `Dc1.domain.com` and `Fel.domain.com`.

After completing these steps you can publish presence for your RealPresence DMA system VMR contacts. You must complete Active Directory integration before publishing presence to enable RealPresence DMA system to automatically manage contacts.



Note: Set an allow rule if Windows Firewall is enabled.

If Windows Firewall is enabled on any or all domain controller(s) and front end(s), you must set an allow rule for inbound connectivity between RealPresence DMA system and the Windows Remote Management service. You can do this by executing the following within the same command prompt, for example with Windows Server 2008:

```
netsh advfirewall firewall add rule name="Secure Windows Remote Management" protocol=TCP dir=in localport=443 action=allow
```

Alternatively, you can set it for Windows Server 2008 R2 or greater:

```
netsh advfirewall firewall add rule name="Secure Windows Remote Management" protocol=TCP dir=in localport=5986 action=allow
```

To publish presence for VMR contacts:

- 1 On the RealPresence DMA system, go to **Admin > Conference Manager > Conference Settings**.
- 2 Under **Presence Publishing**, check one of the following two options:
 - Publish Presence for Polycom conference contacts. Select this if you want to create contacts manually, and then complete the following fields:
 - ♦ Choose the Lync pool you created as a part of your Microsoft SIP peer.
 - ♦ Enter the contact SIP domain used to manually created contacts or which were assigned during the automated contact creation process.

The following illustration shows a RealPresence DMA system presence publishing configuration for VMR accounts when manually created by the Lync administrator.

Presence Publishing

☒ Publish presence for Polycom conference contacts

Lync pool to create/publish to: Lync Pool

Contact SIP domain: sipdomain.com *

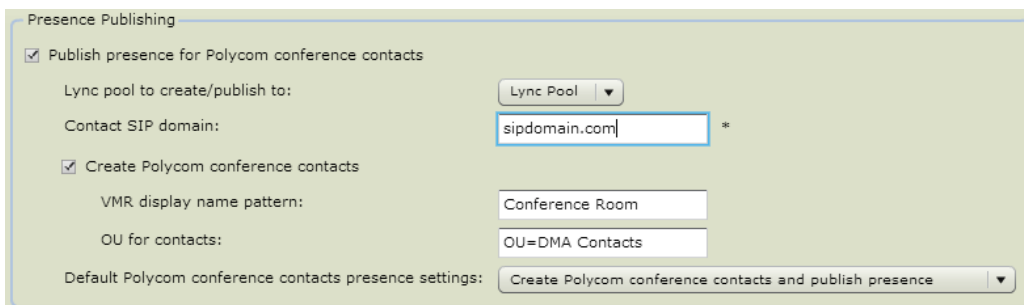
☐ Create Polycom conference contacts

VMR display name pattern: Conference Room

OU for contacts: OU=DMA Contacts

Default Polycom conference contacts presence settings: Publish Polycom conference contacts presence

- Create Polycom conference contacts. Select this to enable automatic contact creation and complete the following fields:
 - ♦ Enter a VMR display name pattern you want to use as a naming convention for all contact names.



Presence Publishing

☒ Publish presence for Polycom conference contacts

Lync pool to create/publish to: Lync Pool

Contact SIP domain: sipdomain.com *

☒ Create Polycom conference contacts

VMR display name pattern: Conference Room

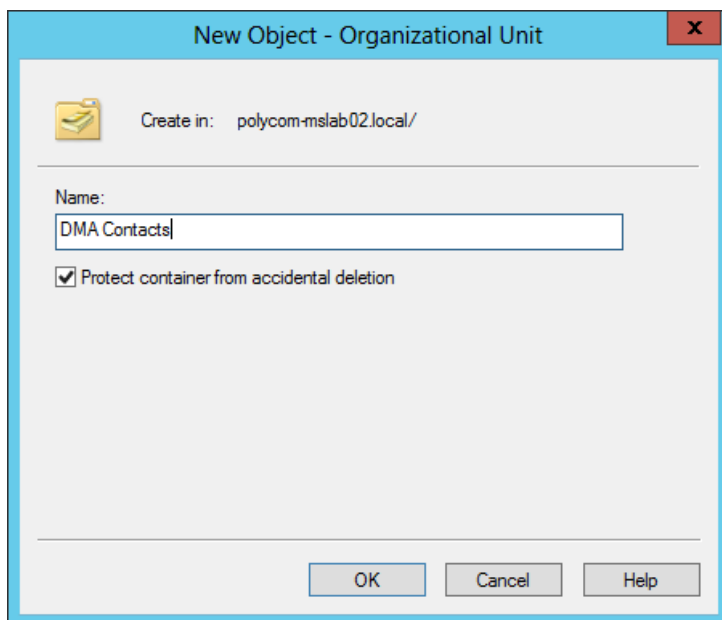
OU for contacts: OU=DMA Contacts

Default Polycom conference contacts presence settings: Create Polycom conference contacts and publish presence

- ♦ (Optional): The Organizational Unit (OU) you enter here assigns an individual Active Directory container or organizational unit in the order that RealPresence DMA system contacts are situated independently from Active Directory Users and Groups. If you do not enter an OU, the RealPresence DMA system will use `CN=Users`. If you enter an OU, the RealPresence DMA system will create contacts only within this container. Note that you must create the OU before entering it in RealPresence DMA system; the DMA informs you if the OU is not complete.

To create an Organizational Unit:

- 1 Open **Active Directory Users and Computers**.
- 2 Right-click your root domain.
- 3 Select **New > Organizational Unit**. When assigning an OU, you do not need to identify the full Distinguished Name for the container as the root domain information is already accounted for.



New Object - Organizational Unit

Create in: polycom-mslab02.local/

Name: DMA Contacts

☒ Protect container from accidental deletion

OK Cancel Help

To manually create a Virtual Meeting Room or manage the Presence publishing setting for an existing locally defined room:

- 1 On the **DMA** control panel, go to **Access User > Users > Manage Conf Rooms**. Here you can add or manage an existing room and override the global settings you defined previously.
- 2 To publish presence for a VMR, go to **Edit Conference Room**, check **Presence**, and choose **Create contact and publish presence**.

Edit Conference Room

Room ID: 1000 * Generate

Dial-in #: 1000

☐ Territory: Default DMA Territory (dma11) ▼

☐ Conference template: Factory Template ▼

☐ MCU pool order: Factory Pool Order ▼

☐ MCU Selection: Prefer MCU in first MCU pool ▼

☐ Max participants: Automatic ▼

☐ Chairperson passcode:

☐ Conference passcode:

Conference room pass-through to CDR:

☐ Resource priority namespace: None ▼

Resource priority value:

☒ Presence Create contact and publish presence ▼

☐ Conference duration Create contact and publish presence

☒ Unlimited Do not create contact or publish presence

☐ Hours: 0 Minutes: 00

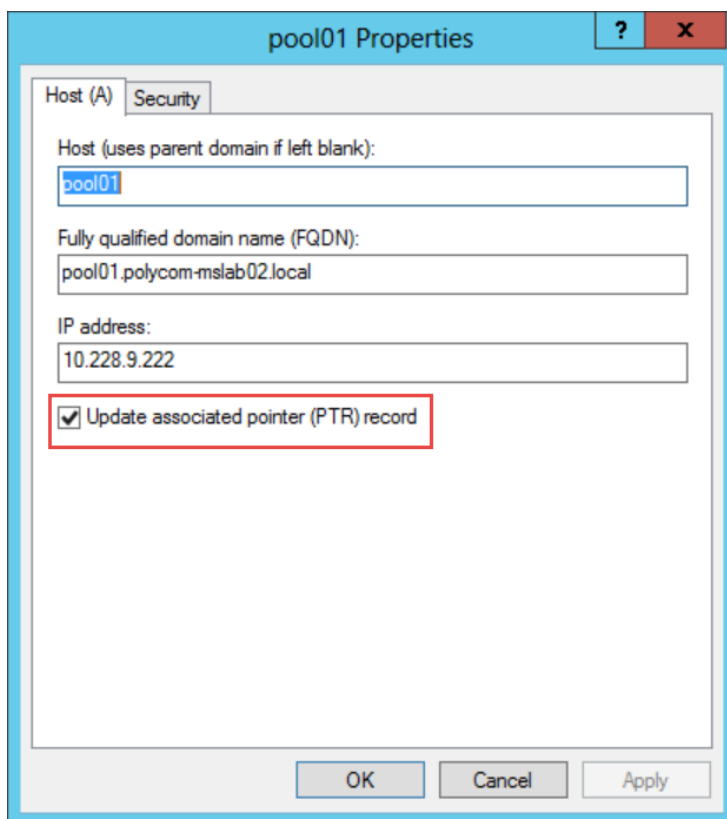
OK Cancel Help

- 3 In **Presence Publishing**, complete the fields as shown next.



Note: Enable Update associated pointer (PTR record) for your Enterprise Pool A Record

When you set RealPresence DMA system to automatically create VMRs with Lync and you create Lync-enabled publish presence contacts within Active Directory, DMA uses PTR records to perform discovery for Active Directory and Lync Servers. If you are deploying Enterprise Lync Pools with manual records, you must ensure that reverse lookup is possible by selecting **Update associated pointer (PTR) record**, as shown next.



Configure RealPresence DMA System for Polycom ContentConnect Software

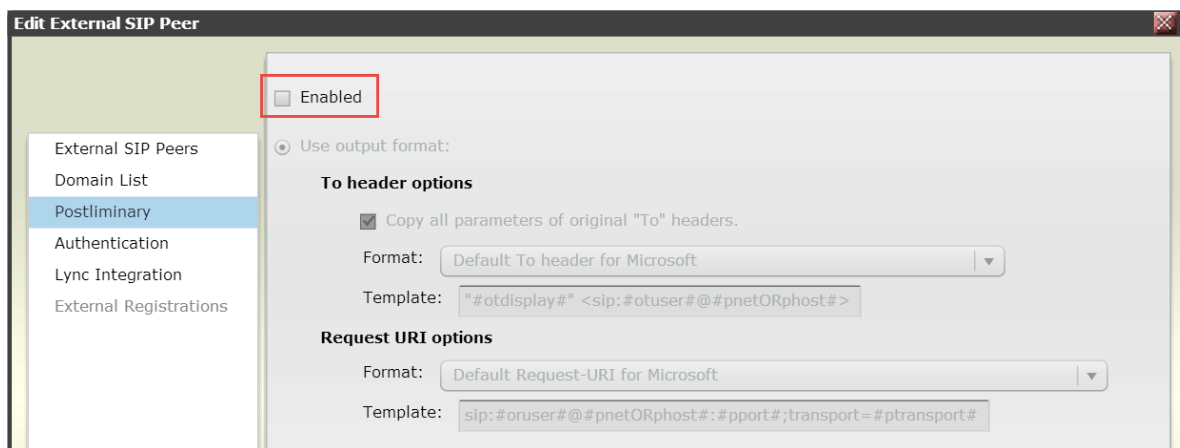
There are no Polycom ContentConnect software-specific RealPresence DMA system settings you need to configure. However, you must configure certain RealPresence DMA system settings to deploy RealPresence DMA system in a Microsoft Lync environment. To configure RealPresence DMA system to work within a Lync environment, see the section [Deploy Polycom RealPresence DMA Systems](#).

For your RealPresence DMA system setup, consider the following:

- Within the RealPresence DMA system, you must configure an external SIP peer for the Microsoft Lync Server. This allows SIP calls routed from the RealPresence DMA system to reach devices registered to the Lync Server.

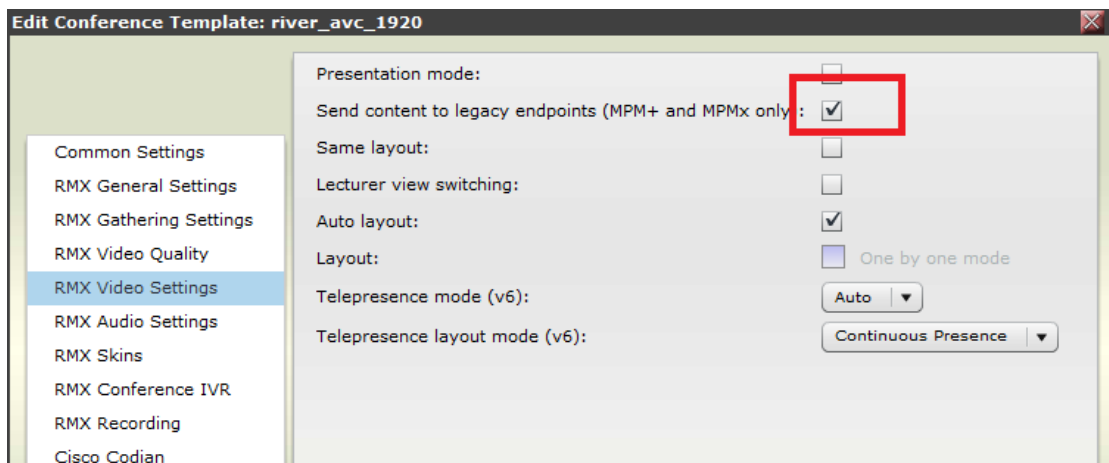
To configure RealPresence DMA system for Polycom ContentConnect Software:

- 1 Ensure that the postliminary is not enabled. Polycom DMA system v6.3 postliminary configuration for the SIP peer is not the same as for Polycom DMA system v6.2.



- 2 For the conference template you created in the section [Configure the RealPresence DMA system Lync Dial Rule](#), select **Send content to legacy endpoints (MPM+ and MPMx only)**, as shown next.

Selecting this setting enables endpoints that don't support H.239 to receive the Content channel over the video (People) channel. For information on creating conference templates in RealPresence DMA system, see the *Operations Guide* for your RealPresence DMA system, at [Polycom RealPresence Distributed Media Application \(DMA\)](#) on Polycom Support.



- 3 When running Polycom ContentConnect software in Gateway Mode, add a dial rule for authorized calls for external SIP peers, with the following settings:
 - **Description** External Lync SIP peer
 - **Action** Resolve to external SIP peer
 - **Preliminary Enabled** No
 - **Enabled** Enabled

Edit Dial Rule For Authorized Calls

Description:

Action:

☒ Enabled

Routing policy:

Available SIP peers

Lync Pool02

Selected SIP peers (weight)

Lync Pool01 (-)

The following illustration shows the new dial rule for Polycom ContentConnect software.

Dial rules for authorized calls:

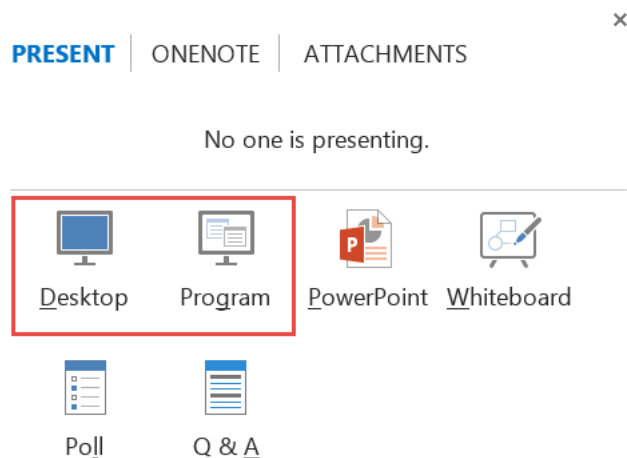
Order	Description	Action	Preliminary Enabled	Enabled
#1	Dial registered endpoints by alias	Resolve to registered endpoint	No	Enabled
#2	Dial by conference room ID	Resolve to conference room ID	No	Enabled
#3	Dial by Lync conference ID	Resolve to Lync Conference ID	No	Enabled
#4	Dial by virtual entry queue ID	Resolve to virtual entry queue	No	Enabled
#5	Dial services by prefix	Resolve to service prefix	No	Enabled
#6	Dial external networks by H.323 URL	Resolve to external address	No	Enabled
#7	Dial endpoints by IP address	Resolve to IP address	No	Enabled
#8	External Lync SIP Peer	Resolve to external SIP peer	No	Enabled

Deploy Polycom ContentConnect Software

This section explains how to configure Polycom ContentConnect software solution components with Microsoft Lync. You'll learn how to set up Polycom ContentConnect and enable for Gateway Mode.

Polycom ContentConnect software v1.5 operates by default in Gateway Mode. Gateway Mode enables the Polycom ContentConnect software server to work as an RDP-BFCP content gateway, fully transcoding RDP and BFCP H.264 content streams. For instructions on setting up a Polycom ContentConnect software environment and installing and configuring components in "Add-on Mode", see the *Polycom RealPresence Content Sharing Suite Administrator Guide* at [Polycom RealPresence Content Sharing Suite](#) on Polycom Support.

Because Gateway Mode facilitates RDP-BFCP transcoding, not all Lync sharing modalities are supported. When sharing content via Lync, you must use either Desktop or Program sharing.



Note: Using Gateway Mode with Skype for Business

Gateway Mode facilitates content sharing only between standards-based video room systems and Lync for Polycom RealConnect conferences. You must set Polycom ContentConnect to Gateway Mode when using with Skype for Business and/or RealConnect. If you are direct dialing to RealPresence Platform, you must set Polycom ContentConnect to Add-On Mode.

Required Components

The following table lists required components that must be set up in your environment before you deploy Polycom ContentConnect software with Lync Server. Note that to support remote access for standards-based video endpoints, you will require either a RealPresence Access Director or Acme Packet Net-Net Enterprise Session Director (ESD). For Lync clients, only a Lync Edge server is required.

Required Polycom ContentConnect software components for Microsoft Lync

<i>Component</i>
Management Systems and Recorders Microsoft Active Directory Server
Gatekeepers, Gateways, and MCUs Microsoft Lync Server 2013 Polycom RealPresence Distributed Media Application (DMA) 7000 (6.2 or higher) Polycom RealPresence Collaboration Server (RMX) Software MCU/1500/1800/2000/4000 (8.5 or higher)
Microsoft Endpoints Gateway Mode Microsoft Lync Client installed on Windows, Mac, mobile platforms (iOS, Android, Windows), and Lync Room Systems.
Video Endpoints Your environment requires one or more video endpoints that receive content from RealPresence Collaboration Server (RMX). For more information on interoperability, see the Interoperability Tables section in the RealPresence Collaboration Server (RMX) Software MCU/1500/1800/2000/4000 Release Notes at Collaboration & Conferencing Platforms .
Polycom ContentConnect software Product Component VMware or Hyper-V software, the host of the Polycom ContentConnect OVA-formatted Virtual Appliance Software Installation Package/VHD-Formatted Virtual Appliance Software Installation Package. For more information, see the section <i>Install the RealPresence Content Sharing Server Components</i> in the <i>Polycom RealPresence Content Sharing Suite Administrator Guide</i> on Polycom Support .

Optional Components

The following table lists optional and compatible components that you can install and set up before you deploy Polycom ContentConnect software with Lync Server.

Optional Polycom ContentConnect software components for Microsoft Lync

<i>Component</i>
Firewall, Border Controllers Lync Edge Server Polycom RealPresence Access Director Acme Packet® Net-Net Enterprise Session Director (ESD)
Recorders Polycom RSS 4000 solution or RealPresence Capture Server

Component

Load Balancers

Polycom has tested the following load balancer:

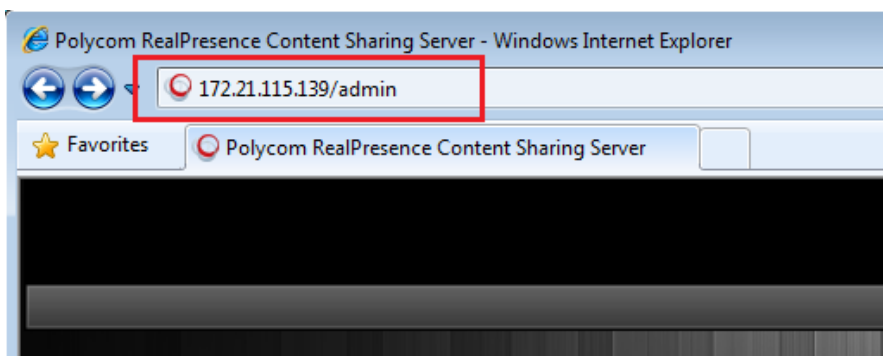
F5 BIG-IP LTM 1600 and BIG-IP 10.2.1.297.0

Access and Use the Polycom ContentConnect Server Web Configuration Tool

This section shows you how to access the Content Sharing Server Web Configuration Tool, and use it to configure the Content Sharing Server.

To access the Content Sharing Server Web Configuration Tool:

- 1 Launch a web browser and enter **<IP address of the Content Sharing Server>/admin** in the address bar as shown next. For example, enter 172.21.115.139/admin, where 172.21.115.139 is the IP address of the Content Sharing Server.



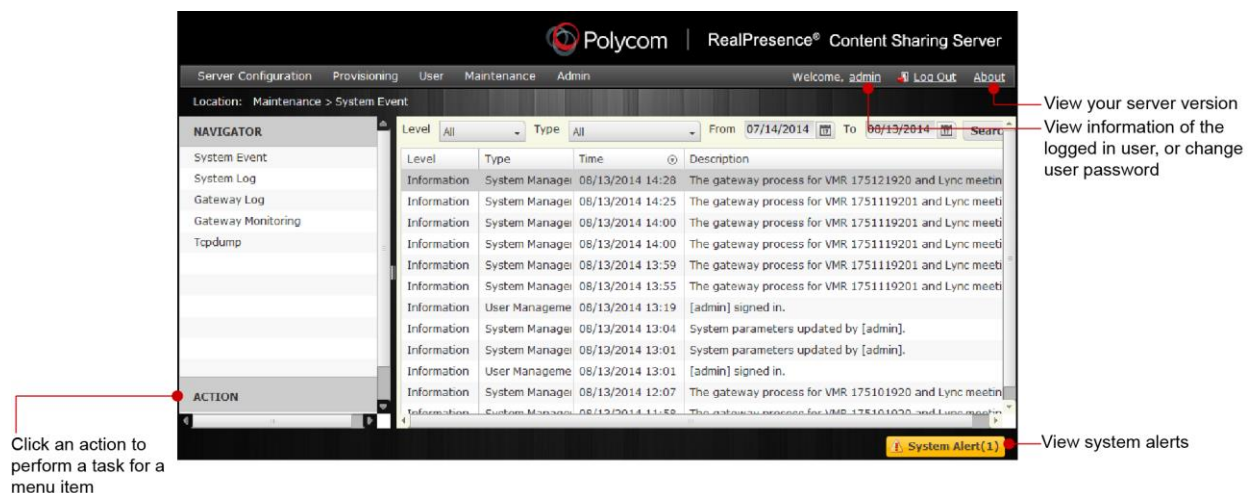
- 2 Press **Enter**.
The Content Sharing Server Web Configuration Tool **Log In** screen displays.
- 3 Enter your **User ID** and **Password**, and click **Log In**. The default login credential for both user ID and password is admin.

**Note: Default user name and password**

For information on default user names and passwords, see the *Polycom RealPresence Content Sharing Suite Administrator Guide* at [Polycom RealPresence Content Sharing Suite](#) on Polycom Support.

The Content Sharing Server Web Configuration Tool screen displays.

The Content Sharing Server Web Configuration Tool has a primary menu bar with five main menus: Server, Provisioning, User, Report, and Admin. Selecting a menu reveals additional submenus as shown next. Under the primary menu bar is additional navigation information, to let you know which menu item you're currently configuring.



Each page of the Content Sharing Server Web Configuration Tool also displays the following items:

- User ID, **Log Out**, and **About** display on the top right. Click each to do the following:
 - Click the user's ID to view information about the currently logged-in user (in this case, *admin*, and to change the user's password.
 - Click **Log Out** to log out of the Content Sharing Server Web Configuration Tool and return to the **Log In** screen.
 - Click **About** to display the version of the RealPresence Content Sharing Server.
- At the bottom-right of the screen is an alert to let you know if there are any important messages. Click **System Alert** to view these messages.
- On the far left of the screen, a list of actions display that enable you to perform specific tasks. For example, depending on the menu item you're configuring, you may be able to create, refresh, edit, export, clear, import, delete, or update items or settings.

Configure the Content Sharing Server Using the Content Sharing Server Web Configuration Tool

To configure the Content Sharing Server for Gateway Mode, you need to configure server information. RealPresence Access Director is required for standards-based video room systems requiring remote content sharing capabilities. For information, refer to the *Polycom RealPresence Content Sharing Suite Administrator Guide* at [Polycom RealPresence Content Sharing Suite](#) on Polycom Support.

Configure Polycom ContentConnect Software Server Running Mode

Polycom ContentConnect software server works in two modes:

- Gateway Mode
 - Lync clients don't need to install the Polycom RealPresence Content Add-on for Lync Service for content sharing.
 - Polycom ContentConnect software server works as an RDP - BFCP content gateway, providing full transcoding between RDP and BFCP H.264 content streams.
- Add-On Mode
 - All Lync clients must install the Polycom RealPresence Content Add-on for Lync Service for content sharing.
 - The add-on handles content sharing when there is legacy participant with BFCP content supported in the conference.
 - Content media is BFCP H.264 video stream and goes directly through RealPresence Collaboration Server (RMX) from the Polycom ContentConnect software plugin.



Note: This guide focuses on Gateway Mode deployment

This guide focuses on the deployment steps required for Gateway Mode and does not address Add-on Mode.

To configure Polycom ContentConnect software server running mode:

- 1 From the RealPresence Content Sharing Server Web Configuration Tool, select **Server Configuration > Running Mode**.
- 2 Select a running mode:
 - Gateway Mode

If you select this option and you have the **Polycom RealPresence Content Add-on for Lync Service** installed already, it will be disabled.
- 3 Click **Save**.



Note: Only H.264 content is supported on legacy endpoints in the Gateway mode

In this release, only H.264 content is supported on legacy endpoints in the Gateway mode.

Configure Server Information

You can configure a SIP server and load balancer server to work with the Polycom ContentConnect software server.

To configure server settings:

- 1 Log in to the Content Sharing Server Web Configuration Tool.
- 2 Select **Server Configuration > Server**.

3 Enter the following information:

- **SIP Server Address** The IP address or host name of the RealPresence DMA system.
- **SIP Server Administrator User** The user name of a RealPresence DMA system administrator.
- **SIP Server Administrator Password** The password of a RealPresence DMA system administrator.
- **SIP Proxy Port** The RealPresence DMA system port number.
- **SIP Registrar Port** The RealPresence DMA system registrar port.
- **SIP Domain Suffix** The SIP domain suffix. This must be the same value you entered in the destination network field for the SIP Peer defined for Lync on RealPresence DMA system.
- **SIP Authorization Name, SIP Password** SIP authentication credentials created in RealPresence DMA system (if RealPresence DMA system needs to authenticate Polycom ContentConnect software Gateway).
- **Call Rate** The call rate for the SIP call with RealPresence Collaboration Server (RMX).
- **SIP Transport Protocol** The transport protocol to be used for the SIP call.
- **Media Encryption** Whether to enable media encryption. If you select **Auto**, the SIP server decides whether or not to enable media encryption.
- **Media Transport Port Range** The port range allocated for media transmission.
- **F5 Virtual Server Address** Load Balancer virtual server address.

4 Click **Save**.

The following illustrates an example Gateway Mode configuration.

Gateway Mode configuration example

▼ Server Configuration

The server is running in "Gateway Mode" now.

SIP Server Address *	<input type="text" value="192.168.1.100"/>	
SIP Server Administrator User *	<input type="text" value="admin"/>	
SIP Server Administrator Password *	<input type="password" value="*****"/>	
SIP Proxy Port *	<input type="text" value="5061"/>	1 ~ 65535
SIP Registrar Port *	<input type="text" value="5061"/>	1 ~ 65535
SIP Domain Suffix	<input type="text" value="sipdomain.com"/>	
SIP Authorization Name	<input type="text"/>	
SIP Password	<input type="password" value="*****"/>	
Call Rate *	<input type="text" value="1024"/>	kbps
SIP Transport Protocol *	<input type="text" value="TLS"/>	
Media Encryption *	<input type="text" value="AUTO"/>	
Media Transport Port Range *	<input type="text" value="33300"/> - <input type="text" value="43300"/>	1 ~ 65535
F5 Virtual Server Address	<input type="text"/>	

Make sure your SIP Proxy Port, SIP Registrar Port, and SIP Transport Protocol settings match corresponding settings in your SIP Server.

Save

(Optional) Configure your Polycom ContentConnect Software Provisioning Profile

When in Gateway Mode, the Polycom ContentConnect software provisioning profile is used only for meeting attendees that want to join Polycom RealConnect meetings and receive or send content via the Web client.

To configure Polycom ContentConnect software server:

- 1 Log in to the Content Sharing Server Web Configuration Tool.
- 2 Select **Provisioning > Provisioning Profile**.
- 3 Under **Action**, select **Edit**.

The **Edit the profile** dialog displays, as shown next.

The screenshot shows the 'Edit the profile' window with the following details:

- Name:** default profile
- Description:** (empty field)
- Table of settings:**

Key	Value	Action
conferenceIDRule	^sip:\d+@dma51\-ccs\.pctc\.local\$	Inherit
enableEncryption	AUTO	Inherit
preferredCallRate	512	Inherit
sipClientListeningPort	5070	Inherit
sipClientListeningTLSport	5071	Inherit
sipTransport	TLS	Inherit
tcpPortEnd	20000	Inherit
tcpPortStart	10000	Inherit
- Buttons:** Save, Cancel

4 From the **Edit the profile** window, update one or more of the following:

- **Name** The name of the provisioning profile.
- **Description** A description of the provisioning profile.
- **conferenceIDRule** Defines whether a call is a Lync-only call, or a RealPresence Collaboration Server (RMX) bridge call that will use Polycom ContentConnect software. You need to configure the rule with a JavaScript regular expression to match the RealPresence DMA system conference room ID format, which is dialed from the Lync client. For example, for 123456@dma51-ccs.pctc.local, the route dma51-ccs.pctc.local has been created in Lync.

A valid conference ID must start with “^sip:”. For example, to configure a rule that allows any combination of digits as a meeting room ID, create the following rule:

```
^sip:\d+@dma51\-ccs\.pctc\.local$
```

Note that dma51-ccs.pctc.local is the FQDN of the RealPresence DMA system.

If the rule is defined, any combination of digits that is used as a meeting ID created in RealPresence DMA system can be used to join a meeting and share content with a Lync client.

- **enableEncryption** Determines whether encryption should be enabled for the SIP call.
- **preferredCallRate** The preferred call rate for the client for the SIP call with RMX. Note that to share content, you need to set a call rate equal to or higher than 128K.
- **sipClientListeningPort** The client listening port (UDP/TCP).
- **sipClientListeningTLSport** The client listening TLS port.
- **sipTransport** The SIP transport for the SIP call.
- **tcpPortEnd / tcpPortStart / udpPortEnd / udpPortStart** If the port configured for sipClientListeningPort is occupied, the new listening port will be chosen during tcp/udpPortStart and tcp/udpPortStop.
- **verifyCert** Determines if the client verifies the server’s certificate authority (CA).

5 Click **Save**.

Appendix A: Polycom HDX System Configuration Files

The table [Polycom HDX .dat Files](#) lists all of the .dat files that the Polycom HDX system can read from the USB boot device.

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

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

Polycom HDX .dat Files

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

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

Appendix B: Exchange Calendar Polling Information

This appendix provides information on Microsoft Exchange Calendar polling.

Polycom HDX and RealPresence Group Series System

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

Polycom RealPresence DMA System

Polycom RealPresence 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, RealPresence DMA system connects to Exchange to download the meeting details. When doing this, RealPresence 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, RealPresence 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 RealPresence Collaboration Server (RMX) System

The Polycom RealPresence Collaboration Server (RMX) solution polls the Exchange server for updates every 15 seconds. When polling, the RealPresence Collaboration Server (RMX) considers events two hours in the past and 24 hours into the future.

Polycom RSS Solution

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

Appendix C: Lync Client and Server Support

This appendix lists Lync client and server support for features and deployment connectivity options.



Note: Lync Virtual Entry Queue not supported

On RealPresence DMA systems, Virtual Entry Queues (VEQs) do not support direct dialing from Lync clients into RealPresence Platform.

Lync Client and Server Support for Features

<i>Feature</i>	<i>Client</i>	<i>Server</i>	<i>Comments</i>
Scheduling – dial using a Lync conference ID	Lync 2010, Lync 2013 and Skype for Business 2015	Lync 2013 and Skype for Business Server 2015	
Multipoint Lync conference invite (drag/drop) a VMR	Lync 2010, Lync 2013 and Skype for Business 2015	Lync 2013 and Skype for Business Server 2015	
Meet Now calls to a VMR	Lync 2010, Lync 2013 and Skype for Business 2015	Lync 2013 and Skype for Business Server 2015	
Escalated calls – Lync client drag and drop multiparty call	Lync 2010, Lync 2013 and Skype for Business 2015	Lync 2013 and Skype for Business Server 2015	
Direct Lync call to VMR	Lync 2010, Lync 2013 and Skype for Business 2015	Lync 2013 and Skype for Business Server 2015	
Point-to-point calls between an endpoint registered to a RealPresence DMA system and a Lync client	Lync 2010, Lync 2013 and Skype for Business 2015	Lync 2013 and Skype for Business Server 2015	Audio only for calls with Lync 2013 clients
Presence enabled VMRs	Lync 2010, Lync 2013 and Skype for Business 2015	Lync 2013 and Skype for Business Server 2015	

Appendix D: Polycom RealConnect Technology Resources and Licenses

This appendix lists resources used and licenses required when operating Polycom RealConnect technology with Polycom ContentConnect software on Polycom products.

Required Polycom RealConnect Technology Resources and Licenses

<i>Mode</i>	<i>Product</i>	<i>Resources Used and Licenses Required</i>
Polycom RealConnect technology (Polycom ContentConnect software Gateway Mode)	RealPresence DMA system	<ul style="list-style-type: none"> No concurrent call license for the SVC cascaded connections with Lync AVMCU Two concurrent call licenses for Polycom ContentConnect software content gateway for the duration of the meeting One additional concurrent call license when sharing content
	RealPresence Collaboration Server (RMX) solution	<ul style="list-style-type: none"> 2.5 HD ports for Microsoft SVC cascade with AVMCU (standard definition resolution) 3.5 HD ports for Microsoft SVC cascade with AVMCU (720p resolution) 1 audio port for content
	Polycom ContentConnect software (Gateway Mode)	<ul style="list-style-type: none"> One Polycom ContentConnect software license per conference One Polycom ContentConnect software license web client
Polycom ContentConnect software (Add-on mode)	RealPresence DMA system	<ul style="list-style-type: none"> One concurrent license per Lync client One concurrent call license per Polycom ContentConnect software Lync add-on
	RealPresence Collaboration Server (RMX) solution	<ul style="list-style-type: none"> Each Lync client consumes video resources depending on the video resolution One audio port for content for each Polycom ContentConnect software Lync Add-on or web client
	Polycom ContentConnect software	<ul style="list-style-type: none"> One Polycom ContentConnect software license per Lync (with add-on) on VMR One Polycom ContentConnect software license per Polycom ContentConnect software web client

Appendix E: Configure Static Routes in Skype for Business

In Lync Server 2013 and Skype for Business Server 2015, you can configure static routes by routing SIP queries for a specific domain to a PBX, CSTN Gateway, or a third-party conferencing solution.

You must configure a static route if you are deploying VMRs with Skype for Business. This section shows an example of configuring static routes using a third-party conferencing solution.



Note: Polycom RealConnect does not require static routes or VMRs

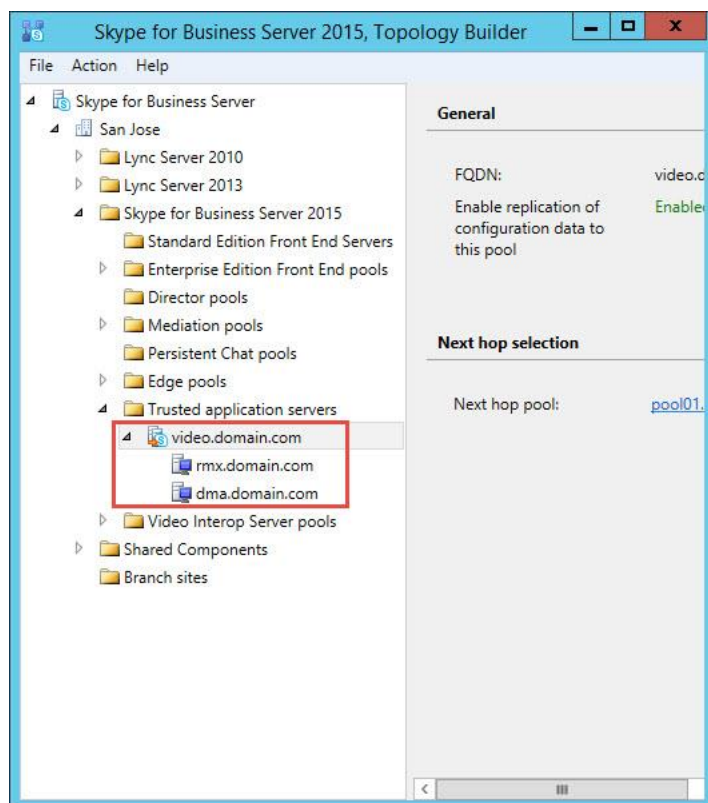
You do not require static routes or VMRs to deploy Polycom RealConnect technology as the Polycom DMA system automatically creates VMRs with the same number as the Skype for Business conference ID.

Trusted Application Pool

Third-party conferencing solutions are typically deployed within a Trusted Application Pool. The next example shows a Trusted Application Pool configured with two Trusted Applications:

- A SIP domain named `domain.com`
- A MatchURI, the domain triggering the static route, named `video.domain.com`.

The Trusted Application Pool defined as `video.domain.com` has no bearing on the SIP domain.



TLS Security

Prior to Skype for Business, you could configure a MatchURI without TLS validation by generating a certificate for the Trusted Application Server with the fully qualified domain name (FQDN) of the server (dma.domain.com in this example). With Skype for Business, the TLS route is validated. You must now generate a Subject Alternative Name (SAN) that includes both the FQDN for your Trusted Application Server and the MatchURI. If you do not configure, or configure incorrectly, an error message displays *“Certificate trust with another server could not be established”*, as shown next.

SIP/2.0 504 Server time-out

Authentication-Info: TLS-DSK qop="auth", opaque="D2C9D33D", srand="79431127", snum="12", rspauth="4a0211a65861e5faea17297d3df9f5dde8d19488", targetname="fe20.polycom-mslab03.com", realm="SIP Communications Service", version=4

From: "Adam Jacobs" <sip:adam.jacobs@polycom-mslab03.com>;tag=0f69acac28;epid=87255376f8

To: <sip:1000@video.polycom-mslab03.com>;tag=FE609E0504EC1DFCABDBE60FDEEB1CF8

Call-ID: 2e5c68d886604d10a71e76a4e3af7344

CSeq: 1 SUBSCRIBE

Via: SIP/2.0/TLS 10.230.27.26:56939;ms-received-port=56939;ms-received-cid=5648200

ms-diagnostics: 1010;reason="Certificate trust with another server could not be established";ErrorType="The peer certificate does not contain a matching FQDN";tls-target="video.polycom-mslab03.com";PeerServer="dma21.polycom-mslab03.com";HRESULT="0x80090322 (SEC_E_WRONG_PRINCIPAL)";source="fe20.polycom-mslab03.com"

Server: RTC/6.0

Content-Length: 0

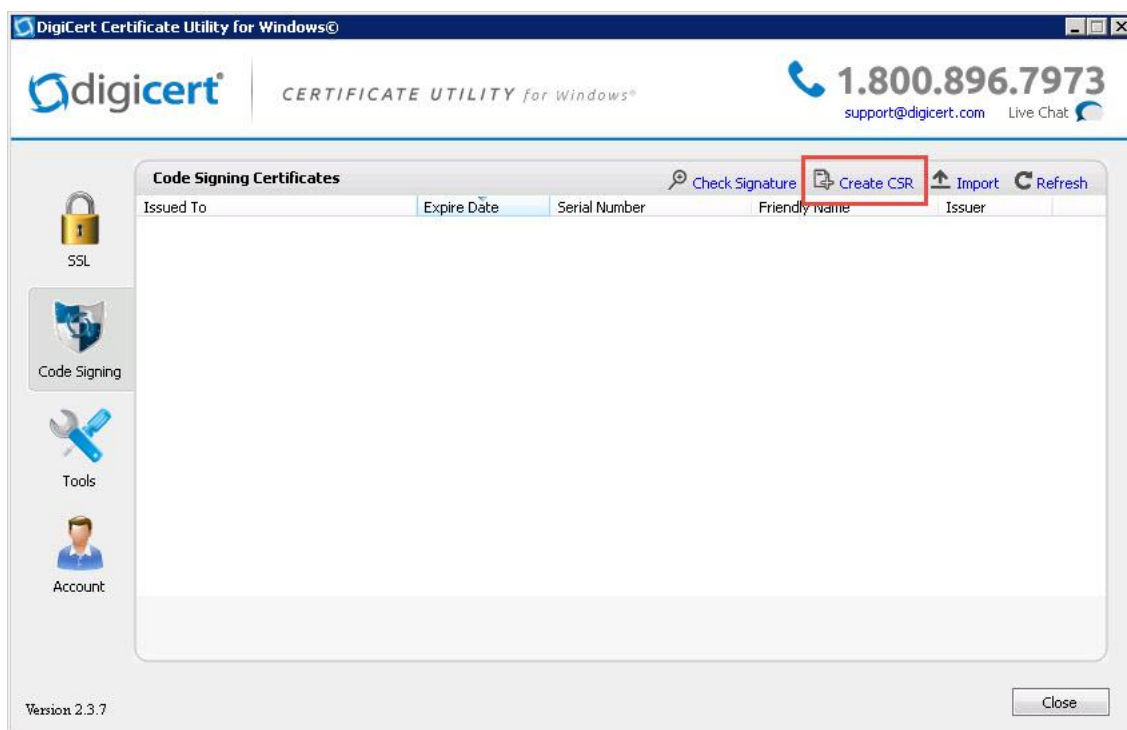
Configure a Certificate

The next example configuration shows how to generate a certificate for the Trusted Application Server `dma.domain.com` and the Match URI `video.domain.com` using a Windows Enterprise Certificate Authority.

This example configuration creates a SAN as explained in Microsoft's [How to Request a Certificate With a Custom Subject Alternative Name](#) rather than using IIS, and creates certificate signing requests (CSRs) using the [DigiCert Utility for Windows](#).

To configure a certificate:

- 1 Open the certificate utility executable from one of your Front End Servers and select **Create CSR** at top right.



2 In **Certificate Details**:

- a Set **Certificate Type** to SSL.
- b Enter your common name domain in **Common Name**.
- c In **Subject Alternative Names**, duplicate the common name domain and add the MatchURI.

d Click Generate.

DigiCert Certificate Utility for Windows®

Create CSR

Certificate Details

Certificate Type: ☒ SSL ☐ Code Signing

Common Name: dma.domain.com

Subject Alternative Names: dma.domain.com, video.domain.com

Organization: Polycom Inc.

Department: MSLAB

City: San Jose

State: California

Country: USA

Key Size: 2048

Provider: Microsoft RSA SChannel Cryptographic Provider

Information

Country

Choose the country your organization is located in. If your country does not appear in this list, there is a chance we cannot issue certificates to organizations in your country.

Generate Cancel

3 Click Save to File after the certificate request is generated.

DigiCert Certificate Utility for Windows® - Create CSR

The certificate request has been successfully created

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC+DCAeACAQAwDTELMAkGA1UEBhMCVVMxEzARBgNVBAGTCkNhbmG1mb3JuaWEu
ETAPBgNVBACQFNhbiBkZ3N1MQ4wDAYDVQQLEwVNUU0xBoQjEVMBEMGA1UEChMMUG9s
eWVubSBzJmFuMRcwFQYDVQQDEw5kbWVud2C9cTYW1uLmNvbTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALRBxIGbr0+SH7TVWsbCUIXKt7eus03K90gxLzX
PrFobvBm6XQ1v10FQKHv0G02d+3JIq3Mmk20MLa4+sAf8JyrxpDXyD4f9d8myg
UHV0CEBb1IeTrwfKjnK60FBg9Cy/PZooRSu+2EzXumDE6cwVuemsD26W09syavu
TlbXJ5jqX2L128y7/ut7TodP+upaTgBuixCBiZsJvRd6FFxebb0tUAPgM/89Gd7
SdAvHy9Yy0D4243TaA8/CZzWS21wQhvQo/4C4MnCDQbBo1FFb0CqVJjEgOktRf6C
hY5ysRUHcn/582zt+4PD27fUEj43o1qseYe3zraFpehEf3SkCAwEAaAA+MDwGCSQG
SIlb3DQEJDjEvMCOwKwYDVR0RBCCQwIoI02G1hLmRvbWVpb15jb22CEHZp2GVvLmRv
bWVpb15jb20wDQYJKoZIhvcNAQEFBQADggEBAIcubrJtYAiVBjN0qMSqspk11ogv
3ch5W18G1qoYj184oo68DpY0ISgfzIvF+cAxDi1bPj08/Fpq2HF/7gLfdIS92Kg
TUxHEsyXZP9ajV79D8ScHD\UHRbbRsX0SFVXdc8sYwK2p fGlu61wvQ0eoAYksA6W
3mElP89rpNPztI2f02qUva0YFP LRP8y1B70MTXxJJLDVdshjc5pENC3wdx+Nft1J
BVYicHDqX41VtWoRjBYRK466xmCwP4bL1K3n0zHNYBfTrCwEhR4A3khjN0fEBv8
SoGJmmu0DKjYuEk571wB2TxLVYRwCj3A2dRt5/q0JqVTT+Itqh9GKxrlYCG=
-----END NEW CERTIFICATE REQUEST-----
```

Copy CSR Save to File Close

4 Upload the certificate request file to your Windows CA. Typically, you can do this using web enrollment at <http://<CA.FQDN>/CertSrv>. When prompted to authenticate, select **Request a certificate > Advanced certificate request.**

- 5 Copy and paste the certificate file to the **Saved Request** field, in **Certificate Template** select **Web Server**, and click **Submit**.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	<div>TUrhE5yXZP9ajV79D8ScHDXUHRbbRsXOSFVXdc8s 3mE1P89rpNPztIZfOZqOvaOYFPLRP8ylB70MTXxJ BVYicHDqX41VIw0RjBYRK466xmCwP4bLA1K3n0zH SoGJmnuODKjYuEk571wB2TxLVYRWtj3AZdRt5/q0 -----END NEW CERTIFICATE REQUEST-----</div>
-------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

- 6 Download the certificate.

Certificate Issued

The certificate you requested was issued to you.

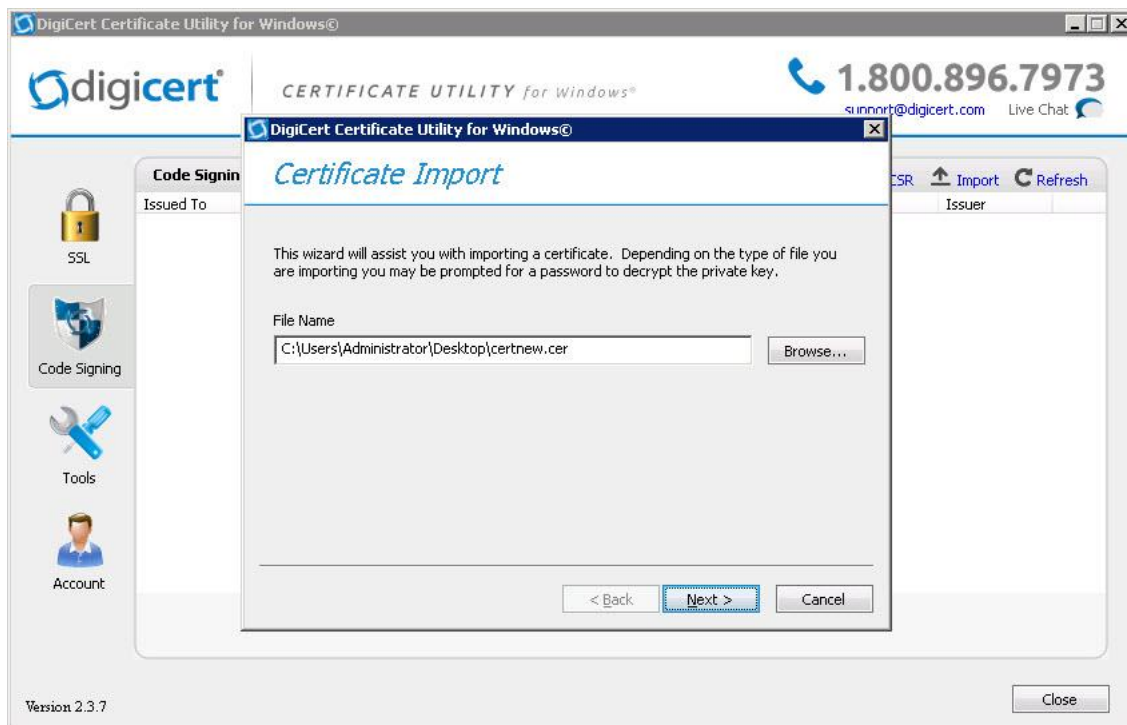
☒ DER encoded or ☐ Base 64 encoded



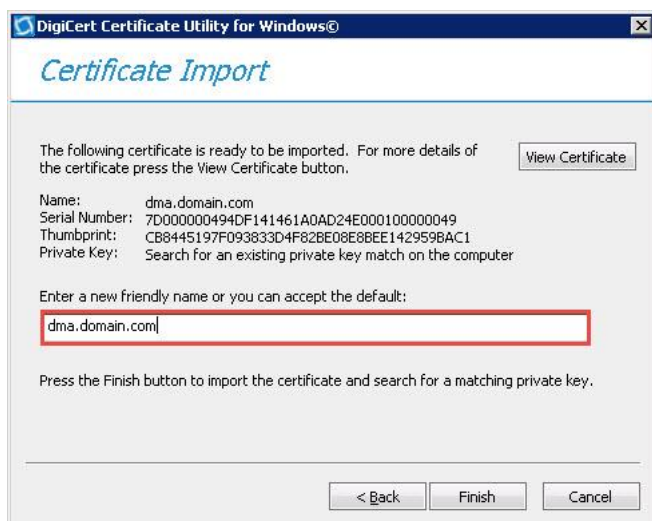
[Download certificate](#)

[Download certificate chain](#)

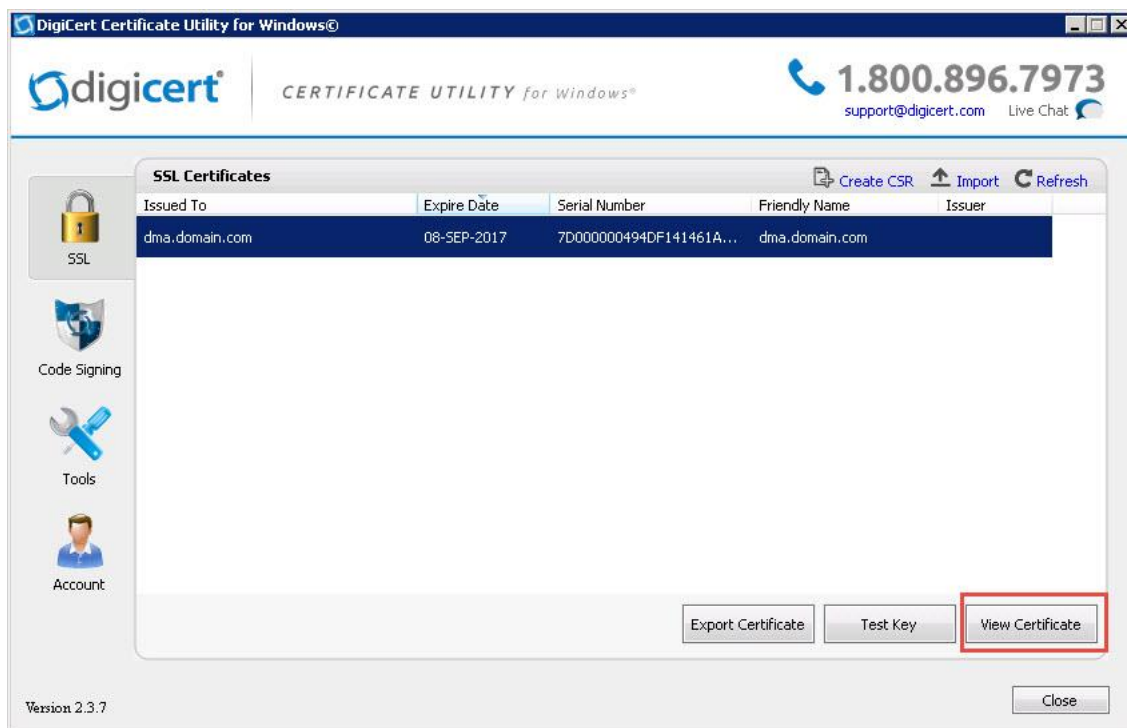
- Click **Import** at top right, and point to the certificate file, assigning a friendly, easily identifiable name, and click **Finish**.



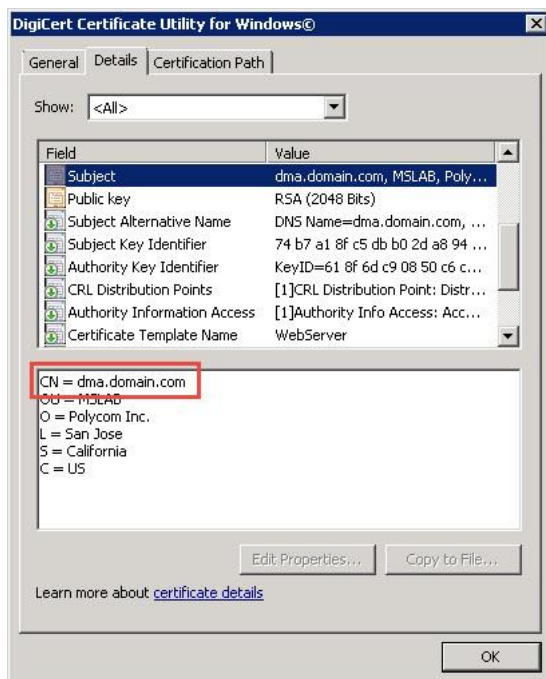
This examples uses the name `dma.domain.com`.

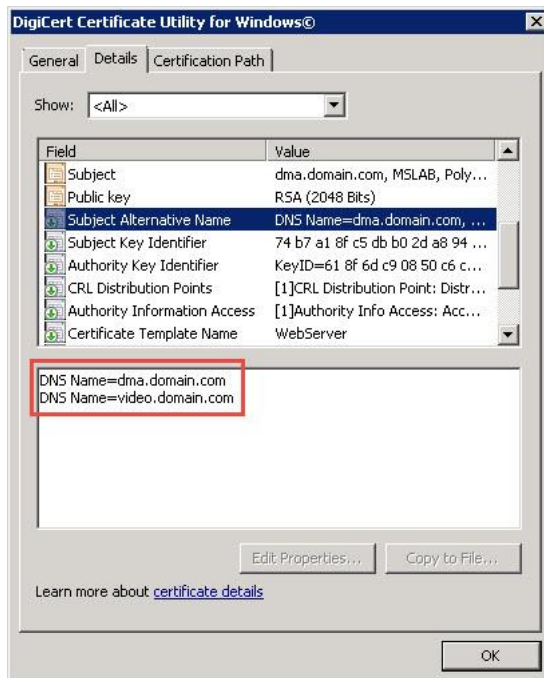


8 Next, validate your certificate by clicking **View Certificate**.



Ensure that the common name (CN) displays your Trusted Application Server FQDN (`dma.domain.com`) and that the Subject Alternative Name contains both the Trusted Application Server FQDN (`dma.domain.com`) and the Match URI (`video.domain.com`), as shown next.



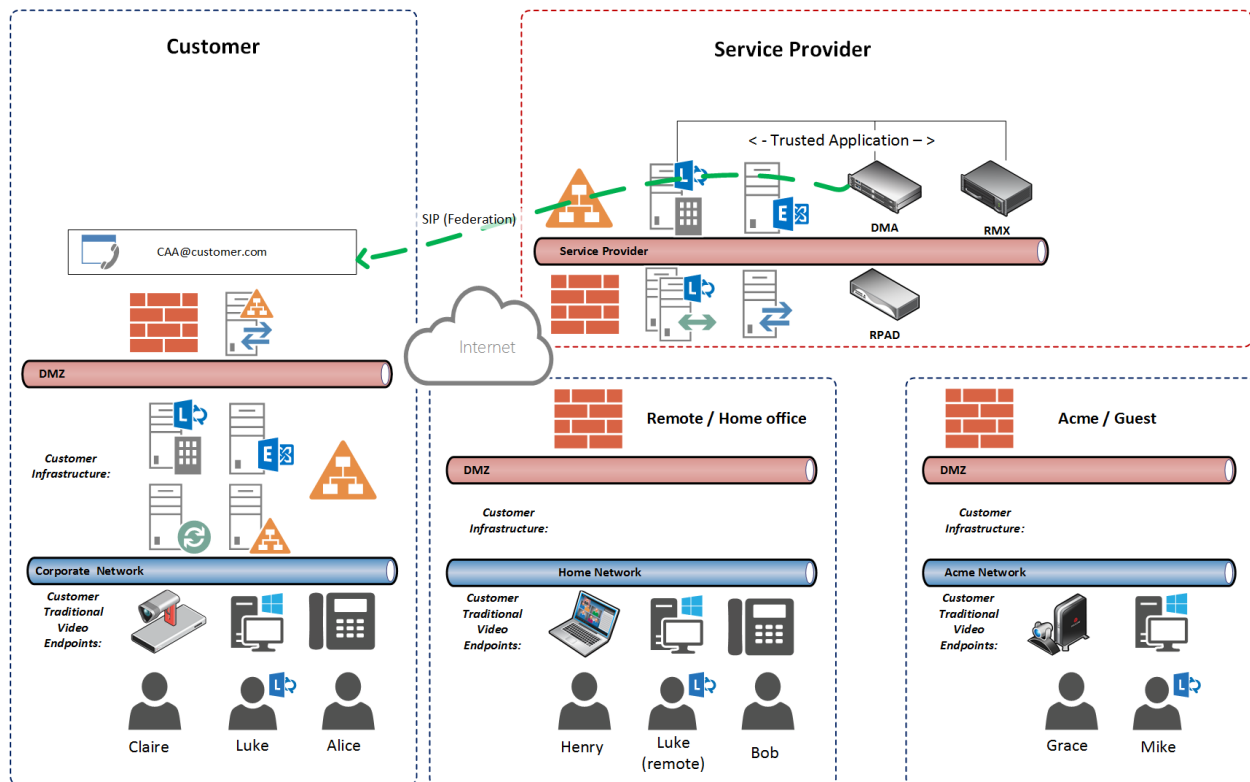


You can now upload the certificate to your third-party conferencing server.

Appendix F: Polycom RealConnect for Service Providers

Polycom RealConnect technology for Microsoft Lync offers a seamless way to bring standards-based video conferences into meetings scheduled in an on-premise Microsoft Lync environment.

Polycom now offers service providers the ability to host a multi-tenant instance of the RealPresence Platform that offers customers full Polycom RealConnect functionality. In this scenario, customers can schedule Lync conferences from their on-premise Lync environment and join video conferences using Polycom RealConnect hosted by the service provider. Communication is handled via Lync Federation and Polycom RealConnect VMRs automatically join the corresponding Lync conference with voice, video, and content.



Prerequisites for Service Providers

To deploy this solution, service providers must have the following versions of Polycom products:

- RealPresence Collaboration Server (RMX) 8.6 or later (for a hardware-based Collaboration Server (RMX) you must deploy MPMrx cards)
- Polycom RealPresence DMA 6.3 or later
- Polycom® ContentConnect™ 1.5 or later
- Integration with a local instance of Lync Server 2013

RealPresence System and Lync 2013 for Polycom RealConnect

Polycom RealPresence Collaboration Server (RMX) solution, RealPresence DMA and Polycom ContentConnect systems introduce Polycom RealConnect technology for Lync 2013, a new RealPresence platform function for Lync 2013 customers. Polycom RealConnect technology enables you to dial into scheduled Lync 2013 conferences using H.323 or standard SIP. Because all of the call control and media translation is handled by the RealPresence Collaboration Server (RMX) solution and RealPresence DMA system, any standards-based H.323 or SIP endpoint can use Polycom RealConnect technology even if the endpoint does not support Lync.

The figure 'Lync Invitation with Conference ID' shows a Lync invitation populated with a Conference ID, which is provided automatically by the customer's respective Lync Server and represents the H.323 number or SIP URI you dial on the endpoint.

For example:

Dialing from H.323 endpoint: 17894

Dialing from SIP endpoint: 17894@dmadomain.net



Note: Configure Microsoft dial-in conferencing

Conference IDs are generated only when you deploy Lync Dial-in Conferencing and are typically enabled when PSTN dial-in conferencing capabilities are also enabled. However, you can use a dummy dial-in access number. For full Lync 2013 dial-in conference deployment steps, refer to Microsoft's Configuring Dial-in Conferencing.

Lync invitation with conference ID

Start time	<input type="text" value="Tue 4/15/2014"/>	<input type="text" value="5:00 PM"/>
End time	<input type="text" value="Tue 4/15/2014"/>	<input type="text" value="5:30 PM"/>

[→ Join Lync Meeting](#)

Join by phone

[VMR-Number](#) (London, UK)

English (United Kingdom)

[Find a local number](#)

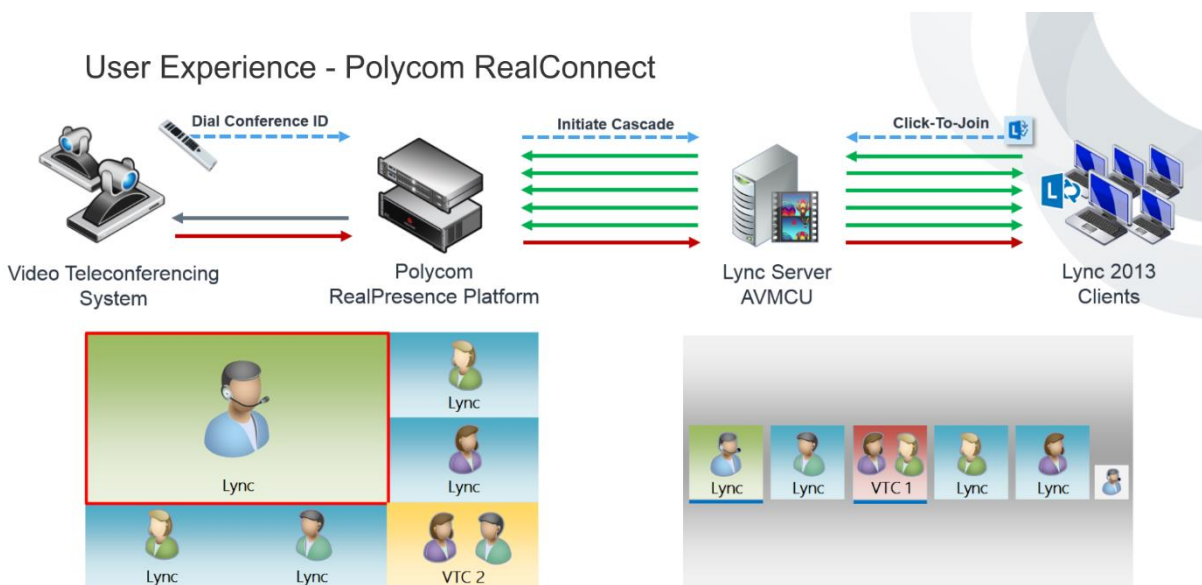
Conference ID: 17894

[Forgot your dial-in PIN?](#) | [Help](#) | [Legal](#)



Polycom RealConnect technology with Lync 2013 provides Lync clients with Microsoft's familiar Gallery View with Lync Application/Desktop Sharing and standards-based video endpoints a Continuous Presence experience on the RealPresence Collaboration Server (RMX). Conferences on RealPresence Collaboration Server (RMX) are bridged or use Polycom RealConnect technology automatically, and up to five of the active Lync 2013 participants display as individual participants on the RealPresence Collaboration Server (RMX) layout. In addition, all participants are joined in a single virtual meeting room which displays video from participants using a standards-based endpoint. This conference scenario is illustrated next.

Polycom RealConnect conference scenario



This Appendix includes the following sections:

- [Deploy Lync Dial-in Conferencing](#)
- [Deploy Polycom RealPresence Collaboration Server \(RMX\) Solution](#)
- [Deploy Polycom ContentConnect Software](#)
- [Configure Your RealPresence DMA System for Lync Server](#)

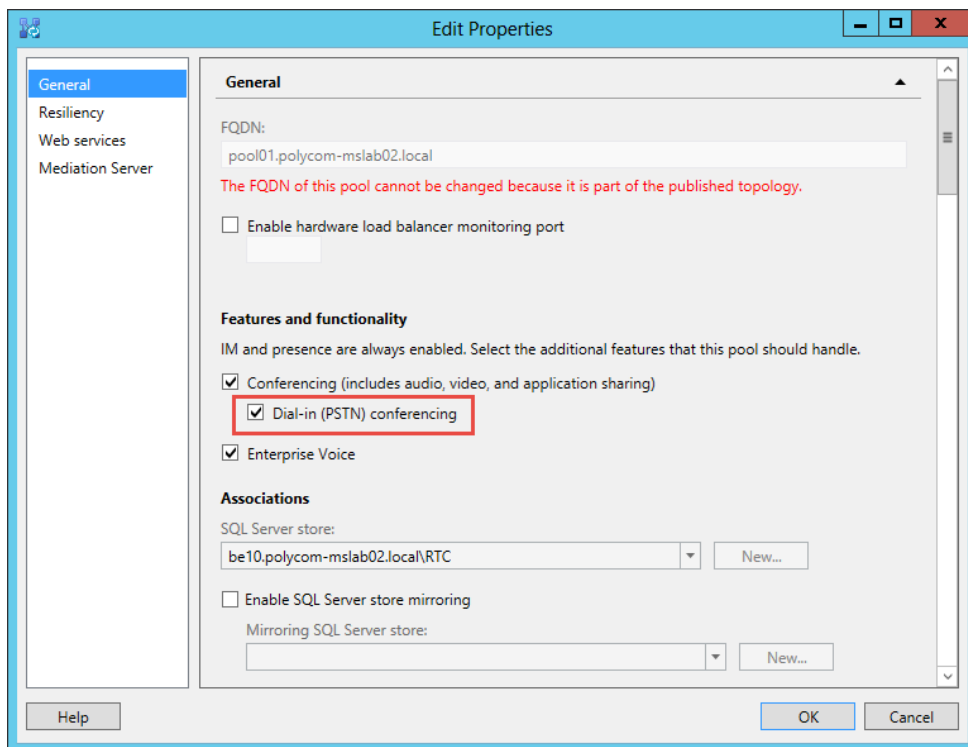
Deploy Lync Dial-in Conferencing

This section is for customers enabling Dial-in Conferencing on Lync Server 2013. If you require more details, refer to [Configuring Dial-in Conferencing](#) on Microsoft TechNet.

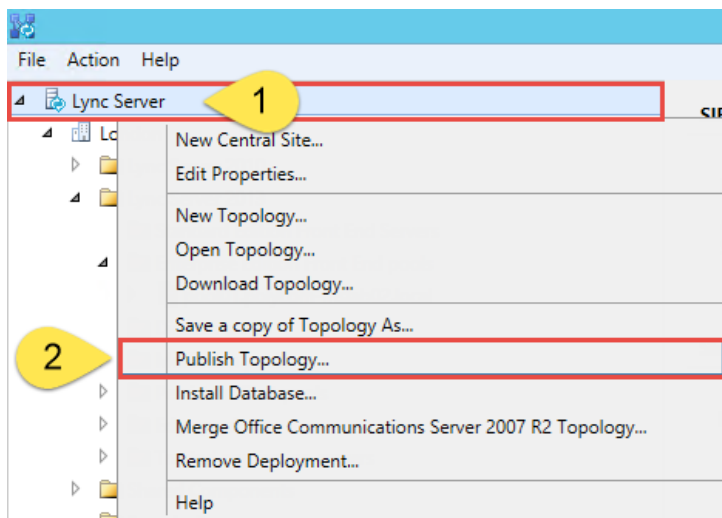
The customer must first enable dial-in conferencing.

To enable Dial-in Conferencing:

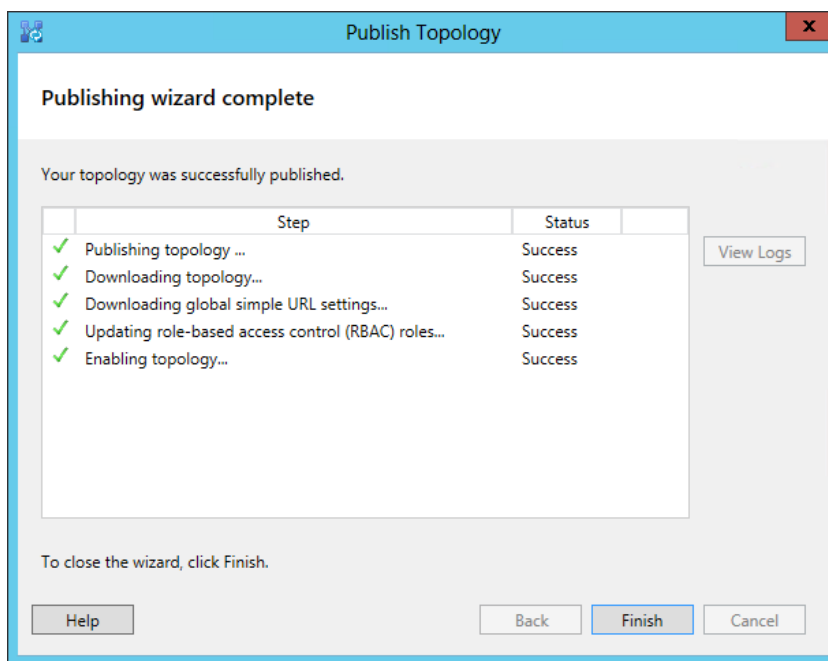
- 1 In the Lync 2013 topology builder, install the dial-in (PSTN) conferencing component for the Lync front end server or pool by going to **Edit Properties > General > Features and Functionality**.
- 2 Select **Dial-in (PSTN) conferencing** and click **OK**.



- 3 Publish the topology by right-clicking the central site name and clicking **Publish Topology > Next > Finish**.



After publication, the output displays, as shown next.

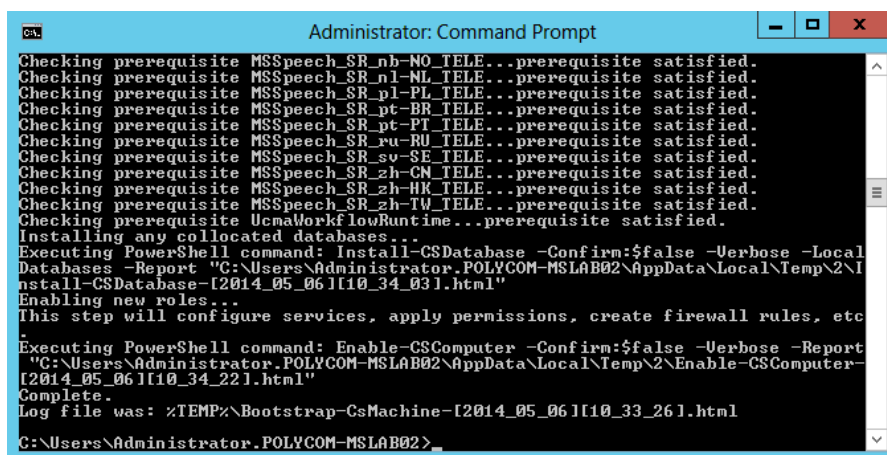


After you change the topology, deploy the application on the Lync Server by running the Lync 2013 bootstrapper process.

To deploy the application:

- 1 On your Lync front end server, open the command prompt and execute the command:

```
%ProgramFiles%\Microsoft Lync Server 2013\Deployment\Bootstrapper.exe
```



- 2 Install the associated service by opening the Lync Server Management Shell and executing Start-CSWindowsService.

Next, ensure that a dial-in conferencing region is configured. Typically, you will need to configure multiple regions and assign local access numbers. In the following example, we add a default region in order to generate an H.323 or standard SIP number that users can dial into from any standards-based room

system. You can choose a naming convention but you must populate the dial-in conferencing region to complete the configuration.

To populate the dial-in conferencing region:

- 1 Open the Lync 2013 Server **Control Panel**, go to **Voice Routing > Edit the Global Dial Plan**, and in Dial-in conferencing region enter a region.

The screenshot shows the 'Edit Dial Plan - Global' dialog box. It has a title bar with 'OK' and 'Cancel' buttons. The 'Scope' is set to 'Global'. The 'Name' field contains 'Global'. The 'Simple name' field contains 'DefaultProfile'. The 'Description' field is empty. The 'Dial-in conferencing region' field is highlighted with a red rectangle and contains 'London, UK'. The 'External access prefix' field is empty. There are help icons next to the 'Dial-in conferencing region' and 'External access prefix' fields.

- 2 Specify a dial-in access number by going to **Lync 2013 Server Control Panel > Conferencing > Dial-in Access Number > New** and completing the following fields:
 - **Display number** This field permits alphanumeric entry. This is typically the dial-in access number. This example uses the VMR or Conference ID and is labelled here as VMR-Number.
 - **Display name** Choose a display name. Typically, this name matches the region.
 - **Line URI** The line URI will not be used as the actual dial-in conference is not being used. This example uses a dummy number tel+111.
 - **SIP URI** This field allocates a SIP address to the Conference Auto Attendant (CAA). This SIP URI is used by the service provider instance of RealPresence Platform to locate and join the corresponding Lync meeting.
 - **Pool** Enter the pool you are enabling for dial-in conferencing.
 - **Primary language** This field is not used for Polycom RealConnect.
 - **Associated Regions** Add the region you created in step 1.

Commit **Cancel**

Display number: *
VMR-Number

Display name:
Conference Dial-in (London)

Line URI: *
tel:+111

SIP URI: *
sip:conf:lonuk @ polycom-mslab02.com

Pool: *
pool01.polycom-mslab02.local

Primary language: *
English (United Kingdom)

Secondary languages (maximum of four):
Add... Remove

Associated Regions *
Add... Remove

Region
London, UK

If the customer wants to customize the meeting invitation, they can add custom footer text to allow meeting participants to join a meeting using a standards-based video endpoint.

- 3 In the Lync 2013 Control Panel, go to **Conferencing > Meeting Configuration**.
- 4 Edit the default global template as shown next.

Custom footer text:

For traditional video meeting participation dial the Lync conference ID from your endpoint, external participants can also join by appending the ID with video.polycom-mslab02.com.

For SIP 123456@video.polycom.com and for H.323 video.polycom.com##123456

This example shows external addresses. If you want to show external addresses, you need to enable standards-based video Firewall traversal using, for example, a RealPresence Access Director.

Your Lync environment now includes Conference IDs in Lync-enabled meeting invitations.

Deploy Polycom RealPresence Collaboration Server (RMX) Solution

This section outlines the steps service providers must complete to integrate Polycom RealPresence Collaboration Server (RMX) solution with Lync Server 2013. You must add a DNS entry, and create and install a security certificate. You also need to add a static route on the Lync Server for the RealPresence Collaboration Server (RMX) solution to use, and enable Lync presence for each RealPresence Collaboration Server (RMX) solution's virtual meeting room that you use.



Note: Use a Lync Server Edge Server to support remote and federated users

If you need to support remote or federated users, your deployment must include a Lync Server 2013 Edge Server.

This section outlines the following tasks required to configure Polycom RealPresence Collaboration Server (RMX) solution with Lync Server 2013. Note that Microsoft Presence is available only with Lync Server 2013.

Complete the following major tasks in order:

- 1 Configure Polycom RealPresence Collaboration Server (RMX) System for Lync Server
- 2 Enable Edge Server Integration with Polycom RealPresence Collaboration Server (RMX) System

Configure Polycom RealPresence Collaboration Server (RMX) System for Lync Server

To begin, you must configure your RealPresence Collaboration Server (RMX) solution for use in a Lync Server environment. This includes setting up your RealPresence Collaboration Server (RMX) solution for SIP, creating security certificates, and ensuring encryption settings.

Complete the following steps:

- [Set up the RealPresence Collaboration Server \(RMX\) System for Security and SIP](#)
- [Create a Security Certificate for the Polycom RealPresence Collaboration Server \(RMX\) System](#)
- [Install the Certificate on your RealPresence Collaboration Server \(RMX\) solution](#)
- [Configure Encryption](#)
- [Configure Lync Server for use with a Polycom RealPresence Collaboration Server \(RMX\) System](#)

Set Up the RealPresence Collaboration Server (RMX) System for Security and SIP

Your RealPresence Collaboration Server (RMX) solution must be accessible via DNS and must be configured for SIP calls.

In this section, complete the following two tasks:

- [Task 1: Configure the RealPresence Collaboration Server \(RMX\) IP Network Service](#)
- [Task 2: Add the RealPresence Collaboration Server \(RMX\) FQDN \(SIP signaling IP address\) in DNS](#)

Task 1: Configure the RealPresence Collaboration Server (RMX) IP Network Service

You must configure the IP network services to include SIP.

To configure the RealPresence Collaboration Server (RMX) IP Network Service:

- 1 Using a web browser, connect to the RealPresence Collaboration Server (RMX).
- 2 In the **RealPresence Collaboration Server (RMX) Management** pane, expand the **Rarely Used** list and click **IP Network Services**.
- 3 In the **IP Network Services** pane, double-click the **Default IP Service** entry.
The Default IP Service - Networking IP dialog opens.
- 4 Make sure the **IP Network Type** is set to **H.323 & SIP** even though SIP will be the only call setup you use with the Lync Server.
- 5 Make sure that the correct parameters are defined for the Signaling Host IP Address, Media Card 1 IP Address, Media Card 2 IP Address (RealPresence Collaboration Server 2000/4000 if necessary), Media Card 3 IP Address (RealPresence Collaboration Server 4000 if necessary), Media Card 4 IP Address (RealPresence Collaboration Server 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 Lync Front End server or Pool name and the server domain name.
- 10 If not selected by default, change the **Transport Type** to **TLS**.

Task 2: Add the RealPresence Collaboration Server (RMX) FQDN (SIP Signaling IP address) in DNS

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

The RealPresence Collaboration Server (RMX) solution and the Lync Server must both resolve the RealPresence Collaboration Server (RMX) host record identically, regardless of the domain you select to store the DNS Host record.

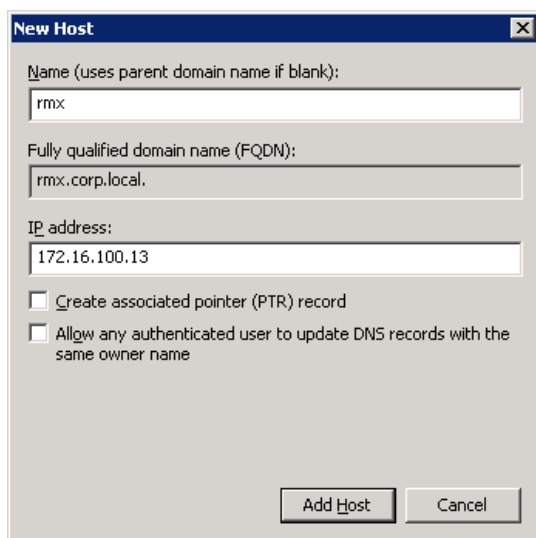
To create a DNS record:

- 1 On the computer where the DNS manager is installed, open the **DNS Manager** and expand the **Forward Lookup Zone**.

- 2 Right-click the appropriate domain zone and select **New Host (A or AAAA)**.

The New Host dialog opens.

- 3 Define the new record. The following figure defines a record using `rmx.corp.local` for the FQDN for the RealPresence Collaboration Server (RMX) SIP signaling domain and 172.16.100.13 as the IP address of the RealPresence Collaboration Server (RMX) signaling host.



- 4 Click **Add Host**.
- 5 Click **OK** to confirm and then click **Done**.

Create and Install a Security Certificate for the Polycom RealPresence Collaboration Server (RMX) System

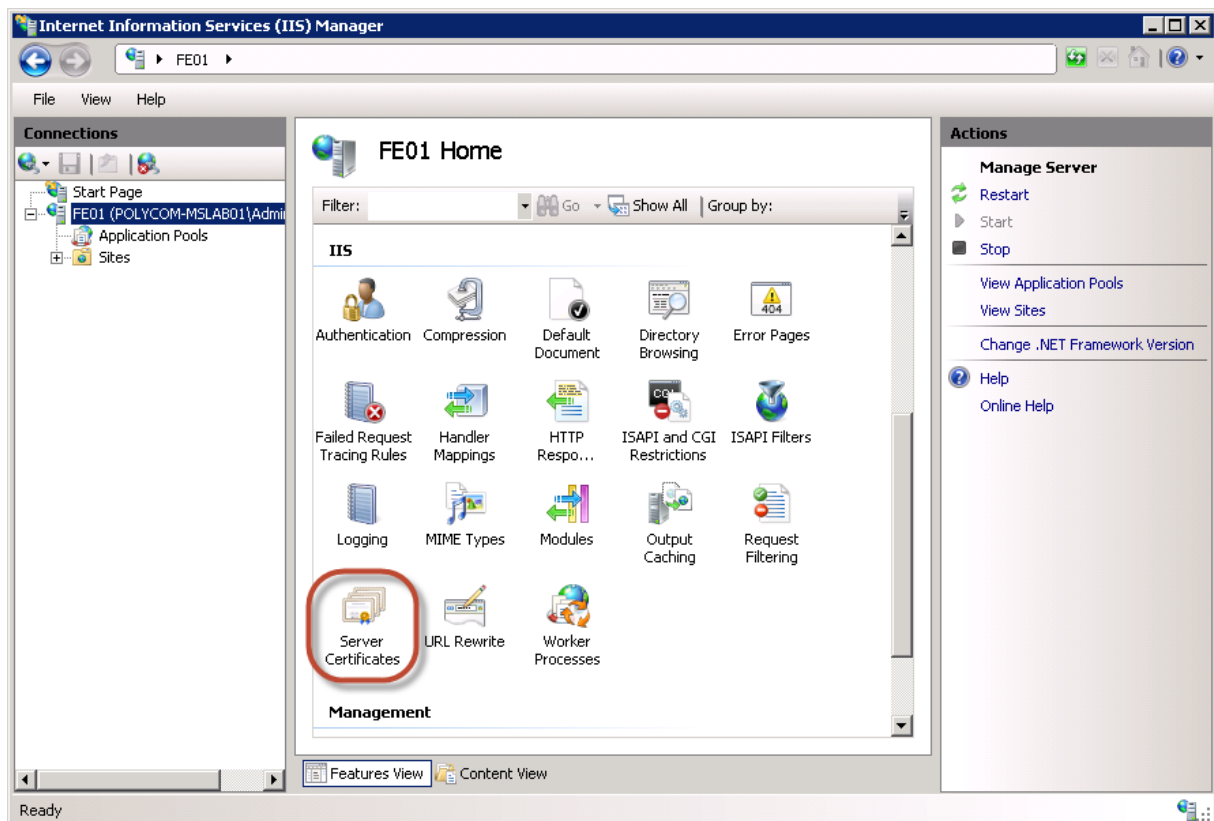
You must install a security certificate on the RealPresence Collaboration Server (RMX) solution so that Lync Server trusts it.

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

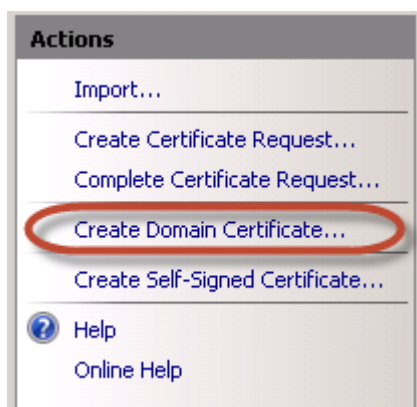
- Purchase and install a certificate from a commercial Trusted Root certificate authority (CA) such as VeriSign or Thawte. Use the procedures in the Polycom RealPresence Collaboration Server (RMX) solution's documentation for certificate management to create a certificate signing request and to install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

To request a security certificate for the Polycom RealPresence Collaboration Server (RMX) solution using IIS Manager 7:

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



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



The Create Certificate wizard displays.

- 5 In the **Distinguished Name Properties** panel, shown next, complete all fields. Do not leave any fields blank.
 - In the **Common Name** field, enter the FQDN of RealPresence Collaboration Server (RMX) SIP signaling interface.

Create Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: rmx.corp.local

Organization: Video Infrastructure

Organizational unit: IT

City/locality: London

State/province: London

Country/region: UK

Previous Next Finish Cancel

- 6 Click **Next**.
 - 7 In the **Online Certification Authority** panel, select a certificate authority from the list and enter a name.
 - 8 Click **Finish**.
- Your certificate is created.

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

- 1 Open **Microsoft Management Console** and add the Certificates snap-in.
 - a Choose **File > Add/Remove Snap-in**.
 - b Select **Certificates** from the Available Snap-ins area and click **Add**.
 - c On the **Certificates snap-in** dialog, select **Computer Account** and click **Next**, as shown next.

Certificates snap-in

This snap-in will always manage certificates for:

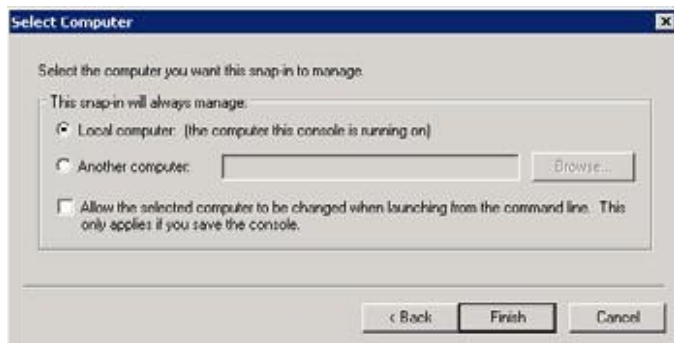
☐ My user account

☐ Service account

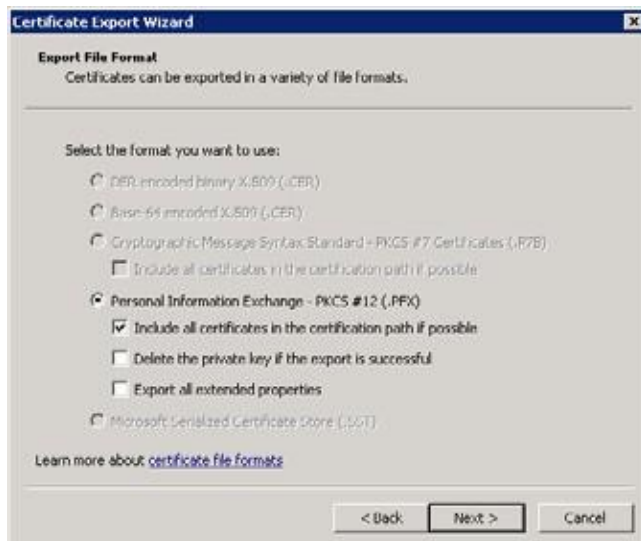
☒ Computer account

Back Next > Cancel

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



- 2 Click **OK**.
- 3 Browse to **Certificates (Local Computer) > Personal > Certificates**.
- 4 Right-click the created certificate and select **All Tasks > Export** to view the Certificate Export wizard.
- 5 In the Certificate Export wizard, do the following:
 - a In the **Export Private Key** panel, select **Yes, export the private key**.
 - b Click **Next**.
 - c In the **Export File Format** panel, select **Include all certificates in the certification path if possible**.



- d Click **Next**.
 - e In the **Password** panel, enter a password. This password cannot include special characters or numbers.
 - f Click **Next**.
- 6 In the **File to Export** panel, enter a path where you want to save the new file, for example, `c:\temp\rmxcert.pfx`.

Install the Certificate on your RealPresence Collaboration Server (RMX) solution

To install the Certificate on Your RealPresence Collaboration Server (RMX) System

- » After the .pfx file is on your computer, you can upload it to the Polycom RealPresence Collaboration Server (RMX) solution and install it, using the procedures in the Polycom RealPresence Collaboration Server (RMX) solution documentation.

Configure Encryption

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

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

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

To change the Lync Server encryption setting:

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

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

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

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

- 3 Verify your encryption settings:

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

Configure Lync Server for use with a Polycom RealPresence Collaboration Server (RMX) System

The Polycom RealPresence RealPresence Collaboration Server 1800/2000/4000/VE systems can host multiple video endpoints in a single conference and host multiple conferences simultaneously. To

accommodate these features, you must configure your RealPresence Collaboration Server (RMX) solution as a trusted application and not as a single user in Lync Server 2013.

Polycom recommends using Lync PowerShell commands to perform the following tasks. For detailed documentation on using Lync PowerShell, see [Microsoft Lync Server Management Shell](#).

**Note: Using domain names**

In Microsoft environments, SIP domains often match the email domain. As an alternative, you can use a separate SIP domain for your Lync Server. Be sure you use the correct domain names when configuring your SIP integration, especially if your primary SIP domain is different from the Active Directory domain for your Polycom devices.

Complete the following tasks to set the Lync routing for the Polycom RealPresence Collaboration Server (RMX) solution:

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

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

To define your trusted application pool:

- 1 Navigate to **Start > All Programs > Microsoft Lync Server2013 > 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, `video.sipdomain.com`.
As a best practice, Polycom recommends configuring this pool to be a multiple computer pool.
- 5 Click **Next** to add computers to this pool.
- 6 In **Define the computers in this pool**, enter the FQDN for the RealPresence Collaboration Server (RMX) SIP signaling domain and click **Add**.
- 7 When finished adding computers, click **Next**.
- 8 Select the appropriate next hop pool and click **Finish**.
- 9 Select **Action > Topology > Publish** to verify and publish your topology changes.

Task 2: Use Lync PowerShell to Create the Trusted Application

This step creates the trusted application using the Lync PowerShell.

To create the trusted application:

- 1 Navigate to **Start > All Programs > Microsoft Lync Server 2013 > Lync Server Management Shell** to open the Lync PowerShell terminal.

- 2 Use the `New-CsTrustedApplication` command to set up a trusted application for the RealPresence Collaboration Server (RMX) solution.

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

The parameters are defined as follows:

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

-trustedApplicationPoolFQDN The FQDN of the application pool, in this example, `video.sipdomain.com`.

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

For more information about the `New-CsTrustedApplication` command see Microsoft Lync [New-CsTrustedApplication](#).

- 3 Use the `New-CsTrustedApplicationEndpoint` command to set up a trusted application endpoint for the RealPresence Collaboration Server (RMX) solution.

```
New-CsTrustedApplicationEndpoint -SipAddress sip:video@sipdomain.com -
ApplicationId video -TrustedApplicationPoolFqdn video.sipdomain.com
```

The parameters are defined as follows:

-SipAddress An internal SIP address used by RealPresence Collaboration Server (RMX) for ICE.

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

For more information about the `New-CsTrustedApplicationEndpoint` command see Microsoft Lync [New-CsTrustedApplication](#).

**Settings: Creating the trusted application**

When creating your trusted application:

- Add all RealPresence Platform Trusted Servers within the same Trusted Application Pool
- Ensure that the Trusted Application Pool FQDN and Trusted Application Endpoint URI share the same name
- Ensure that the Trusted Application '-applicationId' uses the same suffix, shown as 'video' is the example in step 2

Task 3: Use Lync PowerShell to Update the Topology

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

To update the topology:

- 1 Navigate to **Start > All Programs > Microsoft Lync Server 2013 > Lync Server Management Shell** to open the Lync PowerShell terminal.

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

`Enable-CsTopology`

Enable Edge Server Integration with Polycom RealPresence Collaboration Server (RMX) System

Before enabling Edge Server integration with your RealPresence Collaboration Server (RMX) solution, you must configure the RealPresence Collaboration Server (RMX) SIP signaling domain as a trusted application.

When your RealPresence Collaboration Server (RMX) solution is configured with a Microsoft Edge Server, the following Microsoft features are available for your RealPresence Collaboration Server (RMX) solution:

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



Note: Federation and CAC require Lync Server or Edge Server support

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

Required Ports

This section lists RealPresence Collaboration Server (RMX) firewall port requirements when deployed with Lync Server. Signalling is as follows:

- **Call Signaling** External Lync participant <> Firewall <> Lync Edge <> Lync Front-end <> DMA <> RMX Signalling IP <> DMA <> Lync Front-end <> Lync Edge <> Firewall <> External Lync Participant.
- **Media** External Lync participant <> Firewall <> Lync Edge <> RMX Media IP <> Lync Edge <> Firewall <> External Lync Participant.

The following table lists port requirements for Lync to Collaboration Server (RMX).

Microsoft Required Ports

Connection type	Collaboration Server (RMX) Ports	Lync Server	Lync Ports	Protocol	Use
ICE	49152 – 65535; 20000 – 35000	Lync Edge Server Internal network interface controller (NIC)	3478	STUN/TURN over UDP	ICE
ICE	49152 – 65535; 20000 – 35000	Lync Edge Server Internal network interface controller (NIC)	443	STUN/TURN Over TCP	ICE

Set Up a Microsoft Edge Server for the Polycom RealPresence Collaboration Server (RMX) System

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

- Enable the firewall for UDP.
- Provide the RealPresence Collaboration Server (RMX) solution with a unique account when you create the Trusted Application Endpoint and register it with Edge Server.
- Set up a TLS connection.
- Ensure that the RealPresence Collaboration Server (RMX) solution SIP signaling domain has been allowed on the Edge Server you are federating to (if your deployment does not include a RealPresence DMA system).

To set up a Microsoft Edge Server with the Polycom RealPresence Collaboration Server (RMX) solution and support Microsoft CAC policies, complete the following tasks:

Task 1: Obtain the Trusted Application Service GRUU Identification

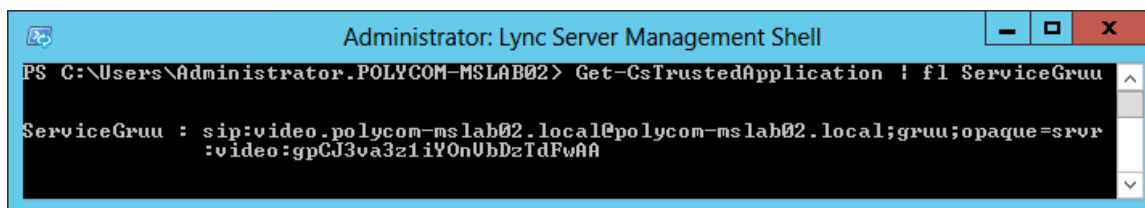
This task shows you how to use Lync PowerShell to obtain the service GRUU for your Polycom RealPresence Collaboration Server (RMX) solution.

If you are deploying multiple RealPresence Collaboration Servers, the Globally Routable User Agent URI (GRUU) information can be shared as long as the existing Trusted Application Pool and Application ID are used.

To obtain the service GRUU identification:

- 1 Navigate to **Start > All Programs > Microsoft Lync Server 2013 > Lync Server Management Shell** to open the Lync PowerShell terminal.
- 2 Use the `Get-CsTrustedApplication` command to display the service GRUU information for the RealPresence Collaboration Server (RMX) solution, and make note of the information.

```
Get-CsTrustedApplication | fl ServiceGruu
```



Note: You must enable Interactive Connectivity Establishment (ICE)

Prior to this release, creating an account in Active Directory was necessary only for Lync deployments with an Edge Server deployed to facilitate federated or remote worker calling. As of this release, you must enable ICE with or without Edge Server deployments.

Task 2: Configure RealPresence Collaboration Server (RMX) System Flags

This section shows you how to configure system flags for the RealPresence Collaboration Server (RMX).

To configure system flags:

- 1 Enable the following system flags on the RealPresence Collaboration Server (RMX) solution:
MS_ENVIRONMENT=YES
- 2 Create a new flag named:
SIP_CONTACT_OVERRIDE_STR
- 3 Configure the service GRUU information obtained in Task 1 without the prefix *sip:*. For example, use:
video.polycom-mslab02.local@polycom-
mslab02.local;gruu;opaque=svr:video:gpCJ3va3z1iYOnVbDzTdFwAA

Task 3: Configure the RealPresence Collaboration Server (RMX) System for Edge Server Support

This section shows you how to configure the RealPresence Collaboration Server (RMX) for Lync Edge Server.

To configure the RealPresence Collaboration Server (RMX) for Edge Server support:

- 1 In the **RealPresence Collaboration Server (RMX)** web browser, in the **RealPresence Collaboration Server Management** pane, expand the **Rarely Used** list and click **IP Network Services**.
- 2 In the **IP Network Services** pane, double-click the **Default IP Network Service** entry.
The Default IP Service - Networking IP dialog opens.
- 3 Click the **SIP Advanced** tab.

- 4 In the **Server User Name** field, enter the SIP URI that you defined for the TrustedApplicationEndpoint, for example, `video`, as shown next.



- 5 In the **ICE Environment** field, select **MS** for Microsoft ICE implementation.
- 6 Click **OK**.

Task 4: Monitor the Connection to the Session Traversal Utilities for NAT (STUN) and Relay Servers in the ICE Environment

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

To monitor the ICE connection:

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

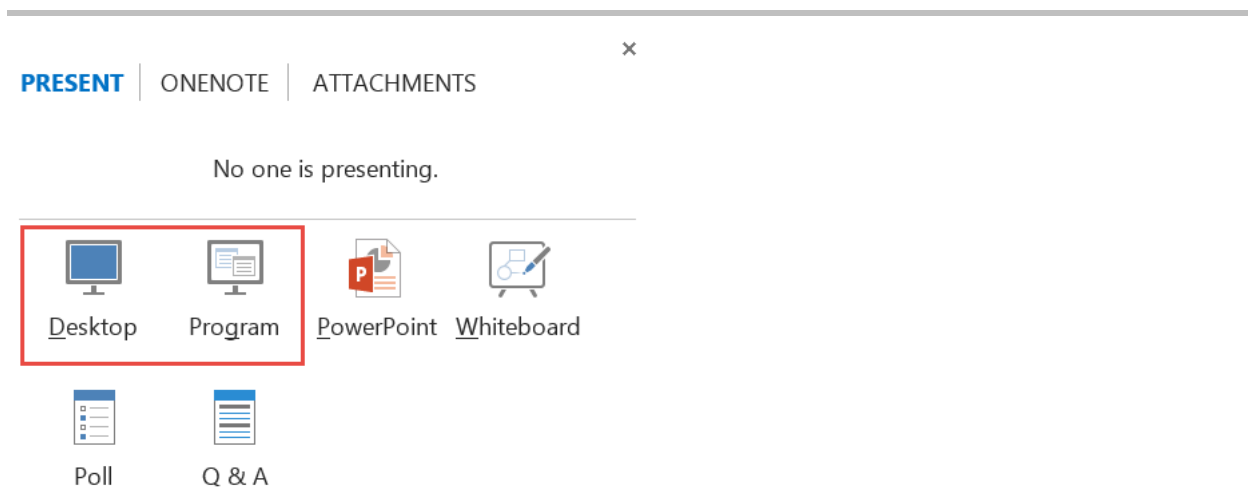
The system lists the ICE servers it is connected to, the connection status, and the status of the firewall detection in the RealPresence Collaboration Server (RMX) solution.

Deploy Polycom ContentConnect Software

This section explains how to configure Polycom ContentConnect software solution components with Microsoft Lync. You'll also learn how to set up Polycom ContentConnect and enable for Gateway Mode.

Polycom ContentConnect software v1.5 operates by default in Gateway Mode. Gateway Mode enables the Polycom ContentConnect software server to work as an RDP-BFCEP content gateway, fully transcoding RDP and BFCEP H.264 content streams.

Because Gateway Mode facilitates RDP-BFCEP transcoding, not all Lync sharing modalities are supported. When sharing content via Lync, you must use either Desktop or Program sharing.



Required Components

The following table lists required components that must be set up in your environment before you deploy Polycom ContentConnect software with Lync Server. Note that to support remote access for standards-based video endpoints, you will require either a RealPresence Access Director or Acme Packet Net-Net Enterprise Session Director (ESD). For Lync clients, only a Lync Edge server is required.

Required Polycom ContentConnect software components for Microsoft Lync

Component
Management Systems and Recorders Microsoft Active Directory Server
Gatekeepers, Gateways, and MCUs Microsoft Lync Server 2013 Polycom RealPresence Distributed Media Application (DMA) 7000 (6.2 or higher) Polycom RealPresence Collaboration Server (RMX) Software MCU/1500/1800/2000/4000 (8.5 or higher)
Microsoft Endpoints Gateway Mode Microsoft Lync Client installed on Windows, Mac, mobile platforms (iOS, Android, Windows), and Lync Room Systems.
Video Endpoints Your environment requires one or more video endpoints that receive content from RealPresence Collaboration Server (RMX). For more information on interoperability, see the Interoperability Tables section in the RealPresence Collaboration Server (RMX) Software MCU/1500/1800/2000/4000 Release Notes at Collaboration & Conferencing Platforms .
Polycom ContentConnect Software Product Component VMware or Hyper-V software, the host of the Polycom ContentConnect OVA-formatted Virtual Appliance Software Installation Package/VHD-Formatted Virtual Appliance Software Installation Package.

Optional Components

The following table lists optional and compatible components that you can install and set up before you deploy Polycom ContentConnect software with Lync Server.

Optional Polycom ContentConnect software components for Microsoft Lync

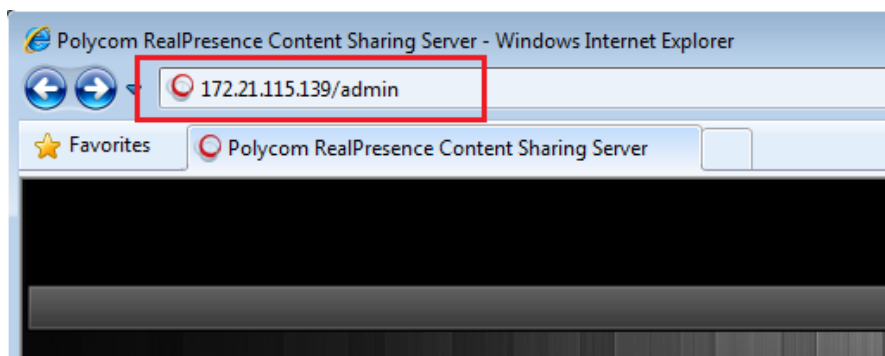
Component
Firewall, Border Controllers Lync Edge Server Polycom RealPresence Access Director Acme Packet® Net-Net Enterprise Session Director (ESD)
Recorders Polycom RSS 4000 solution or RealPresence Capture Server
Load Balancers Polycom has tested the following load balancer: F5 BIG-IP LTM 1600 and BIG-IP 10.2.1.297.0

Access and Use the Polycom ContentConnect Server Web Configuration Tool

This section shows you how to access the Content Sharing Server Web Configuration Tool, and use it to configure the Content Sharing Server.

To access the Content Sharing Server Web Configuration Tool:

- 1 Launch a web browser and enter **<IP address of the Content Sharing Server>/admin** in the address bar as shown next. For example, enter 172.21.115.139/admin, where 172.21.115.139 is the IP address of the Content Sharing Server.



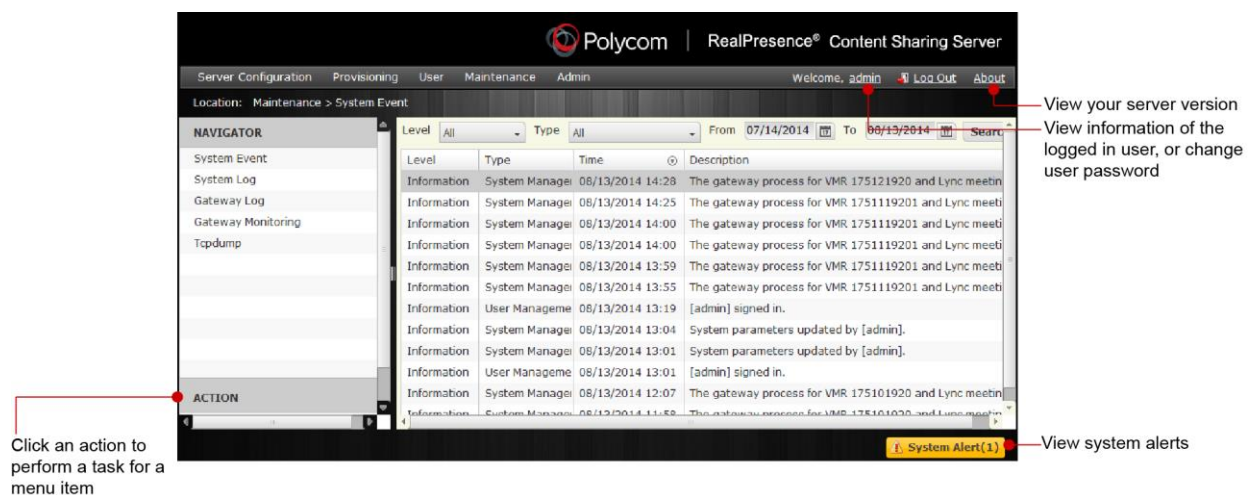
- 2 Press **Enter**.

The Content Sharing Server Web Configuration Tool **Log In** screen displays.

- 3 Enter your **User ID** and **Password**, and click **Log In**. The default login credential for both user ID and password is admin.

The Content Sharing Server Web Configuration Tool screen displays.

The Content Sharing Server Web Configuration Tool has a primary menu bar with five main menus: Server, Provisioning, User, Report, and Admin. Selecting a menu reveals additional submenus as shown next. Under the primary menu bar is additional navigation information, to let you know which menu item you're currently configuring.



Each page of the Content Sharing Server Web Configuration Tool also displays the following items:

- User ID, **Log Out**, and **About** display on the top right. Click each to do the following:
 - Click the user's ID to view information about the currently logged-in user (in this case, *admin*, and to change the user's password.
 - Click **Log Out** to log out of the Content Sharing Server Web Configuration Tool and return to the **Log In** screen.
 - Click **About** to display the version of the RealPresence Content Sharing Server.
- At the bottom-right of the screen is an alert to let you know if there are any important messages. Click **System Alert** to view these messages.
- On the far left of the screen, a list of actions display that enable you to perform specific tasks. For example, depending on the menu item you're configuring, you may be able to create, refresh, edit, export, clear, import, delete, or update items or settings.

Configure the Content Sharing Server Using the Content Sharing Server Web Configuration Tool

To configure the Content Sharing Server for Gateway Mode, you need to configure server information. RealPresence Access Director is required for standards-based video room systems requiring remote content sharing capabilities.

Configure Polycom ContentConnect Software Server Running Mode

Polycom ContentConnect software server works in two modes:

- Gateway Mode
 - Note that you must set Polycom ContentConnect to Gateway Mode if you are using Polycom RealConnect technology. If you are direct dialing to RealPresence Platform, you must set Polycom ContentConnect to Add-On Mode. Lync clients don't need to install the Polycom RealPresence Content Add-on for Lync Service for content sharing.
 - Polycom ContentConnect software server works as an RDP - BFCP content gateway, providing full transcoding between RDP and BFCP H.264 content streams.
- Add-On Mode
 - All Lync clients must install the Polycom RealPresence Content Add-on for Lync Service for content sharing.
 - The add-on handles content sharing when there is legacy participant with BFCP content supported in the conference.
 - Content media is BFCP H.264 video stream and goes directly through RealPresence Collaboration Server (RMX) from the Polycom ContentConnect software plugin.

**Note: This guide focuses on Gateway Mode deployment**

This guide focuses on the deployment steps required for Gateway Mode and does not address Add-on Mode.

To configure Polycom ContentConnect software server running mode:

- 4 From the RealPresence Content Sharing Server Web Configuration Tool, select **Server Configuration > Running Mode**.
- 5 Select a running mode:
 - Gateway Mode

If you select this option and you have the **Polycom RealPresence Content Add-on for Lync Service** installed already, it will be disabled.
- 6 Click **Save**.

**Note: Only H.264 content is supported on legacy endpoints in the Gateway mode**

In this release, only H.264 content is supported on legacy endpoints in the Gateway mode.

Configure Server Information

You can configure a SIP server and load balancer server to work with the Polycom ContentConnect software server.

To configure server settings:

- 1 Log in to the Content Sharing Server Web Configuration Tool.
- 2 Select **Server Configuration > Server**.

3 Enter the following information:

- **SIP Server Address** The IP address or host name of the RealPresence DMA system.
- **SIP Server Administrator User** The user name of a RealPresence DMA system administrator.
- **SIP Server Administrator Password** The password of a RealPresence DMA system administrator.
- **SIP Proxy Port** The RealPresence DMA system port number.
- **SIP Registrar Port** The RealPresence DMA system registrar port.
- **SIP Domain Suffix** The SIP domain suffix. This must be the same value you entered in the destination network field for the SIP Peer defined for Lync on RealPresence DMA system. This setting is not required for Polycom ContentConnect.
- **SIP Authorization Name, SIP Password** SIP authentication credentials created in RealPresence DMA system (if RealPresence DMA system needs to authenticate Polycom ContentConnect software Gateway).
- **Call Rate** The call rate for the SIP call with RealPresence Collaboration Server (RMX).
- **SIP Transport Protocol** The transport protocol to be used for the SIP call.
- **Media Encryption** Whether to enable media encryption. If you select **Auto**, the SIP server decides whether or not to enable media encryption.
- **Media Transport Port Range** The port range allocated for media transmission.
- **F5 Virtual Server Address** Load Balancer virtual server address.

4 Click **Save**.

The following illustrates an example Gateway Mode configuration.

Gateway Mode configuration example

▼ Server Configuration

The server is running in "Gateway Mode" now.

SIP Server Address *	<input type="text" value="192.168.1.100"/>	
SIP Server Administrator User *	<input type="text" value="admin"/>	
SIP Server Administrator Password *	<input type="password" value="*****"/>	
SIP Proxy Port *	<input type="text" value="5061"/>	1 ~ 65535
SIP Registrar Port *	<input type="text" value="5061"/>	1 ~ 65535
SIP Domain Suffix	<input type="text" value="sipdomain.com"/>	
SIP Authorization Name	<input type="text"/>	
SIP Password	<input type="password" value="*****"/>	
Call Rate *	<input type="text" value="1024"/>	kbps
SIP Transport Protocol *	<input type="text" value="TLS"/>	
Media Encryption *	<input type="text" value="AUTO"/>	
Media Transport Port Range *	<input type="text" value="33300"/> - <input type="text" value="43300"/>	1 ~ 65535
F5 Virtual Server Address	<input type="text"/>	

Make sure your SIP Proxy Port, SIP Registrar Port, and SIP Transport Protocol settings match corresponding settings in your SIP Server.

Configure Your RealPresence DMA System for Lync Server

Complete the five tasks in this section to configure a RealPresence DMA system with Lync Server.

Ensure DNS is Configured Properly

To configure DNS properly, ensure that:

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

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

Create a Security Certificate for the RealPresence DMA 7000 System

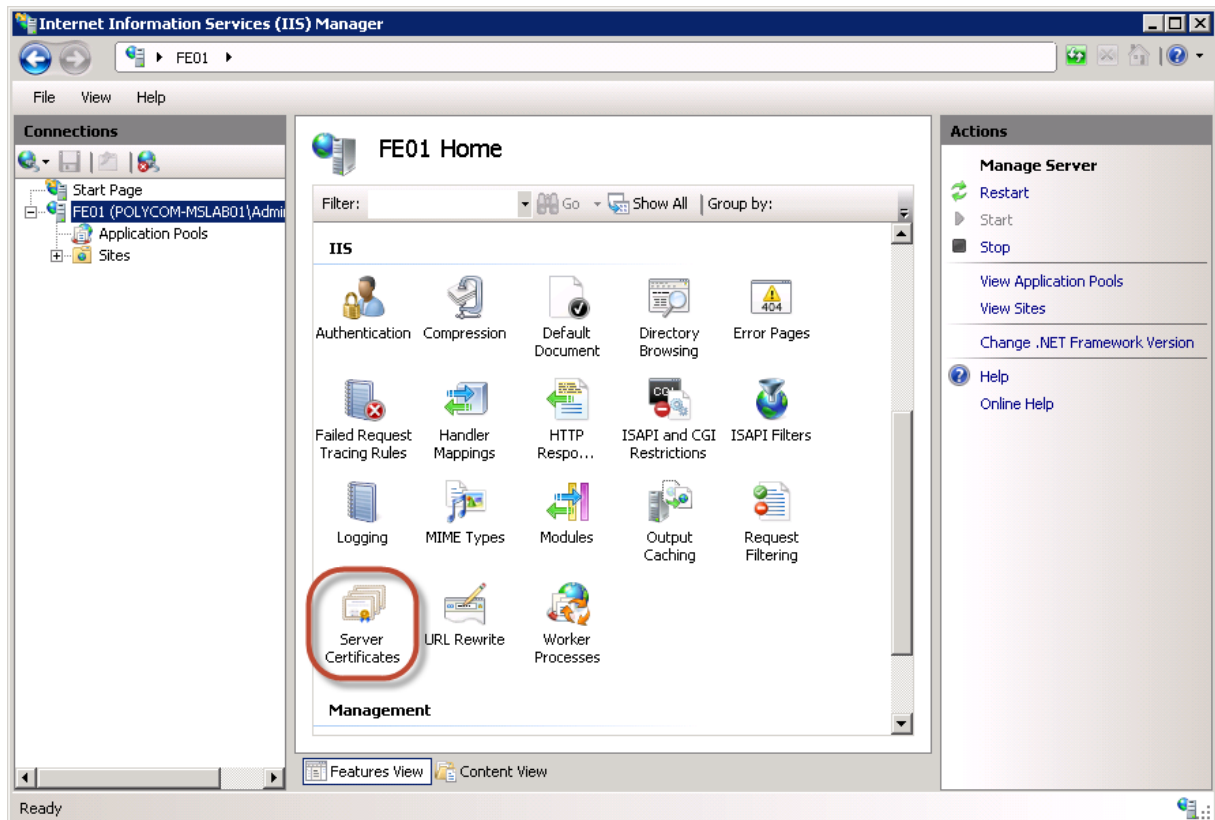
The second step in configuring a RealPresence DMA system with Lync Server is to install a security certificate on the RealPresence DMA system so that Lync Server trusts it. You can purchase or install a certificate or request and obtain a certificate from your enterprise CA, as explained next:

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

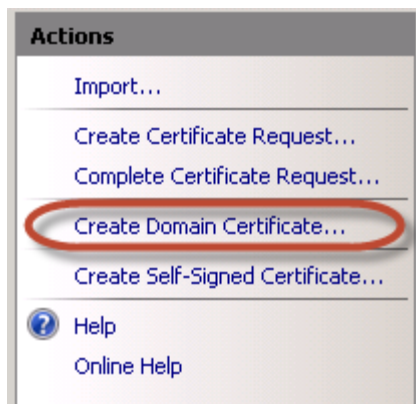
To create a security certificate for the RealPresence DMA system using IIS Manager 7:

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

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



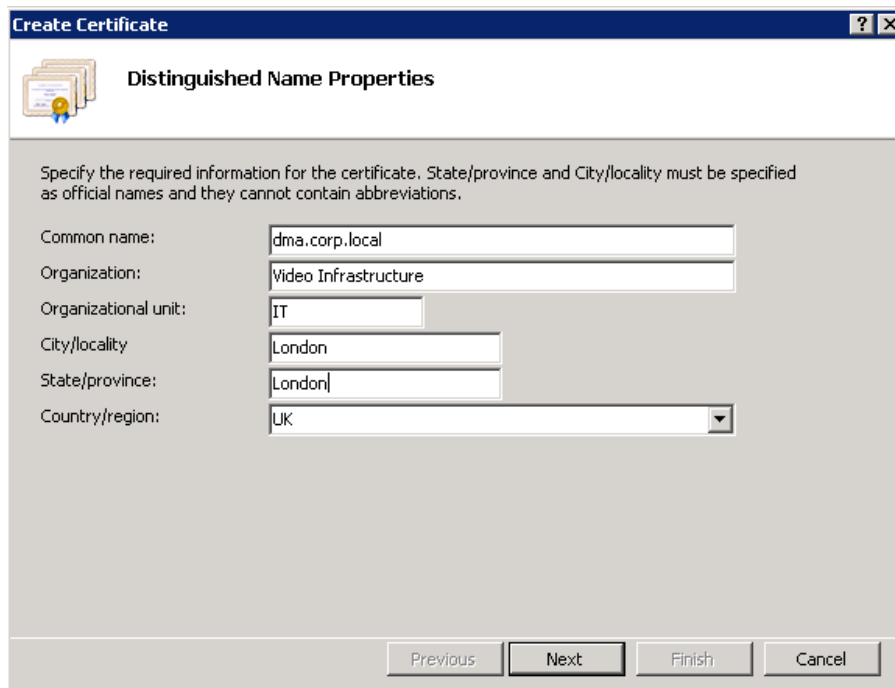
- 4 In the **Actions** pane (far right), select the **Create Domain Certificate**, shown next.



The **Create Certificate** wizard displays.

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

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



The image shows a Windows dialog box titled "Create Certificate" with a sub-header "Distinguished Name Properties". It contains a text area with instructions: "Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations." Below this are several input fields: "Common name:" with the value "dma.corp.local", "Organization:" with "Video Infrastructure", "Organizational unit:" with "IT", "City/locality" with "London", "State/province:" with "London", and "Country/region:" with a dropdown menu showing "UK". At the bottom are four buttons: "Previous", "Next", "Finish", and "Cancel".

6 Click **Next**.

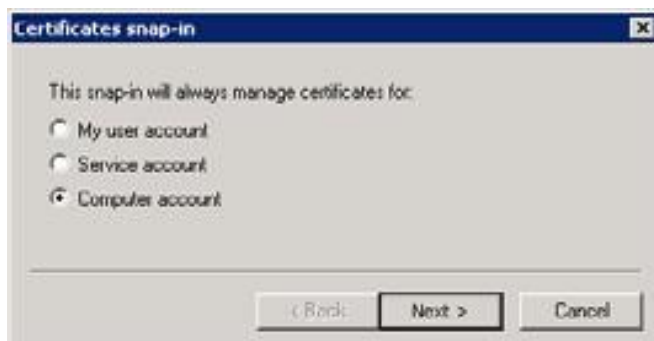
7 In the **Online Certification Authority** panel, select a Certificate authority from the list and enter a name that you can easily identify, for example, RealPresence DMA certificate.

8 Click **Finish**.

You have created the certificate.

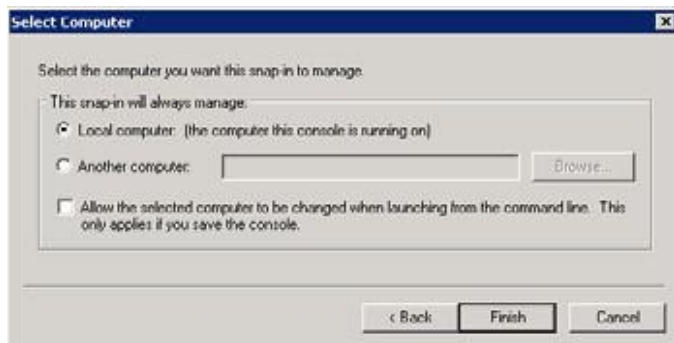
To use the Microsoft Management Console to export the created certificate:

- 1 Open **Microsoft Management Console**. Add the **Certificates snap-in** if it has not been added already.
 - a Choose **File > Add/Remove Snap-in**.
 - b Select **Certificates** from the **Available Snap-ins** area and click **Add**.
 - c On the **Certificates snap-in** dialog, select **Computer Account** and click **Next**.



The image shows a Windows dialog box titled "Certificates snap-in". It contains a text area with the instruction: "This snap-in will always manage certificates for:". Below this are three radio button options: "My user account", "Service account", and "Computer account", with "Computer account" selected. At the bottom are three buttons: "Back", "Next >", and "Cancel".

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



- e Click **Finish**.

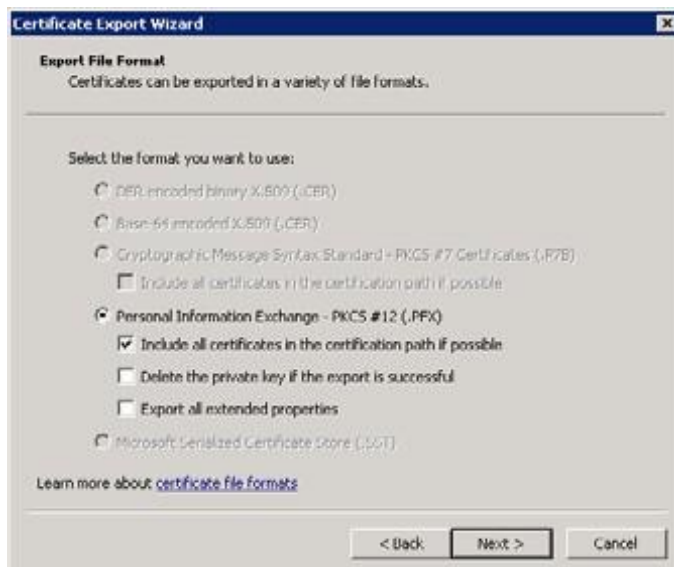
- 2 Click **OK**.

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

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

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

- a In the **Export Private Key** panel, select **yes, export the private key**.
- b Click **Next**.
- c In the **Export File Format** panel, shown next, select the option **Include all certificates in the certification path if possible**.



- d Click **Next**.

- e In the **Password** panel, enter a simple password.

- f Click **Next**.

- 6 In the **File to Export** panel, enter a path where you want to save the new file, for example, `c:\temp\dmacert.pfx`.
- 7 Once the `.pfx` file is on your computer, you can upload it to the RealPresence DMA system and install it, using the procedures in the RealPresence DMA system's online help for Certificate Management.

Configure a RealPresence DMA System SIP Peer for Lync Server

In the RealPresence DMA system, configure Microsoft Lync Server as an external SIP peer. This allows SIP calls routed from the RealPresence DMA system to reach devices registered to the Lync Server.

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

- 1 Log into the RealPresence DMA system.
- 2 Navigate to **Network > External SIP Peers**.
- 3 In the **Actions** menu, click **Add**.

The Add External SIP Peer dialog displays, shown next.

Edit External SIP Peer

☒ Enabled

Name: Lync Pool *

Description: Lync Front End or Pool Name

Type: Microsoft

Next hop address: lyncpool.corp.local *

Destination network: sipdomain.com *

Port: 5061

Transport type: TLS

Use route header: ☐

Downgrade: ☒ Downgrade "sips:" to "sip:" if TLS is not supported by this SIP peer.

Prefix range:

Strip prefix: ☐

Register externally: ☐

Supports SIP OPTIONS ping: ☐

OK Cancel Help

- 4 Ensure that **Enabled** is selected.
- 5 Type a name and description for the SIP Peer.
- 6 In the **Next hop address** field, type the FQDN address of the Microsoft Lync Server Front End Pool.

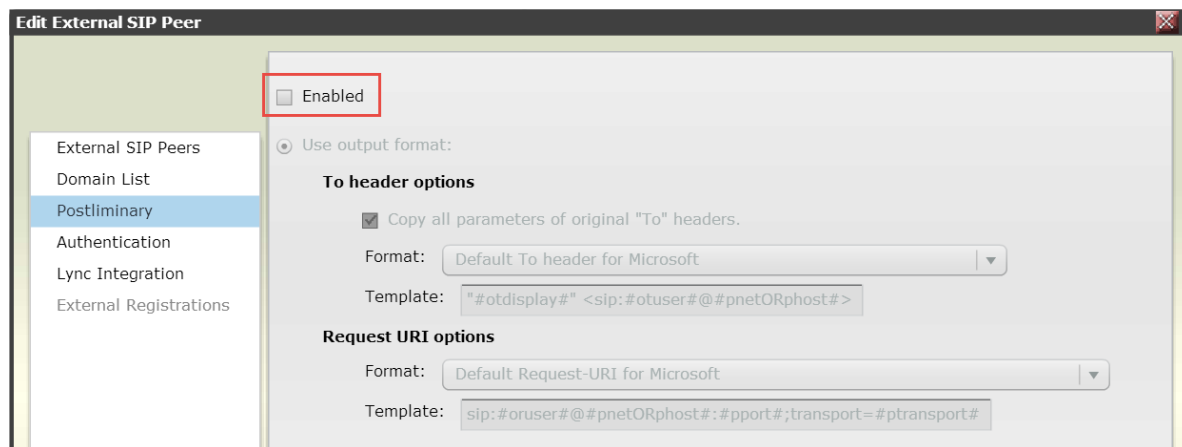
- 7 In the **Destination network** field, enter the SIP domain used for Polycom RealConnect conferences. This is not the domain extension for your Lync Front End Server or your Pool.
- 8 In the **Port** field, enter the SIP port to use. Lync typically is configured to use the SIP port 5061.
- 9 Leave **Use route header** unchecked.
- 10 Leave the Prefix range field blank.

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

- 11 In the **Type** drop-down list, select **Microsoft**.
- 12 In the **Transport Type** drop-down list, select **TLS**.
- 13 Go to the **Lync Integration** tab, check **CsTrustedApplication ServiceGruu**, and enter the GRUU information you obtained in the section [Task 1: Obtain the Trusted Application Service GRUU Identification](#) into the **CsTrustedApplication ServiceGruu** field. Note that in the example shown next, unlike Collaboration Server (RMX), the 'sip:' comment needs to be included.
- 14 Click **OK**.

The RealPresence DMA system can now route outgoing SIP calls to endpoints registered to the Microsoft Lync server.

Note that for Polycom DMA system v6.3, the postliminary configuration for the SIP peer is not the same as for Polycom DMA system 6.2. As shown in the following illustration, do not enable the preliminary script, which by default handles the Polycom ContentConnect gateway.



Next, complete the Lync 2013 and RealPresence DMA system integration. The following steps assume that you have created a security certificate, as shown in [Create a Security Certificate for the Polycom DMA 7000 System](#).

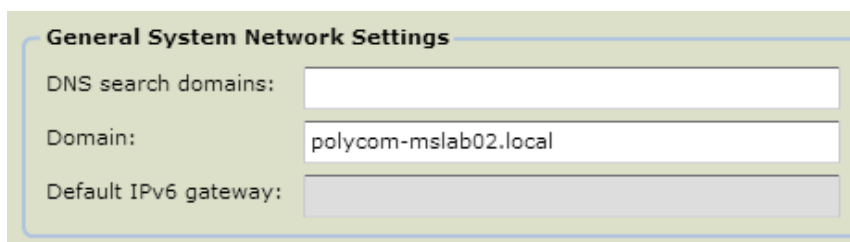
Configure RealPresence DMA system network settings to match the Lync Server, specifically, Time and Domain. You need to configure the domain to match the extension you gave to the RealPresence DMA system DNS name.

Specify a Domain and Time on the RealPresence DMA System

Next, specify domain and time on the RealPresence DMA system.

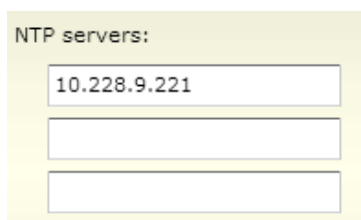
To specify domain and time on the RealPresence DMA system:

- 1 From the DMA administrator screen go to **Local Cluster > Network Settings > General System Network Settings**.



The screenshot shows the 'General System Network Settings' configuration page. It contains three input fields: 'DNS search domains' (empty), 'Domain' (filled with 'polycom-mslab02.local'), and 'Default IPv6 gateway' (empty).

- 2 Configure the time to synchronize with the same source as the Lync Server, typically one of your domain controllers, by going to **Local Cluster > Time Settings**. Specify an IP address for your time server, as well as a time zone.



The screenshot shows the 'NTP servers' configuration page. It contains three input fields for NTP server IP addresses. The first field is filled with '10.228.9.221', and the other two are empty.

Configure the RealPresence DMA System Lync Dial Rule

Next, service providers must create a conference template that is assigned to Polycom RealConnect Lync conferences.

In multiple tenant scenarios, the DMA maintains a prefix table, in which each Federated organization is allocated a unique 2-digit prefix, mapped to the respective organization initiating the meeting by its Conference Auto Attendant (CAA) SIP URI.

In single tenant scenarios, since the conference ID, is unique only within the Lync server which allocated it, a prefix is added to the conference ID to enable the DMA to identify remote Polycom RealConnect Lync conferences.

The Lync service administrator of an organization hosting Lync meetings, can add the respective organization prefix into the Outlook meeting invites sent by meeting organizers. This insertion requires the Lync service administrator to configure the added text only once, via the Lync conference template, at the point of the Polycom RealConnect service deployment.

To create a conference template:

- 1 Set **Conference mode** to **AVC only**. Mixed mode is not supported.

- 2 Enable the dial rule on RealPresence DMA system by going to the **DMA administrator screen > Call Server > Dial Rules**.

The Description field displays *Dial to Polycom RealConnect Conference*.

- 3 Highlight **Dial by Lync conference ID** and select **Edit**.
- 4 Select **Enabled** to enable both the rule and the Conference template created in the previous step.
The available SIP peer(s) you assigned displays in Selected SIP peers.
- 5 Click **OK**.
Polycom RealConnect configuration is complete.



Note: Define a specific MCU pool order

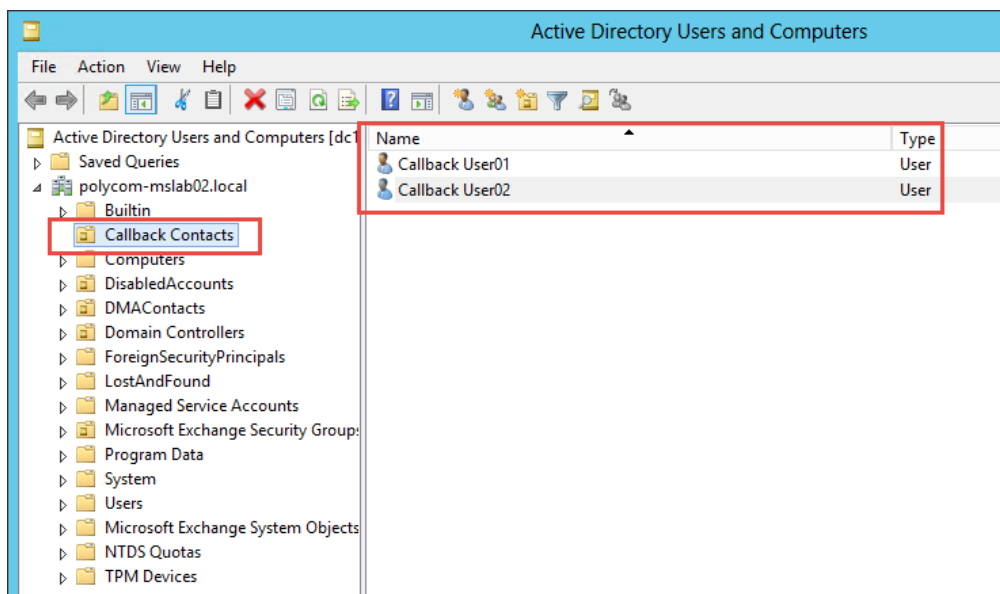
As of RealPresence DMA system 6.2 you have the option to define a specific MCU pool order.

Configure the Directory Server and Domain

Next, configure the directory server and domain using the Active Directory domain and not the SIP domain.

To configure the directory server and domain:

- 1 If you are deploying an external Lync system, configure a 'Callback contacts' Active Directory Organizational Unit that contains Lync-enabled contacts that establish federated Lync conferences. The following example illustrates a container created from the root domain `Polycom-mslab02.local`.



- 2 Enable callback Lync accounts for telephony between computer endpoints and enable dial out via federation.

The screenshot shows the 'Display name' configuration page for a Lync user. The 'Display name' field is set to 'Callback User01'. The 'Enabled for Lync Server' checkbox is checked. The 'SIP address' field is set to 'sip:Callback.User01' and the domain dropdown is set to 'polycom-mslab02.com'. The 'Registrar pool' field is set to 'pool01.polycom-mslab02.local'. The 'Telephony' dropdown is set to 'PC-to-PC only'.

- 3 Configure the following container within the Active Directory Integration page on the DMA system.

The screenshot shows the 'Lync RealConnect' configuration page. The 'Callback contacts OU' checkbox is checked, and the text field next to it contains 'ou=Callback Contacts'. Below the configuration area are two buttons: 'Update' and 'Restore Defaults'.

Accounts located within the container are automatically allocated to MCUs by the DMA system when you initiate the dial rule.

4 Go to **Admin > Integrations > Microsoft Active Directory**.

Active Directory Connection

Directory Server

☒ Auto-discover from FQDN: polycom-mslab02.local *

☐ IP address or host name: [Empty]

Domain: polycom-mslab02.local

Domain\user name: polycom-mslab02\Administrator *

Password: ***** *

User LDAP filter: (!(userAccountControl:1.2.840.113556.1.4.803:=2))

Base DN: All Domains



Troubleshooting: Log in and dial to confirm

Log into one of the callback user accounts in Lync and ensure you can dial each customer's conference auto attendant via federation.

Next, configure the connection to the customer's federated Lync deployment.

To add the remote Lync environment:

- 1 In the DMA system manager go to **Admin > Conference Manager > External Lync Systems**.
- 2 In **CAA Dial-in SIP URI**, specify a CAA SIP URI (include *sip:*).
- 3 In **CAA prefix**, specify a dial prefix that initiates routing to the remotely scheduled Lync meetings. You can configure an external Lync system with or without a specific prefix. Note however that you can define only one external Lync system without a prefix.

Edit External Lync System

Name: Customer *

Description: Customer Inc.

CAA prefix: 76

CAA Dial-in SIP URI: sip:caa@customer.com *

☒ Conference template: Factory Template

☒ MCU pool order: Factory Pool Order

☒ MCU selection: Prefer MCU in first MCU pool

OK Cancel Help

- 4 Enable a corresponding dial rule named 'Dial to RealConnect conference by external Lync system conference ID', shown next.

Dial rules for authorized calls:				
Order	Description	Action	Preliminary Enabled	Enabled
#1	Dial registered endpoints by alias	Resolve to registered endpoint	No	Enabled
#2	Dial by conference room ID	Resolve to conference room ID	No	Enabled
#3	Dial by virtual entry queue ID	Resolve to virtual entry queue	No	Enabled
#4	Dial to on-premises RealConnect conference	Resolve to Lync conference ID	No	Disabled
#5	Dial services by prefix	Resolve to service prefix	No	Enabled
#6	Dial external networks by H.323 URL, Email ID or SIP URI	Resolve to external address	No	Enabled
#7	Dial endpoints by IP address	Resolve to IP address	No	Enabled
#8	Dial to RealConnect conference by external Lync system conference ID	Resolve Lync Conference ID by Conference Auto Attendant	No	Enabled
#9	External Lync SIP Peer	Resolve to external SIP peer	No	Enabled

- 5 Add the external Lync system you created previously and enable the dial rule.

Polycom RealConnect technology for Service Provider VMRs can be dialed in one of three ways:

- Manual dial via <Prefix><LyncConferenceID>@<Domain> (enabled above)
- Click-to-Connect via the Polycom RealConnect Proxy service (a Polycom professional services offering)
- Creating a speed dial to a tenant-specific virtual entry queue (VEQ). Documented below:

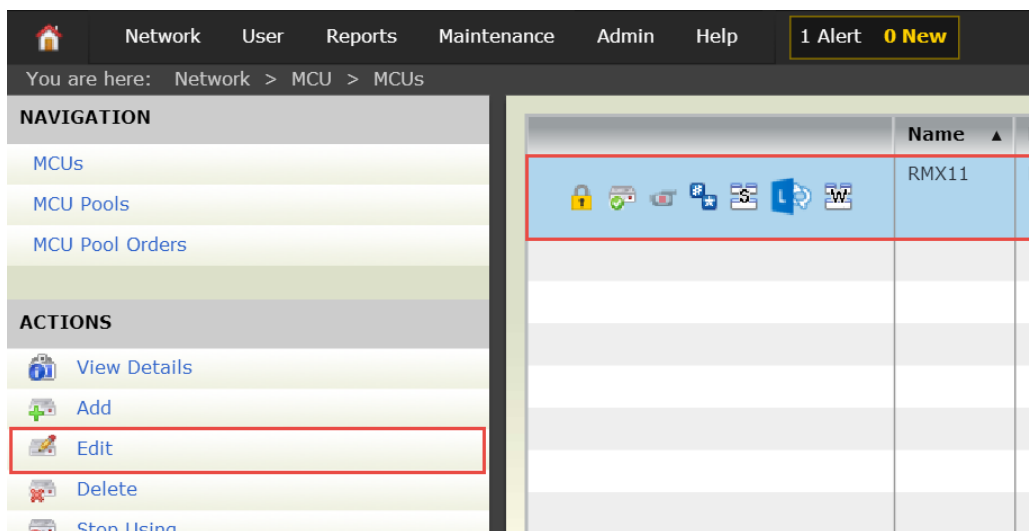
If you are using SIP-registered VTCs, when you create a VEQ, you do not need to dial a prefix and users can dial the Lync Conference ID directly.

Enable a Tenant-Specific VEQ

Before you create VEQ, you need to enable 'External IVR Control' for at least one EQ in one or more MCUs. If you are creating VEQ after adding the MCU to the DMA system, you need to configure the existing MCU.

To edit the existing MCU:

- 1 In the existing MCU, go to **Network > MCU > MCUs**, select the existing MCU, and click **Edit > OK**.



- 2 In the **DefaultEQ Properties** dialog, make the following edits:
 - In **Display Name**, enter DefaultEQ

- In **Entry Queue Mode**, select **External IVR Control**, and click **OK**.

The screenshot shows the 'DefaultEQ Properties' dialog box with the 'General' tab selected. The 'Entry Queue Mode' dropdown is highlighted with a red box and set to 'External IVR Control'. Other fields include 'Display Name' (DefaultEQ), 'Routing Name' (DefaultEQ), 'Profile' (Factory_Video_Profile), 'ID' (1000), 'Entry Queue IVR Service' (Entry Queue IVR Service), and 'Cascade' (None). The 'OK' and 'Cancel' buttons are at the bottom right.

After you enable VEQ on one or more of your MCUs integrated with the DMA system, configure the following on the DMA system.

To configure the DMA system:

- 1 In the DMA system, go to **Admin > Conference Manager > Shared Number Dialing > Add Virtual Entry Queue**.
- 2 In **Virtual entry queue number**, enter a global VEQ number, shown here as **2015**.

- 3 Enable **Unique external Lync system**, set to the external Lync system you specified previously, shown here as **Customer**, and click **OK**.

Edit Virtual Entry Queue

Virtual entry queue number: 2015 *

Dial-in number: 2015

Description: Customer Inc. VEQ

Response entry attempts: 3

Polycom MCU entry queue: DefaultEQ (1/1) [External IVR control]

☒ Unique external Lync system: Customer

DMA-based IVR Call Flow (only for "External IVR control" entry queues)

IVR prompt set: defaultpromptset

Timeout for response entry (sec): 30

DTMF terminator: #

Operator assistance URI:

Request operator transfer DTMF: **

Timeout to cancel operator request (sec): 10

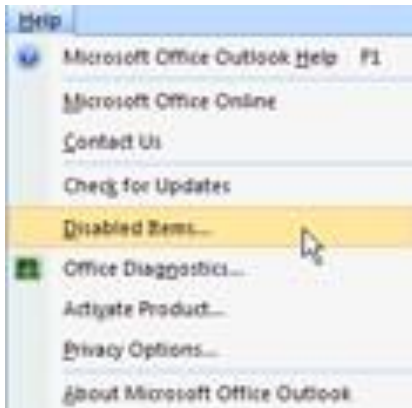
OK Cancel Help

Troubleshoot

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

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

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



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

The Exchange PowerShell commands that delete meeting information after a meeting has been accepted have not been correctly completed.

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

In a Lync Server deployment, you must enable Polycom HDX or RealPresence Group Series system users for remote access and federation as shown in [Task 3: Enable the RealPresence Collaboration Server \(RMX\) Account for Remote Access and Federation](#).

I cannot import a PFX file into the RealPresence Collaboration Server (RMX) solution

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

Follow these instructions:

- 1 Download and install OpenSSL if necessary on the RealPresence Collaboration Server (RMX) workstation. You can download OpenSSL from [Shining Light Productions](#).
- 2 Use OpenSSL to extract the root CA certificate. For example,

```
C:\Program Files\OpenSSL-Win64\bin\openssl pkcs12 -in rmxcert.pfx -cacerts -nokeys -out rootCA.pem
```
- 3 Use OpenSSL to extract the certificate. For example,

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

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

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

5 Manually create your password file.

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

After the *.pfx file is on your PC, you can upload it to the Polycom RealPresence Collaboration Server (RMX) solution and install it, using the procedures in the Polycom RealPresence Collaboration Server (RMX) solution's documentation.