SOLUTION DEPLOYMENT GUIDE

November 2016 | 3725-06675-008A

Polycom® Unified Communications for Microsoft® Environments

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks

End User License Agreement

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

Patent Information

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

Open Source Software Used in this Product

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

Disclaimer

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

Limitation of Liability

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

Customer Feedback

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

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

Contents

Conventions Used in Polycom Guides

Polycom guides contain 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 be successful in accomplishing a procedure or to understand a concept.
Important		Important highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.
Caution		The Caution icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.
Warning		The Warning icon highlights an action you must perform (or avoid) to prevent issues that may cause you to lose information or your configuration setup, and/or affect phone, video, or network performance.
Web Info		The Web Info icon highlights supplementary information available online such as documents or downloads on support.polycom.com or other locations.

Typographic Conventions

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

Typographic Conventions

Convention	*Description*
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.
Italics	Used to emphasize text, to show example values or inputs (in this form: <*example*>), and to show titles of reference documents available from the Polycom Support Web site and other reference sites.

Convention	*Description*
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.
`Courier`	Used for code fragments and parameter names.

Before You Begin

The purpose of this guide is to explain a number of deployment models, architectures, and limitations of the solution and assist administrators deploying Polycom products in a Microsoft environment. Where the Microsoft environment can include Skype for Business or Lync Server, this guide refers to Skype for Business except where a feature is not supported by Skype for Business or instructions apply only to Lync Server.

Audience and Required Skills

The primary audience for this guide is administrators who configure, customize, manage, and troubleshoot Polycom UC components with Skype for Business. Polycom expects the administrator to be a mid-level IT professional experienced in system administration.

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

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 Skype for Business clients and Skype for Business-hosted multipoint calls, your Polycom devices must have an account in a Windows domain accessible by the Skype for Business Server environment. You can create a new Skype for Business account for your Polycom device, or you can set up your Polycom device with an existing Skype for Business account. 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.
- Skype for Business or Lync Server.
  - For help with Skype for Business 2015, see Skype for Business 2015
  - For help with Lync Server 2013, see Microsoft Lync Server 2013
- Skype for Business Server components. In particular, you should be familiar with Skype for Business Server 2015 Management Shell.
- Components of the Polycom UC solution you are using:
  - Polycom® ContentConnect™ software
  - Polycom® RealPresence® Collaboration Server (RMX®) solution (RPCS)
  - Polycom® HDX® system
  - Polycom® RealPresence® Group Series system

- Polycom® RealPresence® Distributed Media Application™ (DMA®) system
- Polycom® RealPresence® Resource Manager
- Polycom® RealConnect™ technology

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:

- Microsoft Skype for Business Server 2015 (6.0.9319.259 – Cumulative Update 3, June, 2016)
- Microsoft Lync Server 2013 (5.0.8308.956 - Cumulative Update, May 2016)
- Microsoft Exchange Server 2013 (15.00.1178.004)

Requirements

This section lists requirements you must complete prior to deploying this solution.

Deploying in a Secure Federal Environment

If you are deploying this solution in a secure federal environment, refer to Appendix G: Deploying in Secure Federal Environments for additional skills, limitations and restrictions, and product-specific configurations.

Limitations

Polycom HDX systems support Lync Server and do not support Skype for Business.

What's New?

New features Skype for Business features vary by Polycom product and for this release include the following:

- Polycom RealPresence Collaboration Server (RMX) and Polycom DMA solutions
  - The panoramic video strip view used by Skype for Business clients can display an additional four standards-based rooms during video conferences.
  - The panoramic strip can be used to display immersive room systems.
  - RealPresence Collaboration Server version 8.7.1 supports a new MCU topology - modular MCU (MMCU) with soft blades – that enables you to directly dial a VMR via Skype for Business and perform Remote Desktop Protocol (RDP)-based content sharing in addition to content sharing within Polycom RealConnect technology. Note that MMCU with soft blades is an alternative to the Microsoft transcoding functionality of Polycom ContentConnect. If you are using the MMCU with soft blades to transcode content, do not use Polycom ContentConnect.

Note: Polycom® RealPresence® Collaboration Server (RMX) 1500/2000/4000 when configured with MPMx blades can operate only with Collaboration Server software versions 8.5.x and earlier. Collaboration Server (RMX) 1800, RMX 2000/4000 when configured with MPMRx blades, and RealPresence Collaboration Server Virtual Edition also operate with Collaboration Server software versions 8.6.x and later.

- Polycom RealPresence Distributed Media Application (DMA)
  - Skype for Business AVMCU-to-MCU Affinity for global Polycom RealConnect deployments makes it easier to choose the Collaboration Server (RMX) closest to the Skype for Business AVMCU used to host a conference. This helps to reduce latency between endpoints attending the conference.
- RealPresence Group Series system
  - Hybrid Skype for Business Online Multi-Tenant Migration
  - Skype for Business mode user interface on RealPresence Touch and RealPresence Group Series systems
  - Displays each room participant in Gallery view with active speaker view
  - Support for Microsoft's Quality of Experience (QoE) Monitoring Server Protocol
  - Support for uploading log diagnostic files to the Skype for Business Server
- Polycom RealConnect technology
  - Calendaring using the Polycom® One Touch Dial application (requires Polycom DMA system and RealPresence Collaboration Server)
  - Microsoft® Office 365 MeetNow and scheduled calls when RealPresence Collaboration Server is registered to Skype for Business on-premises
  - Audience mute on a Polycom RealConnect VMR and standards-based endpoints connected to Collaboration Server in a conference hosted on Polycom RealConnect
  - The Skype for Business conference roster lists all standards-based endpoints connected to RealPresence Platform

Deploying On-Premises Servers with Skype for Business Online

When deploying Skype for Business Online, you must create a small on-premises Skype for Business Server 2015 or Microsoft Lync Server 2013 deployment. At minimum, you must deploy a single Front End Server and single Edge Server to provide SIP connectivity between the Polycom RealConnect technology and Skype for Business Online in Office 365. The required on-premises deployment can use your existing Front End and Edge servers or you can create a new on-premises deployment specifically for this integration.

In either case, you can use either the *Hybrid* (Split-Domain) or *Federated* models to provide the workflow for the Polycom RealConnect technology for any Skype for Business Online users homed in Office 365.

- A split-domain hybrid deployment uses the same SIP domain between the on-premises installation and the online tenancy.

- A federated deployment is an alternate on-premises installation leveraging a different SIP domain used only by the back-end components to communicate with the primary SIP domain that you configure solely within Skype for Business Online.

Web Info: 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:

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

Polycom Resources

All Polycom documentation for Microsoft 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 with Skype for Business Server, 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.

Customer Feedback

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

Polycom-Enabled Unified Communications with Skype for Business Server

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

Features of the Polycom Solution

Integrating Polycom products with Skype for Business Server 2015 enables the following:

- Support for Exchange Online (only on RealPresence Group Series systems) and Microsoft Skype for Business
- Native support for Microsoft Remote Desktop protocol
- Support for native Microsoft application and desktop sharing with the Skype for Business clients
- Support for Microsoft Real-Time Video (RTV) and H.264 SVC
- Easily join Skype for Business meetings from standards-based endpoints using ‘Click to Join’ functionality
- Point-to-point calls among Polycom HDX systems, RealPresence Group Series systems, and Microsoft Skype for Business clients
- Real-time presence information between Polycom devices and Microsoft Skype for Business 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 Skype for Business clients and Polycom endpoints
- Participation in Skype for Business-hosted multipoint conferences using Polycom endpoints
- Optional use of Microsoft Skype for Business 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 content sharing solution for Microsoft Skype for Business clients and standard-based video endpoints. You can enable Polycom ContentConnect software in two modes: Add-on Mode and Gateway Mode. This guide focuses on Gateway Mode, which enables client-less bi-directional content sharing between Microsoft and standards-based video room systems.

Note: Gateway Mode is supported only with Polycom ContentConnect for Skype for Business and Microsoft Lync Server 2013.

Gateway Mode

Polycom ContentConnect software Gateway Mode enables a Skype for Business client or standards-based video room system to share content within a Polycom RealConnect technology meeting. This mode was introduced in Polycom ContentConnect software and supports Skype for Business clients participating within a Skype for Business 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 Microsoft software is no longer required as both signaling and content media conversion is performed infrastructure-side. RealPresence Collaboration Server (RMX) supports Microsoft RDP using MMCU with soft blades – for details, refer to Microsoft Remote Desktop Protocol Content Translator and Polycom Modular MCU.

Note: Gateway Mode facilitates content sharing only between standards-based video room systems and Skype for Business for Polycom RealConnect conferences. 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.

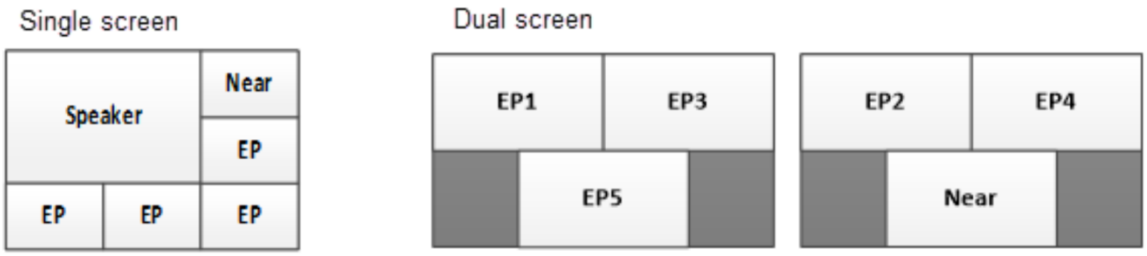
H.264 SVC

This solution supports Microsoft H.264 SVC for Skype for Business and Lync 2013 clients. Backward compatibility mode using RTV is supported for Lync 2010 clients. Note that Polycom HDX systems do not support Microsoft SVC.

Continuous Presence with RealPresence Group Series Systems

Polycom's native support for Microsoft SVC technology means that you can use Skype for Business 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 on RealPresence Group Series Systems

You can use RealPresence Group Series systems to view content from Skype for Business desktop clients in active calls when the Skype for Business client initiates the content-sharing request. RealPresence Group Series can view the following content types from Skype for Business clients:

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

Polycom RealConnect Technology for Skype for Business

RealPresence DMA system and RealPresence Collaboration Server (RMX) solution feature Polycom RealConnect technology for Skype for Business Online and on-premises environments. Polycom RealConnect technology enables you 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 Skype for Business participants, as well as an additional panoramic layout that includes four standards-based endpoints.

Polycom RealConnect also enables you to join traditional standards-based video room systems to Skype for Business-hosted conferences 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-Skype for Business-capable, H.323, or standard SIP-registered endpoints. For more information on configuring RealPresence DMA systems, refer to the section Enabling RealPresence DMA system for Skype for Business and Polycom RealConnect.

Conferences held using RealPresence Collaboration Server (RMX) are bridged or use Polycom RealConnect technology automatically. Up to five of the active Skype for Business 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.

Scheduled Conference Support for Microsoft Office 365

The RealPresence DMA system supports Meet Now and scheduled conferences for Microsoft Office 365 environments. The Office 365 solution requires the Polycom One Touch Dial application and enables video conferencing endpoints to join conferences through calendar invitations from Microsoft Outlook and Exchange.

The RealPresence DMA system also supports conference scheduling for Microsoft Office 365 environments without the use of the One Touch Dial application. RealPresence DMA system administrators can manually create VMRs with an associated focus URI.

Polycom One Touch Dial Application

The Polycom One Touch Dial is an optional application that enables easy ‘Click to Join’ calls held on Polycom RealConnect technology in Skype for Business on-premises deployments. With Polycom RealConnect technology and Skype for Business enabled, a meeting organizer can schedule an online meeting via Microsoft Outlook and the integrated solution automatically sets up the call in the background. Any H.323 or SIP compatible video conferencing system, including telepresence systems in conjunction with supported clients and devices, can use the Polycom One Touch Dial application to join conferences through calendar invitations.

The Polycom One Touch Dial application is required with Office 365 and is used to discover scheduled meetings and create a VMR that includes the conference focus URI and destination network (which are part of the Office 365 meeting invitation) to the RealPresence DMA system using the REST API. To use the Polycom One Touch Dial application with Office 365 and to create VMRs in Office 365, you must install or update to Polycom One Touch Dial version 1.5.2 or later.

Note: The Polycom One Touch Dial Application is available only from Polycom Professional Services.

The Polycom One Touch Dial application is required for and supports the following Office 365 and Skype for Business functionality:

- Click to Join. Endpoints display a list of scheduled meetings and users select a meeting to automatically dial into the conference.
- Cloud Connector Edition (CCE) and Bring Your Own Device (BYOD). Use a smart-phone application or web page to pair with an endpoint, view a list of meetings, click to join a meeting, and dial into the conference.

Microsoft Remote Desktop Protocol Content Translator and Polycom Modular MCU with Soft Blades

RealPresence DMA system supports a new MCU architecture for different media types: Modular MCU (MMCU) with soft blades. For instructions on deploying the MMCU with soft blades, see section *Deployment of Soft Blades in a Modular MCU* in the *RealPresence Collaboration Server – Administrator Guide* version 8.7.1 on Polycom Support.

Polycom RealPresence Collaboration Server version 8.7.1 and later with MMCU with soft blades can transcode Microsoft’s Remote Desktop Protocol (RDP), a content sharing technology used by Skype for Business and Office 365 clients to enable content sharing between Microsoft RDP-based endpoints and H.264 standards-based endpoints.

Note: MMCU with soft blades is an alternative to the Microsoft transcoding functionality of Polycom ContentConnect. If you are using the MMCU with soft blades to transcode content, do not use Polycom ContentConnect.

MMCU with soft blades enables you to:

- Share content to and from the Skype for Business client when dialing directly into a Polycom VMR.
- Share content to and from the Skype for Business client when using Polycom RealConnect technology.

Microsoft Skype for Business AVMCU-to-MCU Affinity

When Skype for Business deployments are geographically distributed, you can start a Polycom RealConnect conference on Skype for Business AVMCUs deployed within the geography depending on the location of the Skype for Business Front End pool. You can configure the RealPresence DMA system to select a Polycom MCU near the Skype for Business AVMCU hosting the Polycom RealConnect conference to reduce call latency, network traffic and costs, and provide for redundancy.

You can also configure Skype for Business clients and non-Skype for Business endpoints to meet in the same conference. Skype for Business AVMCU-to-MCU Affinity enables the RealPresence DMA system to select a Polycom MCU near the on-premises Skype for Business Front End pool hosting the Polycom RealConnect conference. When you configure an MCU pool and MCU pool order to include Polycom MCUs near a Skype for Business deployment, the MCU you select builds a cascade link between the conference and the Skype for Business AVMCU.

You can deploy this feature only for Polycom RealConnect conferences and Skype for Business on-premises deployments. You cannot deploy this feature for Office 365 environments or in federated deployments such as a service provider environment.

Dial Plans for Skype for Business

You can use several dialing plans concurrently in your Skype for Business 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. 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.

For more information, refer to:

- Deploying Polycom RealPresence Collaboration Server Systems
- Setting the Routing for the RealPresence DMA System
- For instructions on creating a MatchURI and provisioning a certificate, refer to Appendix E: Configuring Static Routes in Skype for Business

Remote and Federated Users in Skype for Business Environments

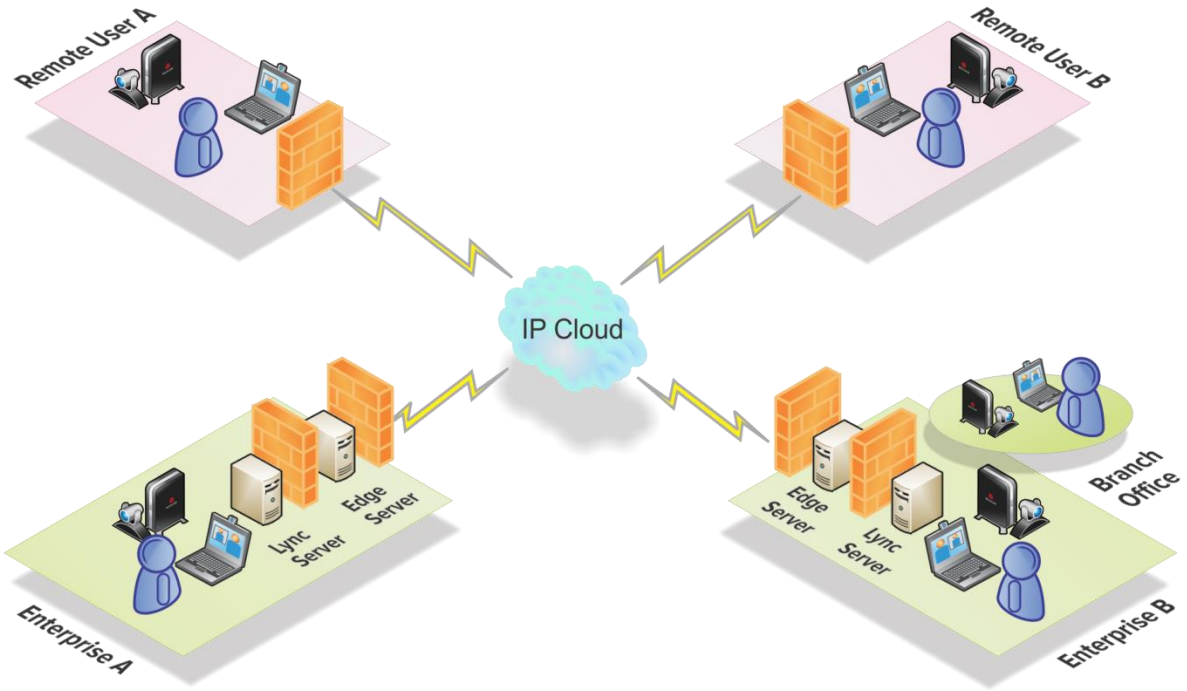
You can support remote and federated users by including a Skype for Business 2015 Edge Server in your environment.

- *Remote users* are users located outside of an organization's firewall. A remote user registered to an enterprise's 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 Skype for Business 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 Skype for Business 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. Remote and federated users are supported with Skype for Business Server 2015, Lync Server 2013, 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.

Skype for Business Server environment with an 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.

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

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

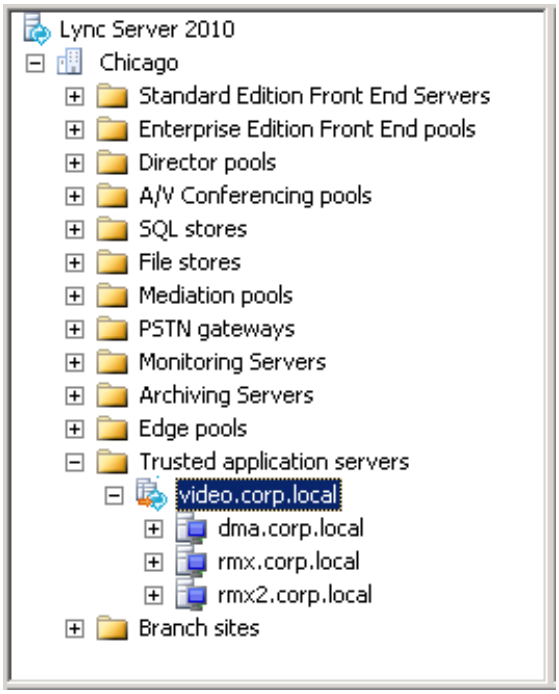
Microsoft Domains and Application Pools Best Practices

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 Skype for Business and when configuring Domain Name System (DNS).

Using 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 Skype for Business MatchURI.

- To configure for RealPresence Collaboration Server (RMX) solution refer to Define a Static Route for the Polycom RealPresence Collaboration Server System Using Microsoft PowerShell.
- To configure for RealPresence DMA system refer to Define a Static Route for the RealPresence DMA System Using Microsoft PowerShell.

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: 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 Skype for Business Presence enabled. If, however, your deployment is created with RealPresence DMA VMRs that are not Skype for Business presence-enabled, you need to create a MatchURI.

Note: 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 Skype for Business SIP domain is not recommended. There are two reasons why using an alternate domain is preferred:

- In larger enterprises, Skype for Business 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 Skype for Business on-premises to 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 Skype for Business. Once this domain is published within your Skype for Business 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 Skype for Business 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

Domain	*Example*	*Usage Notes*
Primary SIP domain for Skype for Business	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.

Domain	*Example*	*Usage Notes*
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.

Deploying Polycom RealPresence Group Series Systems

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

This section contains the following major tasks:

- Configuring Skype for Business Server for use with a RealPresence Group Series System
- Hybrid Deployment for Office 365 Suite
- Configuring Your Polycom RealPresence Group Series System for Skype for Business Server
- Supporting Microsoft Real-Time Video (RTV) and H.264 SVC
- Enable Native Polycom RealConnect Click-to-Join Functionality
- Microsoft Quality of Experience Monitoring Server Protocol

Configuring Skype for Business Server for use with a RealPresence Group Series System

This section explains how to configure Skype for Business Server settings to use a Polycom RealPresence Group Series system within a Microsoft environment. Before completing tasks in this section, you must configure Skype for Business users in Microsoft Active Directory and enabled Skype for Business Server. Talk to your Microsoft Active Directory and administrators or visit Prepare Active Directory for Skype for Business Server 2015 on Microsoft TechNet.

Perform tasks in the following order:

1. Configuring Authentication in Skype for Business Server
2. Microsoft Call Admission Control
3. Enable RTV on the Skype for Business Server
4. Add Calendar and Scheduling Features to Polycom RealPresence Group Series Systems
5. Calendaring Service
6. Enable Conference Rooms for Skype for Business Server
7. Enabling Conference Room Access for Remote and Federated Users
8. Enable RDP Content Sharing
9. Enable Conference Room Accounts for Skype for Business Server
10. Adding Skype for Business Contacts to Conference Room Local Address Book

Configuring Authentication in Skype for Business 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 Skype for Business Server. By default, NTLM is enabled in Skype for Business. 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.

Note: If you have changed the default Skype for Business client version policy, you must create a client version rule for RealPresence Group Series systems to allow them to register. The client version rule must contain the user agent string `PolycomGroup/6.*.*.*`

Microsoft Call Admission Control

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

When a Microsoft CAC policy is enforced in a Skype for Business 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 Skype for Business Server

If you want to support high-quality RTV, you need to change the default video settings on Skype for Business Server 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 Skype for Business Server:

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

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.

Calendaring Service

RealPresence Group systems can connect to Microsoft Exchange Server 2013 or later to retrieve calendar information for a specific Microsoft Outlook or a Microsoft Office 365 individual or system account. The room system connects to Microsoft Exchange Server using the credentials you provide, or by automatically discovering the connection information based on an email address or SIP server address.

Connection to a calendaring service allows the room system to:

- Display the day's scheduled meetings, along with details about each
- Display a Join button on all scheduled meetings for the current day
- Let users join the meeting without knowing the connection details
- Hide or show details about meetings marked Private, depending on the configuration of the system
- Display a meeting reminder before each scheduled meeting, along with a reminder tone

Web Info: Professional Services for Microsoft integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. For additional information and details, refer to *Microsoft Integration Services* on Polycom Collaboration Services.

Configure the Calendaring Service

Before users can view their scheduled meetings on the local interface, you must configure the Calendaring Service on the system web interface. RealPresence Group systems support the Calendaring service with Microsoft Exchange Server 2013 or later and Skype for Business 2015.

To configure the Calendaring Service:

1. In the system web interface, go to **Admin Settings > Servers > Calendaring Service**.
2. Configure these settings as needed.

Setting	Description
Enable Calendaring Service	Enables the room video system to connect to a calendaring service and retrieve meeting information.
Email	Specifies the mailbox account this system should monitor for calendar information. This should match the Primary SMTP Address for the account on Microsoft Exchange or Skype for Business Server, which displays as the value of the mail attribute in the account properties.
Domain	Specifies the domain for registering to the Microsoft Exchange or Skype for Business Server, in either NETBIOS or DNS notation, for example, either company.local or COMPANY. If you are using the Auto Discover Using setting, do not provide a value in this field.
User Name	Specifies the user name to register to Microsoft Exchange or Skype for Business Server, with no domain information included. You can use the system name or an individual's name. If you want the Calendaring Service to use the calendar associated with a Microsoft Office 365 account, enter the user name for that account in this field.
Password	Specifies the system password to register with Microsoft Exchange or Skype for Business Server. You can use the system password or an individual's password. If you want the Calendaring Service to use the calendar associated with a Microsoft Office 365 account, enter the password for that account in this field.
Auto Discover Using	Specifies how the system obtains the Microsoft Exchange or Skype for Business Server address. If you select Email Address, the system uses the value provided in the Email field. If you select SIP Server, the system uses the registered SIP server domain name configured for the RealPresence Group system. When using this feature, you must provide values in the Email, User Name, and Password fields that correspond to the Microsoft Outlook or Microsoft Office 365 individual or system account you want the RealPresence Group system to use for the Calendaring Service. The system may prompt you to confirm the password. If after configuring the Calendaring Service a message displays that the system was unable to discover the service, ensure the information you provided is correct. For example, make sure the email address is in a valid <username@domain> format. You can also use an API command to automatically discover the Microsoft Exchange Server address. For more information, refer to the *Polycom RealPresence Group Series Integrator Reference Guide*.

Setting	Description
Microsoft Exchange Server	Specifies the Fully Qualified Domain Name (FQDN) of the Microsoft Exchange Client Access Server/Skype for Business 2015. If your organization has multiple servers behind a network load balancer, this is the FQDN of the server's Virtual IP Address. If required, an IP address can be used instead of an FQDN, but Polycom recommends using the same FQDN that is used for Outlook clients. Provide a value in this field only if you want to manually provide connection information to Microsoft Exchange or Skype for Business Server. Otherwise, use the Auto Discover Using setting that allows the system to automatically determine the connection information for Microsoft Exchange or Skype for Business Server and populate this field.
Secure Connection Protocol	Specifies the connection protocol to use to connect to the server. Select Automatic or TLS 1.0.
Meeting Reminder Time in Minutes	Specifies the number of minutes before the meeting that a reminder will display on the system.
Play Reminder Tone When Not in a Call	Specifies whether to play a sound along with the text reminder when the system is not in a call.
Show Information for Meetings Set to Private	Specifies whether to display details about meetings marked private.

Enable Conference Rooms for Skype for Business Server

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

Polycom recommends using Microsoft PowerShell to do this. For more information, see Windows PowerShell and Skype for Business 2015 management Tools.

To enable a conference room user for the Skype for Business Server:

1. Access **Microsoft PowerShell**.
2. Enable a conference room user for Skype for Business. For example,

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

Enabling Conference Room Access for Remote and Federated Users

If you are supporting remote users and federated users, you need to configure the following on the 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 Edge Server, you can enable Skype for Business 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 RDP Content Sharing

You can use Remote Desktop Protocol (RDP) to send content to a RealPresence Group system. Use the system web interface to enable the VisualBoard/RDP setting.

To enable RDP content sharing:

1. In the system web interface, go to **Admin Settings > General Settings > System Settings > VisualBoard/RDP**.
2. Select **Enable > Save**.

Enable Conference Room Accounts for Skype for Business Server

RealPresence Group Series system 5.0 enables you to use Remote Desktop Protocol (RDP) with 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 Skype for Business Management Shell, set:

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

Adding Skype for Business Contacts to Conference Room Local Address Book

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

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

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

Hybrid Deployment for Office 365 Suite

When deploying RealPresence Group Series systems with the Office 365 Suite, you can choose to set up your Office 365 services online, or choose a hybrid of online and on-premise services.

See Office 365 integration with on-premises environments and Create a hybrid deployment with the Hybrid Configuration wizard on Microsoft TechNet for additional information.

The following table shows the Office 365 environments Polycom supports.

Office 365 Hybrid Environments

Topologies	*Office 365 Services*		
	Active Directory	Skype for Business	Exchange
Office 365 Multi-Tenant			
Option 1	On-premises with Password Sync	Online	Online
Option 2	On-premises with Active Directory Federation Services (ADFS)	Online	Online
Option 3	Online	Online	Online
Option 4	On-premises	On-premises	Online
On-Premises	On-premises	On-premises	On-premises

Configuring Polycom RealPresence Group Series System for 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:

- Installing the Skype for Business Interoperability License on your RealPresence Group Series System
- Register a Polycom RealPresence Group Series System with the Skype for Business Server
- Understanding SIP Settings
- Configure the Polycom RealPresence Group Series System LAN Properties
- Configure the Skype for Business Directory Server
- Configure Encryption Settings for Skype for Business 2015
- Upload Logs to the Skype for Business Server
- Enable Microsoft® Skype Mode
- Supporting Skype for Business-Hosted Video Conferencing
- Supporting Microsoft Real-Time Video (RTV)

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

When using 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.

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

For instructions on installing the interoperability license, see the *Polycom RealPresence Group Series – Administrator Guide* on Polycom Support.

Register a Polycom RealPresence Group Series System with Skype for Business

When you register a RealPresence Group Series system with a Skype for Business Server, the Polycom RealPresence Group Series system user can see a list of 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 Understanding SIP Settings.

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

To register a RealPresence Group Series system with Skype for Business Server:

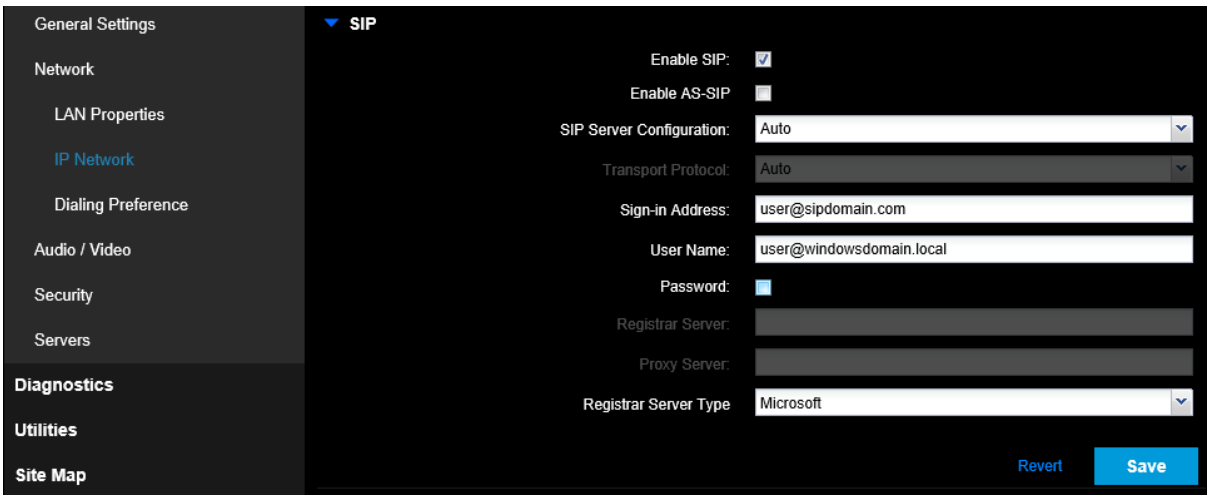
1. Open a browser window and in the **Address** field enter the Polycom system IP address or host name.
2. Go to **Admin Settings > Network > IP Network** and select **SIP**.
3. Configure the settings in the **SIP Settings** section of the **IP Network** screen shown in the section Understanding SIP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

   After the RealPresence Group Series system registers with Skype for Business Server, continue to the section Configure the Polycom RealPresence Group Series System LAN Properties.

Understanding 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 following list describes all SIP settings on the **IP Network** screen.

- **Enable SIP** Select to enable the RealPresence Group Series system to make and receive SIP calls.
- **SIP Server Configuration** Select **Auto** if your Skype for Business Server configuration is set up for automatic discovery, which requires you to correctly configure Skype for Business SRV records. If the Skype for Business 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 Skype for Business environment, specify the DNS name of the Front End Pool or Director. The default port is 5061.
- If registering a remote RealPresence Group Series system with an 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: `pool.corp.local`
- To specify a different Transport Layer Security (TLS) port and use the default Transmission Control Protocol (TCP) port: `pool.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. 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. 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.
- **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, and 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 Skype for Business.
  - **TCP** provides transport via TCP for SIP signaling and is not applicable for Skype for Business. 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 Skype for Business 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 Skype for Business Server this must be set to Microsoft.

Web Info: For more 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 Skype for Business, the RealPresence Group Series system must be able to access a DNS server and the name for the Skype for Business Pool or 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 Skype for Business Server. If you are registering a remote Polycom system, use a public DNS server that shares DNS zone information with the Edge Server.
5. Click **Update**.

Configure the Skype for Business Directory Server

You can configure the RealPresence Group Series system to use Skype for Business Server when the RealPresence Group Series system is automatically provisioned by a RealPresence Resource Manager system or in standard operating mode.

To configure the Skype for Business Server 2015 directory settings:

1. In the system web interface, go to **Admin Settings > Network > IP Network > SIP**.
2. Configure the SIP settings as shown in Understanding SIP Settings.
3. In the system web interface, go to **Admin Settings > Servers > Directory Servers** and select the Microsoft Service Type.
4. Configure the following settings on the Directory Servers screen.

Setting	Description
Registration Status	Specifies whether the system is successfully registered with the Skype for Business Server 2015.
Domain Name	Specifies the Domain Name entered on the SIP Settings screen.
Domain User Name	Specifies the Domain User Name entered on the SIP Settings screen.

Setting	Description
User Name	Specifies the User Name entered on the SIP Settings screen.

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

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 **Skype for Business Server** section of the Directory Servers page, configure these settings:
   - **Server Type** Specifies whether the SIP Registrar Server is a Skype for Business Server. Enabling this setting activates integration features such as the Microsoft global directory and Skype for Business 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**.

Configure Encryption Settings for Skype for Business 2015

Polycom RealPresence Group systems support media encryption in calls with Skype for Business 2015 and Microsoft Lync 2013 Server pool. You must configure encryption settings before using the Polycom RealPresence Group system for video conferences with Skype for Business 2015. 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.

Each codec within Polycom systems must have the same settings.

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

Your system encryption settings must be compatible with your Skype for Business Server settings. If you need to update encryption settings on Skype for Business Server, refer to the section Update Encryption Settings.

To enable encryption for 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`)

Upload Logs to the Skype for Business Server

You can upload diagnostic logs to the Skype for Business Server to provide the Skype for Business administrator access to RealPresence Group Series device logs that can help the administrator troubleshooting issues. The Skype for Business administrator can enable or disable support for this option from the Skype for Business Server.

To upload logs to the Skype for Business Server:

1. Navigate to **Diagnostics > System > Logs**.
2. Click **Upload system log**.

Enable Microsoft® Skype Mode

After the RealPresence Group Series system is registered with the Skype for Business Server online or on-premises, you can enable Skype mode for the RealPresence Group Series system to provide a consistent environment for all Office 365 products in your deployment. When the RealPresence Group Series system is signed into Skype for Business Online, Skype mode is required and enabled automatically, and users can control the RealPresence Group Series system only with the RealPresence Touch device. You cannot disable Skype Mode in Skype for Business Online deployments.

The following limitations apply to RealPresence Group Series systems when Skype mode is enabled:

- Users cannot use the remote control, Polycom Touch Control, the touch interface, or keyboard and mouse to control the RealPresence Group Series system.

  Users can still use the Polycom® SoundStation® IP 7000 to control the system.
- You cannot configure the left and right elements of the address bar.

- You cannot configure the user login for system access.
- You cannot enable Speed Dials, and favorites do not display on the home screen.

To enable Skype mode:

1. In the RealPresence Group system web interface, go to **Admin Settings > General Settings > Home Screen Settings > Skype Mode.**
2. Select **Enable Skype mode**.
3. Click **Save**.

Supporting Skype for Business-Hosted Video Conferencing

Skype for Business-hosted conferencing is supported only when Polycom endpoints are registered to Skype for Business. To participate in Skype for Business-hosted video conferences using a RealPresence Group Series system or to register the system to Skype for Business, 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 or Polycom® RealPresence Touch™.

When using Skype for Business-hosted video conferencing, keep the following points in mind:

- When in a Skype for Business-hosted call, the RealPresence Group Series system displays a Busy presence state and rejects any incoming calls.
- When in a Skype for Business-hosted call, other multipoint calling methods, such as internal multipoint hosting, RealPresence Collaboration Server (RMX) or 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 Skype for Business-hosted conference calls and to use up to 1080p high-definition video between a RealPresence Group Series system and Skype for Business client.
- You need the Skype for Business Interoperability License to enable support for Skype for Business.
- In SVC multipoint calls hosted on Skype for Business Server, you can view multiple far-end sites in layouts. Note that when using 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 Skype for Business-hosted conferences, RealPresence Group Series systems require a Polycom Touch Control or RealPresence Touch to:

- View conference participants
- Add participants to the conference
- Organize and initiate conferences with RealPresence Group Series and Skype for Business clients and groups

Understanding Roles in Skype for Business-hosted Calls

Participants in a Skype for Business-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 Skype for Business-hosted Call and Managing a Skype for Business-hosted

Call . You set up these roles on the Skype for Business Server, but if you are the conference organizer, you can change the roles of other participants using the Skype for Business client.

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

Managing Participants in a Skype for Business-hosted Call

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

Managing a Skype for Business-Hosted Call

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

Supporting Microsoft Real-Time Video (RTV) and H.264 SVC

The 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 Skype for Business.

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 Skype for Business 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 Skype for Business 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 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 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 Skype for Business uses either RTV or H.264 SVC.
- Polycom ITP systems only use RTV on point-to-point calls with a Skype for Business client and connect only with the primary codec.
- When calling from RealPresence Group Series and RealPresence Collaboration Server to Skype for Business, 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 Skype for Business clients to send additional video streams comprised of RTV.

Enable Native Polycom RealConnect Click-to-Join Functionality

Polycom RealPresence Group Series 5.0 includes 'Click to Join' functionality which enables you to directly join room systems to Polycom RealConnect meetings without the need to manually type the Skype for Business Conference ID. This feature is available for H.323 and SIP-registered RealPresence Group Series systems, as well as for dual-registered Skype for Business 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:

1. 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 Skype for Business Conference ID, which is supplied by the Skype for Business Server, this metadata is static. For this reason, Polycom recommends that you update your Skype for Business Server Meeting Configuration with custom footer text indicating the appropriate dial string.

The metadata can be used for two purposes:

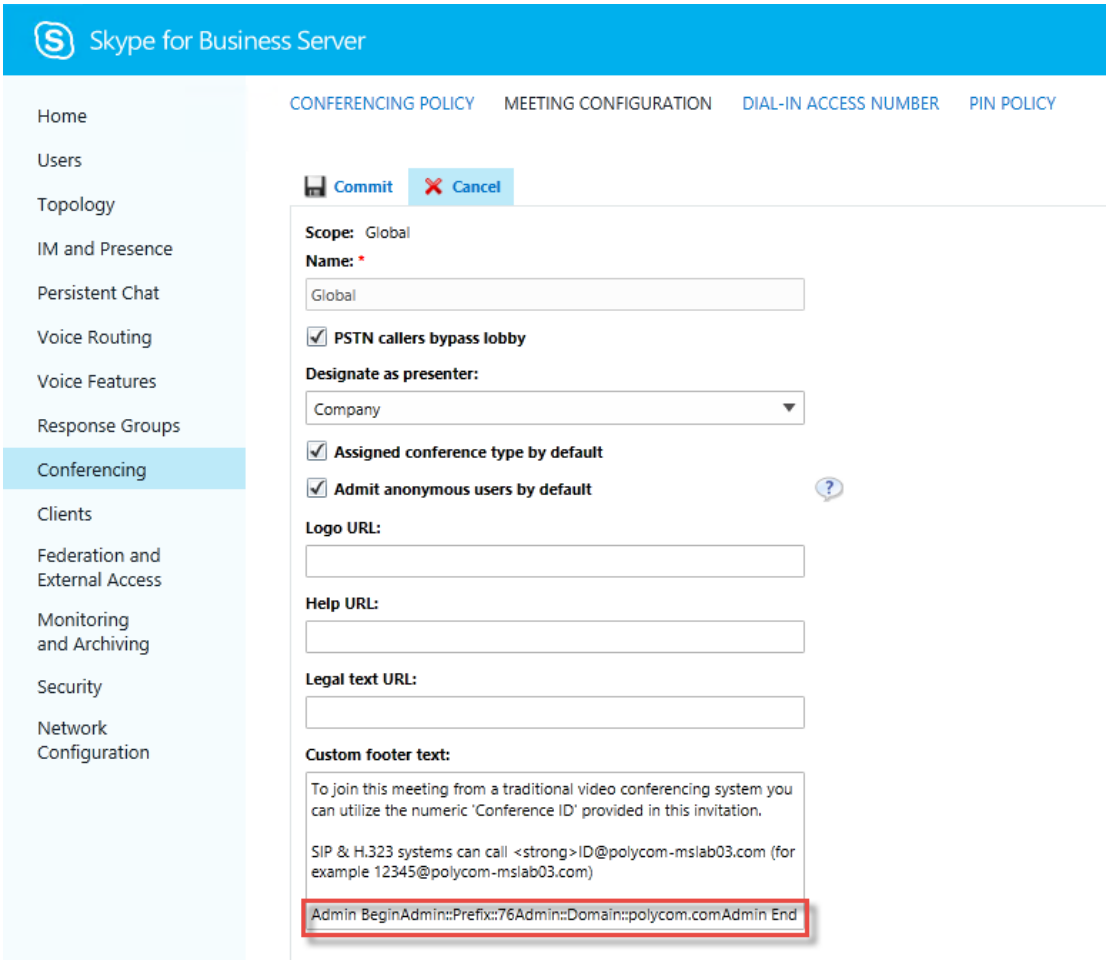
- **Prefix field.** To automatically prepend a prefix number prior to the Conference ID.

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`.



RealConnect Limitations

- When you add another endpoint in an ad hoc point-to-point call, the conference might revert back to Skype for Business Server 2015 or Microsoft Lync Server 2013 and the ad hoc conference is not able to use SmartCascading functionality. However, the conference still functions like a Skype for Business Server 2015/Microsoft Lync Server 2013 call.
- Call participants cannot use their personal VMR ID. Instead, you must use an ID generated by the Lync/Skype meeting invite.

- The RealPresence Collaboration Server (RMX) sends the active speaker that has joined on the conference to Microsoft Lync Server 2013 or Skype for Business Server 2015, so the Lync/Skype server displays only the active speaker.

Microsoft Quality of Experience Monitoring Server Protocol

Using Microsoft's Quality of Experience Monitoring Server Protocol (QoE), you can monitor the audio quality and troubleshoot audio related issues in your deployment. When Skype for Business monitoring is available, the RealPresence Group Series systems publish QoE metrics for each SIP session hosted on the Skype for Business Server. QoE reports contain audio-only metrics and do not contain video or content sharing metrics.

QoE is compatible with Skype for Business Server, and Skype for Business Online, and Lync Server 2013. For more information on QoE, see Quality of Experience Monitoring Server Protocol on Microsoft Developer Network.

The following table includes the QoE metrics published to the Skype for Business Sever for RealPresence Group Series systems.

Supported QoE Metrics for RealPresence Group Series

Parent Element	*Child Element/Attributes*	*Description*
VQReportEvent	VQSessionReport	Quality report for a session (SIP dialog).
	VQSessionIntervalReport	Mid call Quality report
VQSessionReport and **VQSessionIntervalReport**	Endpoint	Information about the endpoint that created the report.
	DialogInfo	Information regarding the SIP dialog
	MediaLine	A media line is the logical equivalent to an m-line in Session Description Protocol (SDP).
Endpoint	Name	Computer name of the device that created the report. If the maximum string length is exceeded, the report is rejected.
	v2:OS	The operating system used for the reporting endpoint.
	v2:VirtualizationFlag	Flag indicating the type of virtualization environment: • '0x00' – None • '0x01' – HyperV • '0x02' – VMWare • '0x04' - Virtual PC • '0x08' - Xen PC

Parent Element	*Child Element/Attributes*	*Description*
DialogInfo	DialogCategory	Information about the QoE Report leg type, which is either a UC or Mediation Server-GW trunk.
	FromURI	SIP URI in the SIP From header that the reporting endpoint uses if it makes a SIP transaction using the reported SIP dialog.
	ToURI	SIP URI in the SIP To header that the reporting endpoint uses if it makes a SIP transaction using the reported SIP dialog.
	Caller	True if the reporter was the caller of the SIP dialog. False if the reporter was not the caller of the SIP dialog.
	LocalContactURI	SIP URI in the SIP Contact header of the reported SIP dialog that was sent from the reporting endpoint.
	RemoteContactURI	SIP URI in the Contact header of the reported SIP dialog that was sent from the remote endpoint.
	LocalUserAgent	SIP User-Agent or Server header content of the reported SIP dialog that was sent from the reporting endpoint.
	RemoteUserAgent	SIP User-Agent or Server header content of the reported SIP dialog that was sent from the remote endpoint.
	LocalPAI	SIP URI in the SIP p-asserted-identity (PAI) header of the reported dialog that was sent from the reporting endpoint
	RemotePAI	The SIP URI in the SIP p-asserted-identity (PAI) header of the reported dialog that was sent from the remote endpoint.
	ConfURI	The SIP URI of a conference bridge that hosted a conference and terminated this dialog. This URI is unique to each conference and common to all the dialogs that participated in the same conference. ConfURI is available for conferences only.
	v2:CallPriority	The SIP Priority header that indicates the priority selected for the call.
	v2:MediationServerBypassFlag	True if the reporting endpoint selected the bypass SDP.

Parent Element	*Child Element/Attributes*	*Description*
	v2:TrunkingPeer	The SIP ms-trunking-peer header that reports the fully qualified domain name (FQDN) of the public switched telephone network (PSTN) gateway.
	v2:RegisteredInside	True if the listening address is registered within the enterprise. This replaces the Inside element in AddrType.
	CallId	SIP Call-ID of the dialog. If the maximum string length is exceeded, the report is rejected.
	FromTag	SIP From tag of the dialog.
	ToTag	SIP To tag of the dialog.
	Start	Start time of the dialog.
	End	End time of the dialog.
MediaLine	Description	Media Line context information
	InboundStream	Information regarding the inbound media stream.
	OutboundStream	Information regarding the outbound media stream (2).
Description	Connectivity	Interactive Connectivity Establishment (ICE) connectivity information.
	Security	The security profile in use. Supported values are "SRTP" and "None".
	Transport	The type of transport in use. Supported values are "TCP" and "UDP".
	LocalAddr	IP address related information for the reporting endpoint.
	RemoteAddr	IP address related information for the remote endpoint.
Connectivity	Ice	Information about the media path, such as direct or relayed. For more information, see the enumeration types in Connectivity Element.
	IceWarningFlags	Information about ICE process described in bits flags.
	RelayAddress	IP address related information of the Audio/Video Edge Server (A/V Edge Server).

Parent Element	*Child Element/Attributes*	*Description*
InboundStream and OutboundStream	Network	Network-based metrics.
	Payload	Payload-based metrics.
Network	Jitter	Jitter related metrics.
	PacketLoss	Packet loss related metrics.
	BurstGapLoss	Burst related metrics.
	Delay	Delay related metrics.
	Utilization	Utilization related metrics.
Jitter	InterArrival	The average inter-arrival jitter, as specified in [RFC3550] section 6.4.1.
	InterArrivalSD	The standard deviation of inter-arrival jitter, as specified in RFC 3550.
PacketLoss	LossRate	The average fraction lost, as specified in RFC 3550, computed over the duration of the session.
	LossRateMax	The maximum fraction lost, as specified in RFC 3550, computed over the duration of the session.
BurstGapLoss	BurstDensity	The average burst density, as specified in RFC 3611, computed with a Gmin=16 for the RTP packets received.
	BurstDuration	The average burst duration, as specified in RFC 3611, computed with a Gmin=16 for the RTP packets received.
	GapDensity	The average gap density, as specified in RFC 3611, computed with a Gmin=16 for the RTP packets received.
	GapDuration	The average gap duration, as specified in RFC 3611, computed with a Gmin=16 for the RTP packets received.
Delay	RoundTrip	The average network propagation round-trip time computed as specified in RFC 3550.
	RoundTripMax	The maximum network propagation round-trip time computed as specified RFC 3550.
Utilization	Packets	Number of Real-Time Transport Protocol (RTP) packets sent in the session.

Parent Element	*Child Element/Attributes*	*Description*
Payload	Audio	Audio-based payload metrics.
Payload.Audio	PayloadType	Payload number used for the codec, as specified in MS-RTP.
	PayloadDescription	Codec name, as specified in MS-SDPEXT or RFC 3551.
	SampleRate	Audio sample rate.
	v4:JitterBufferSizeAvg	Average size of jitter buffer during session.
	v4:JitterBufferSizeMax	Maximum size of jitter buffer during session.
	v4:JitterBufferSizeMin	Minimum size of jitter buffer during session.
	v4:NetworkJitterAvg	Average of network jitter computed over 20 second windows during the session.
	v4:NetworkJitterMax	Maximum of network jitter computed over 20 second windows during the session.
Signal	InitialSignalLevelRMS	The root-mean-square of the received signal for the first 30 seconds of the call.
	Echoeventcauses	It is important to report 0x04; skip 0x01 and skip 0x10
	EchopercentSend	Percentage of time when echo is detected in the audio from the capture or microphone device after echo cancellation.
	RecvSignalLevels	If there is no support for Stereo, use only Ch1.
	RecvNoiseLevels	If there is no support for Stereo, use only Ch1.
	SendSignalLevels	This is the post AGC signal level reported in dBFs
	RenderSignalLevel	Average render speech level after dynamic range compression or analog gain control is applied.
	RenderNoiseLevel	Average render noise level after dynamic range compression or analog gain control is applied.
	RenderLoopbackSignalLevel	Average level of speaker loopback signal (after any device offload effects have been applied).

Parent Element	*Child Element/Attributes*	*Description*
QualityEstimates.Audio		In the QoE / VQ structure, the inbound and outbound blocks contain a “Network” section which has a DSCP field. These fields should be used to indicate what DSCP value was applied to the RTP stream packets outgoing as well as received with incoming packets. This would is valuable information for ensuring the end-to-end network is dealing appropriately with media streams. See QualityEstimates.Audio Element.
	RecvListenMOS	The MOS-LQO wideband for decoded audio received by the reporting entity during the session.
	RecvListenMOSMin	Minimum of the RecvListenMOS for the stream during the session.
	NetworkMOS	Predictive metrics based on network factors alone.
	OverallAvg	The average of MOS-LQO wideband based on the audio codec used and the observed packet loss and inter-arrival packet jitter.
NetworkMOS	OverallMin	The minimum of MOS-LQO wideband based on the audio codec used and the observed packet loss and inter-arrival packet jitter.

Deploying Polycom HDX Systems

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

Note: At this time, the Polycom HDX system supports Lync Server and does not support Skype for Business.

This section contains the following major tasks:

- Configuring Lync Server for use with a Polycom HDX System
- Configuring Polycom HDX System for Lync Server
- Microsoft Real-Time Video (RTV)

Configuring 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. Important: 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 see Preparing Active Directory Domain Services for Lync Server 2013 on Microsoft TechNet.

Consider the following points or perform tasks in the following order:

1. Configuring Authentication in Lync Server
2. 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. Enabling Conference Room Access for Remote and Federated Users
7. Adding Contacts to Conference Room Local Address Book

Configuring Authentication in Lync Server

If you want to include a Polycom HDX system in your Microsoft environment, you must enable NTLM on your 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.

Microsoft Call Admission Control

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

When a Microsoft CAC policy is enforced in a Microsoft 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 video settings when using resolutions beyond VGA.

To change the default video settings for your Lync Server:

1. Access **Microsoft 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.

If the conference room user accounts 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.

The following procedure shows you how to add a conference room user manually in the Active Directory Users and Computers management console.

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.

Polycom recommends using Microsoft 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 **Microsoft PowerShell**.

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

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

Enabling Conference Room Access for Remote and Federated Users

If you are supporting remote users and federated users, you need to configure the following on the 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 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.

Adding 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. 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.

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 Display Options for the Polycom HDX System Contact List.

Configuring Polycom HDX System for Lync

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:

1. Installing the RTV Option Key on your Polycom HDX System
2. Register Polycom HDX System with the Lync Server
3. Understanding SIP Settings
4. Configure the Polycom HDX System LAN Properties
5. Display Options for the Polycom HDX System Contact List
6. Configure AES Encryption
7. Supporting Lync-hosted Video Conferencing and Lync Server
8. Microsoft Real-Time Video (RTV)

Installing 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, support for the RTV option key is mandatory for both point-to-point and multiparty calling scenarios. 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

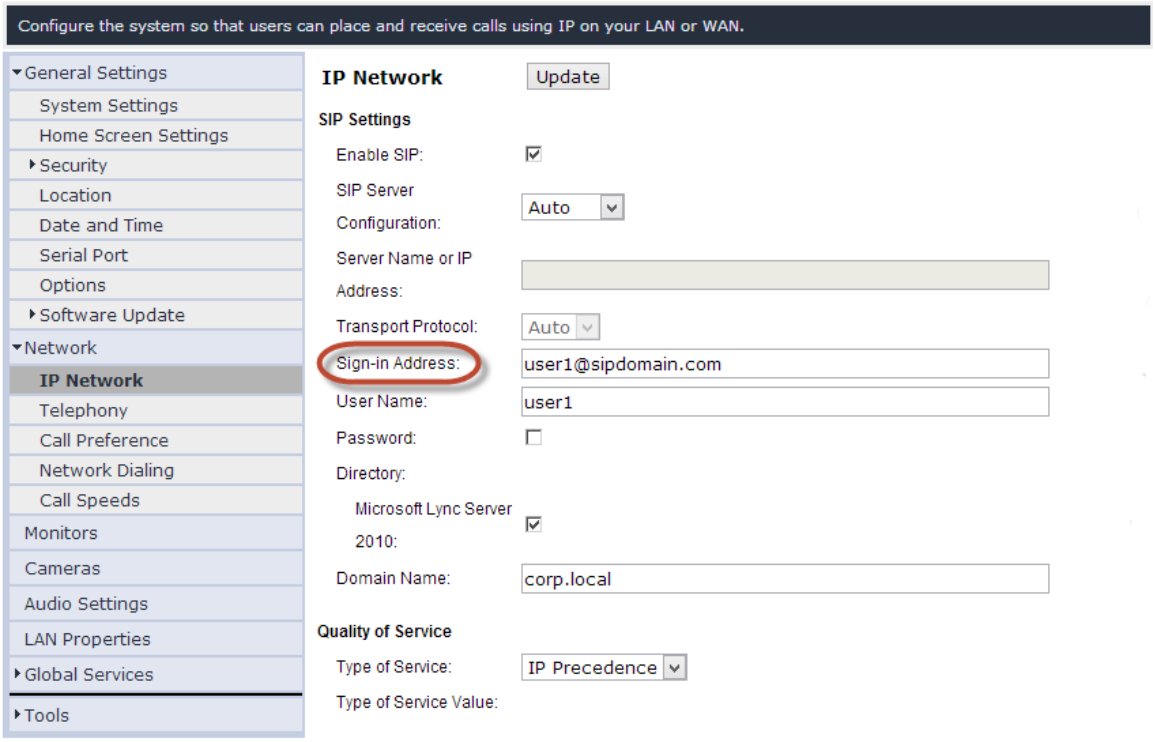
When you register a Polycom HDX system with a Lync Server, the Polycom HDX system user can see a list of contacts and whether contacts are online or offline. Contacts display in the directory and users can choose to display contacts on the home screen or call a contact. You can find descriptions of all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

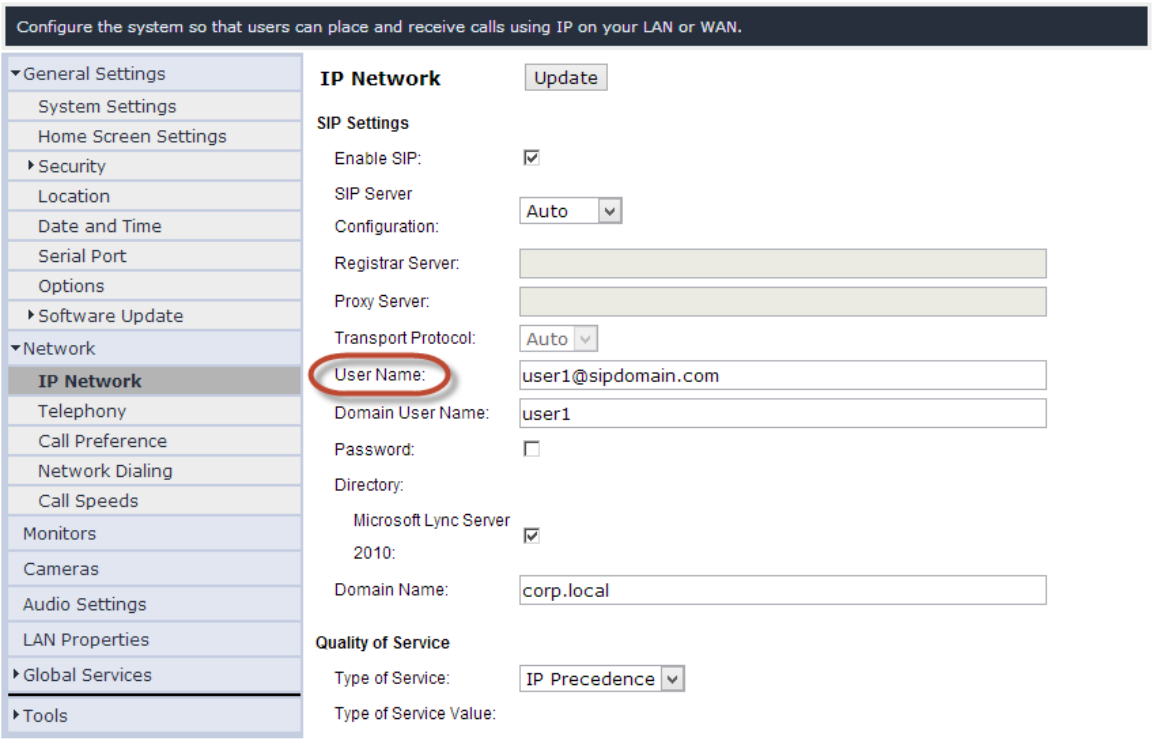
Note: An RTV option key is a requirement for integration with Lync Server 2013 as the H.263 codec has been deprecated. Support for Microsoft H.264 SVC is not planned for HDX series.

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.





4 Click **Update**.

After the Polycom HDX system registers with Lync Server, continue to the section Configure the Polycom HDX System LAN Properties.

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

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

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

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

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

- **Transport Protocol** The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required.
  - **Auto** enables an automatic negotiation of protocols in the following order: TLS, TCP, and 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. 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`. If you have not installed the RTV option key, this setting is named *Domain User Name*.

  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.
- **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.

Web Info: 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**.

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**.

Supporting Lync-Hosted Video Conferencing and Lync Server 2013

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

Understanding Roles in Lync-Hosted Calls

Participants in a Lync-hosted call can have one of three roles depending on the level of user rights granted within the call. The privileges associated with each role are shown in 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

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

Managing a Lync-Hosted Call

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

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.

Deploying Polycom RealPresence Collaboration Server (RMX) Solution

To integrate your Polycom RealPresence Collaboration Server (RMX) solution with Skype for Business Server or 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 Skype for Business Server for the RealPresence Collaboration Server (RMX) solution to use, and enable 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 Remote and Federated Users in Skype for Business Environments.

This section outlines the following tasks required to configure Polycom RealPresence Collaboration Server (RMX) solution with Skype for Business.

Complete these major tasks in the following order:

1. Configuring Polycom RealPresence Collaboration Server (RMX) System for Skype for Business
2. Enabling Edge Server Integration with Polycom RealPresence Collaboration Server (RMX) System
3. Configure RealPresence Collaboration Server (RMX) for Polycom ContentConnect Software

Configuring Polycom RealPresence Collaboration Server (RMX) System for Skype for Business

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

Complete the following steps:

1. Setting up the RealPresence Collaboration Server (RMX) System for Security and SIP
2. Creating and Installing a Security Certificate for the Polycom RealPresence Collaboration Server (RMX) System
3. Install the certificate on your RealPresence Collaboration Server (RMX) solution
4. Update Encryption Settings
5. Configuring Skype for Business for use with a Polycom RealPresence Collaboration Server (RMX) System

Setting 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:

1. Configure the RealPresence Collaboration Server (RMX) IP Network Service
2. Add the RealPresence Collaboration Server (RMX) FQDN (SIP signaling IP address) in DNS

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 Skype for Business 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 Front End server or Pool name and the server domain name.
10. If not selected by default, change the **Transport Type** to **TLS**.

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

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

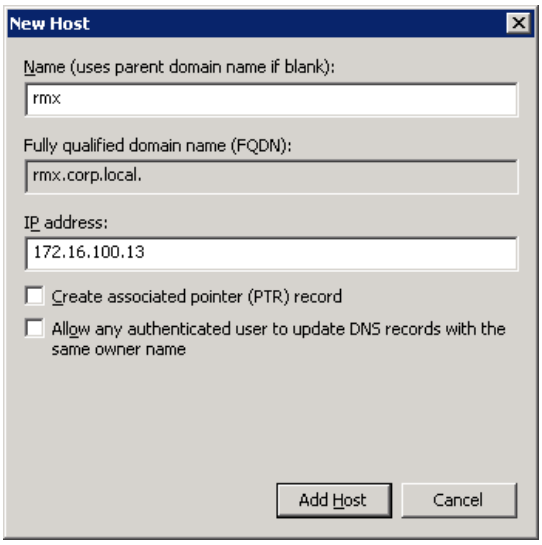
The RealPresence Collaboration Server (RMX) solution and the Skype for Business Server must both resolve the RealPresence Collaboration Server (RMX) host record identically, regardless of the domain you select to store the DNS Host record.

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**.

Creating and Installing 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 Skype for Business 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 Skype for Business 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.

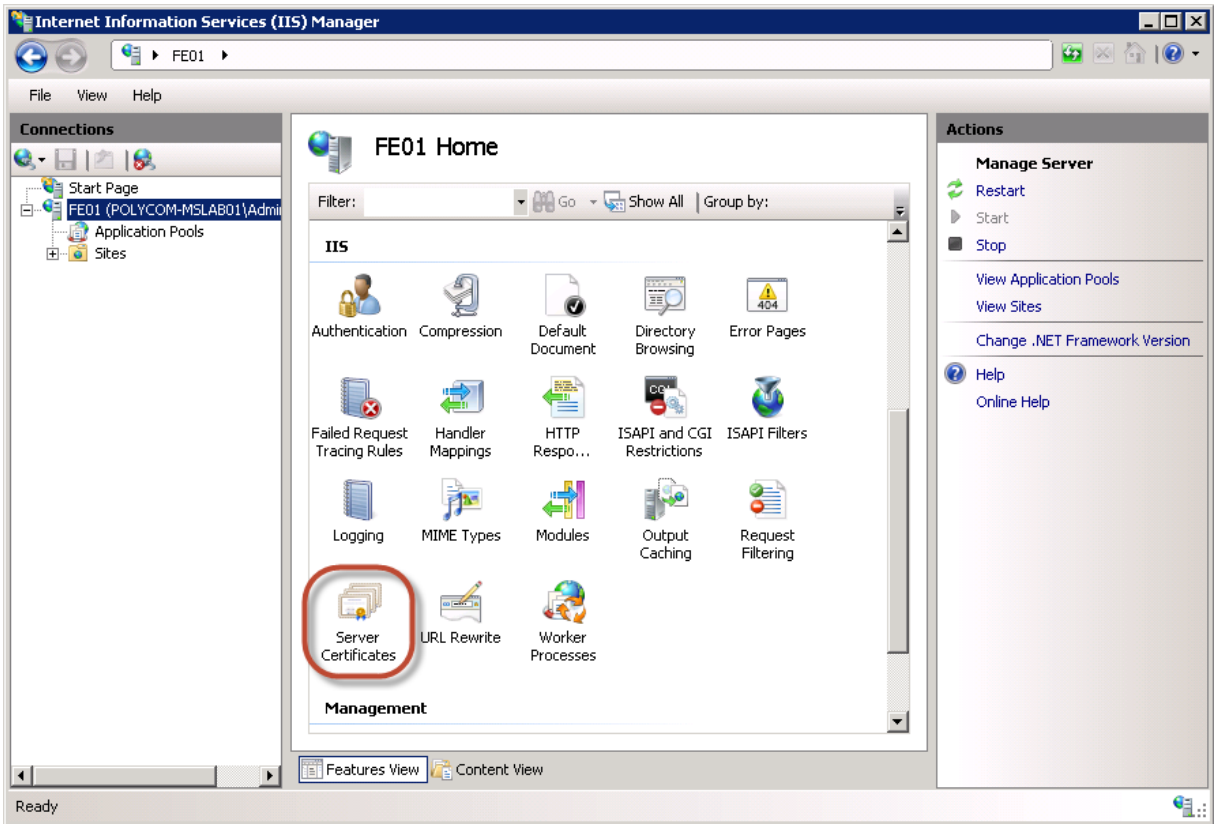
- If your organization requires that all certificates be generated externally, then follow those procedures to generate the certificates and install them on your system using the procedures outlined in *Polycom RealPresence Collaboration Server (RMX) Administrator Guide* for your model at Collaboration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

Create a Security Certificate for RealPresence Collaboration Server

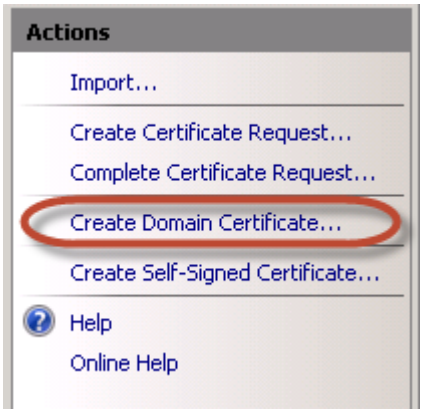
This section shows you how to create a security certificate for the Polycom RealPresence Collaboration Server (RMX) solution using IIS Manager 7.

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

1. On the Skype for Business 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.



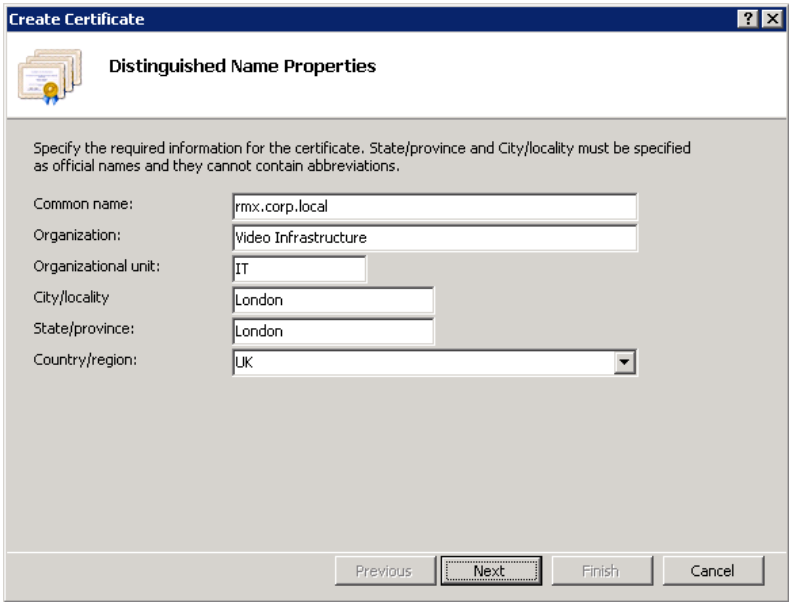
4 In the **Actions** pane on the far right, select **Create Domain Certificate**.



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.



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.

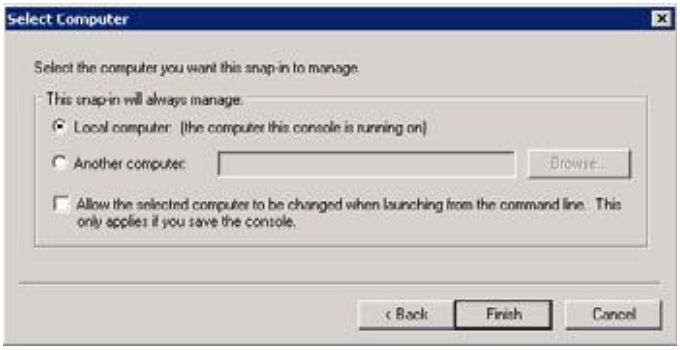
Export a Certificate

After you create a security certificate use the Microsoft Management Console to export the certificate.

To use the Microsoft Management Console to export the certificate:

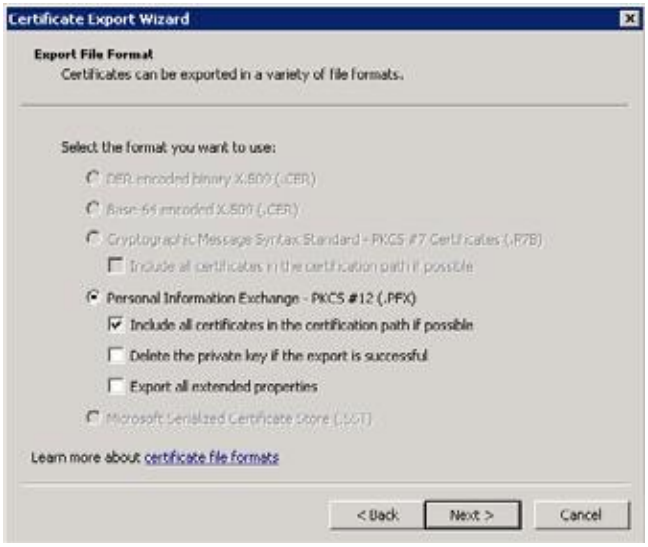
1. Open **Microsoft Management Console** and add the Certificates snap-in.
   a. Choose **File > Add/Remove Snap-in**.
   b. Select **Certificates** from the Available Snap-ins area and click **Add**.
   c. On the **Certificates snap-in** dialog, select **Computer Account** and click **Next**, as shown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

Update Encryption Settings

You must enable encrypted media when integrating RealPresence Platform with Skype for Business Server. Polycom recommends that you enable a minimum of Support Encryption settings.

As a best practice, Polycom recommends using PowerShell commands to update the Skype for Business Server encryption settings. For more details on using PowerShell, see Windows PowerShell and Skype for Business Server 2015 management tools.

To change the Skype for Business Server encryption setting:

1 Use the following PowerShell command to determine the current encryption setting:

```
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 PowerShell command to change your encryption setting to support encryption:

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

3 Verify your encryption settings:

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

Configuring Skype for Business for use with a Polycom RealPresence Collaboration Server (RMX) System

The Polycom 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 Skype for Business Server.

Polycom recommends using PowerShell commands to perform the following tasks. For detailed documentation on using PowerShell, see Skype for Business Server 2015 Management Shell.

Note: In Microsoft environments, SIP domains often match the email domain. As an alternative, you can use a separate SIP domain for your Skype for Business 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 Using Multiple Computer Application Pools.

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

1 Define Your Trusted Application Pool Using Skype for Business Topology Builder

2 Create the Trusted Application Using Microsoft PowerShell

3 Update the Topology Using Microsoft PowerShell

4 (Optional) Define a Static Route for the Polycom RealPresence Collaboration Server (RMX) System Using Microsoft PowerShell

Define Your Trusted Application Pool Using Skype for Business Topology Builder

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 > Skype for Business 2015 > Skype for Business Server Topology Builder** to open the Skype for Business 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 Using 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.

Create the Trusted Application Using Microsoft PowerShell

This step creates the trusted application using the Microsoft PowerShell.

To create the trusted application:

1. Navigate to **Start > All Programs > Skype for Business Server 2015 > Skype for Business Server Management Shell** to open the Microsoft 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 Skype for Business 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 Skype for Business 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 Skype for Business deployment.

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

Note: 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

Update the Topology Using Microsoft PowerShell

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

To update the topology:

1 Navigate to **Start > All Programs > Skype for Business Server 2015 > Skype for Business Server Management Shell** to open the PowerShell terminal.

2 Use the `Enable-CsTopology` command to update the Skype for Business topology.

```
Enable-CsTopology
```

(Optional) Define a Static Route for the Polycom RealPresence Collaboration Server (RMX) System Using Microsoft PowerShell

This step explains how to define a static route for your Polycom RealPresence Collaboration Server (RMX) solution using PowerShell. Note that you must create a static route within Skype for Business for Collaboration Server (RMX) or RealPresence DMA only for RealPresence Platform VMRs without RealPresence DMA presence and/or Polycom RealConnect technology. Route changes you make take effect immediately.

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).

To define a static route:

1. Navigate to **Start > All Programs > Skype for Business Server 2015> Skype for Business Server Management Shell** to open the PowerShell terminal.
2. Use the `New-CsStaticRoute` command to set up a static route for the RealPresence Collaboration Server (RMX) solution

   ```
   $route = New-CsStaticRoute -TLSRoute -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 TechNet 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 Skype for Business client to a SIP address in the RealPresence Collaboration Server (RMX) solution's domain will be routed through that system.

Enabling 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 Skype for Business Server.

Note: Federation and CAC are supported only for Polycom endpoints and devices registered to a Skype for Business Server.

Required Ports

This section lists RealPresence Collaboration Server (RMX) firewall port requirements when deployed with Skype for Business or 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 Skype for Business 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

Setting 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:

1. Obtain the Trusted Application Service GRUU Identification
2. Configure RealPresence Collaboration Server (RMX) System Flags

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

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

Obtain the Trusted Application Service GRUU Identification

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

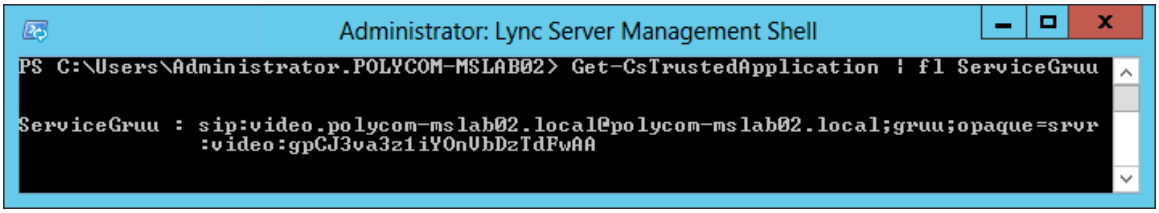
If you are deploying multiple RealPresence Collaboration Servers, the Globally Routable User Agent URI (GRUU) information can be shared as long as the existing Trusted Application Pool and Application ID are used.

To obtain the service GRUU identification:

1 Navigate to **Start > All Programs > Skype for Business Server 2015 > Skype for Business Server Management Shell** to open the Skype for Business 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
```



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 you obtained without the prefix *sip:*. For example, use:

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

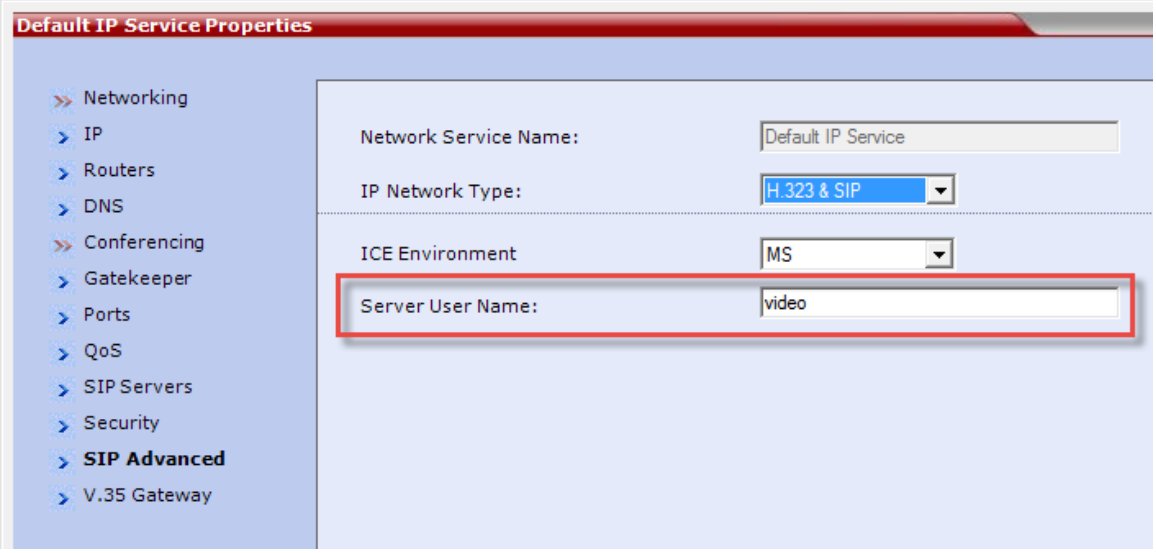
Configure the RealPresence Collaboration Server (RMX) System for Edge Server Support

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

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.

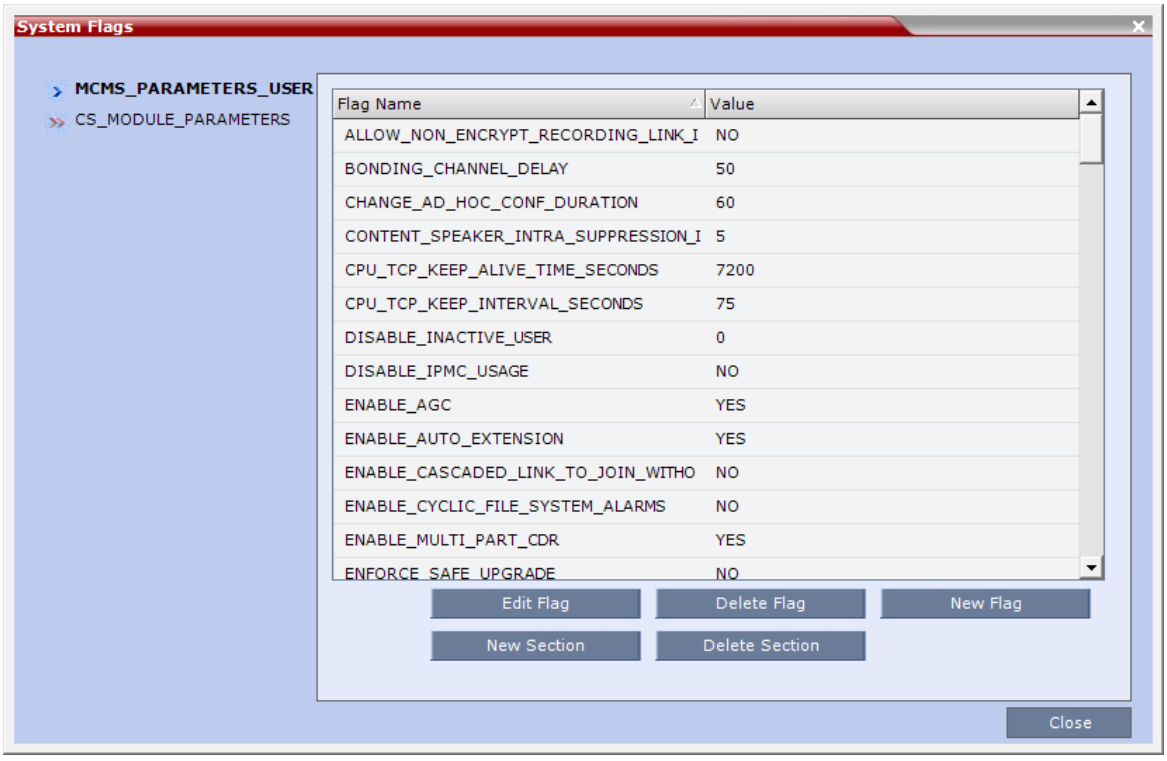
Configuring RealPresence Collaboration Server (RMX) for Polycom ContentConnect software enables the following:

- 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**.

Deploying Polycom RealPresence DMA Systems

When you incorporate Polycom DMA RealPresence systems in a Skype for Business 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 Skype for Business 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 Skype for Business Presence for Virtual Meeting Rooms.
- Integrate with Skype for Business Online Meetings using Polycom RealConnect technology.
- You can use the RealPresence DMA system for calls between endpoints registered to a DMA system and a Skype for Business Server that is SIP peered. Video is supported for calls with Skype for Business and Lync 2010 clients; Lync 2013 clients supports audio-only calls.

To deploy a RealPresence DMA system in a Skype for Business environment, complete the following major tasks for Skype for Business Server and the RealPresence DMA system:

1. Configuring Skype for Business for Use with a RealPresence DMA System
2. Configuring RealPresence DMA System for Skype for Business
3. Enabling RealPresence DMA System for Skype for Business and Polycom RealConnect
4. Enabling RealPresence DMA System for Presence Publishing
5. Configure RealPresence DMA System for Polycom ContentConnect Software

Configuring Skype for Business for Use with a RealPresence DMA System

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

1. Setting the Routing for the RealPresence DMA System
2. Enabling Federation in your Skype for Business Environment

Setting the Routing for the RealPresence DMA System

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

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

- Define Your Trusted Application Pool Using Skype for Business Topology Builder
- (Optional) Define a Static Route for the RealPresence DMA System Using Microsoft PowerShell

Note: 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.

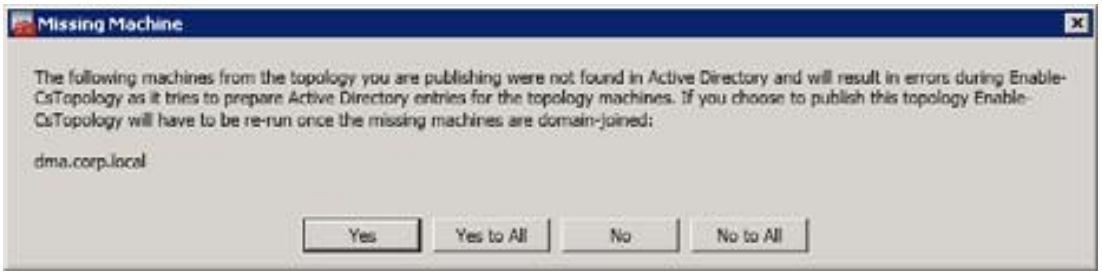
Define Your Trusted Application Pool Using Skype for Business Topology Builder

Before completing this RealPresence DMA task, you must integrate RealPresence Collaboration Server (RMX) with Skype for Business by creating your Trusted Application Pool and Trusted Application Endpoint commands as shown in the section Create the Trusted Application Using Microsoft PowerShell.

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 Skype for Business.
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 Skype for Business 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) Define a Static Route for the RealPresence DMA System Using Microsoft PowerShell

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 > Skype for Business > Skype for Business Management Shell** to open the 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: Polycom recommends enabling VMRs via presence publishing when integrating a RealPresence DMA supercluster with Skype for Business. This provides high-availability without the need to map distinct MatchURIs to specific DMA hosts.

Enabling Federation in your Skype for Business Environment

The second step in configuring Skype for Business 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 Server or Microsoft Office Communications Edge Server.

Complete the following two tasks to enable federation in your Skype for Business environment:

1 Configuring the Microsoft Edge Server

2 Ensuring the Primary SIP Signaling Domain is Allowed

Configuring the Microsoft Edge Server

To include Skype for Business Server or Edge Server in your environment, see Microsoft's detailed instructions Deploy Edge Server in Skype for Business Server 2015.

Microsoft provides a Skype for Business Server 2015 Planning Tool you can use to plan your topology.

Microsoft 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 an Edge Server.

Ensuring the Primary SIP Signaling Domain is Allowed

When federating with another Skype for Business Server environment, ensure that the domain in the MatchURI is allowed on the federated 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 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 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 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 Skype for Business Server for use with a RealPresence DMA system. The second section of this section shows you how to configure your RealPresence DMA system for Skype for Business Server.

Configuring RealPresence DMA System for Skype for Business

This section outlines the following six steps that configure a RealPresence DMA system with Skype for Business:

1. Ensuring DNS is Configured Properly
2. Creating a Security Certificate for the RealPresence DMA 7000 System

Ensuring 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-server cluster has three domain names: one virtual and two physical. A single-server cluster has one (physical) domain name; this configuration has no virtual domain name.
- 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.

Creating a Security Certificate for the RealPresence DMA 7000 System

The second step in configuring a RealPresence DMA system with Skype for Business Server is to install a security certificate on the RealPresence DMA system so that Skype for Business 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 Skype for Business 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.

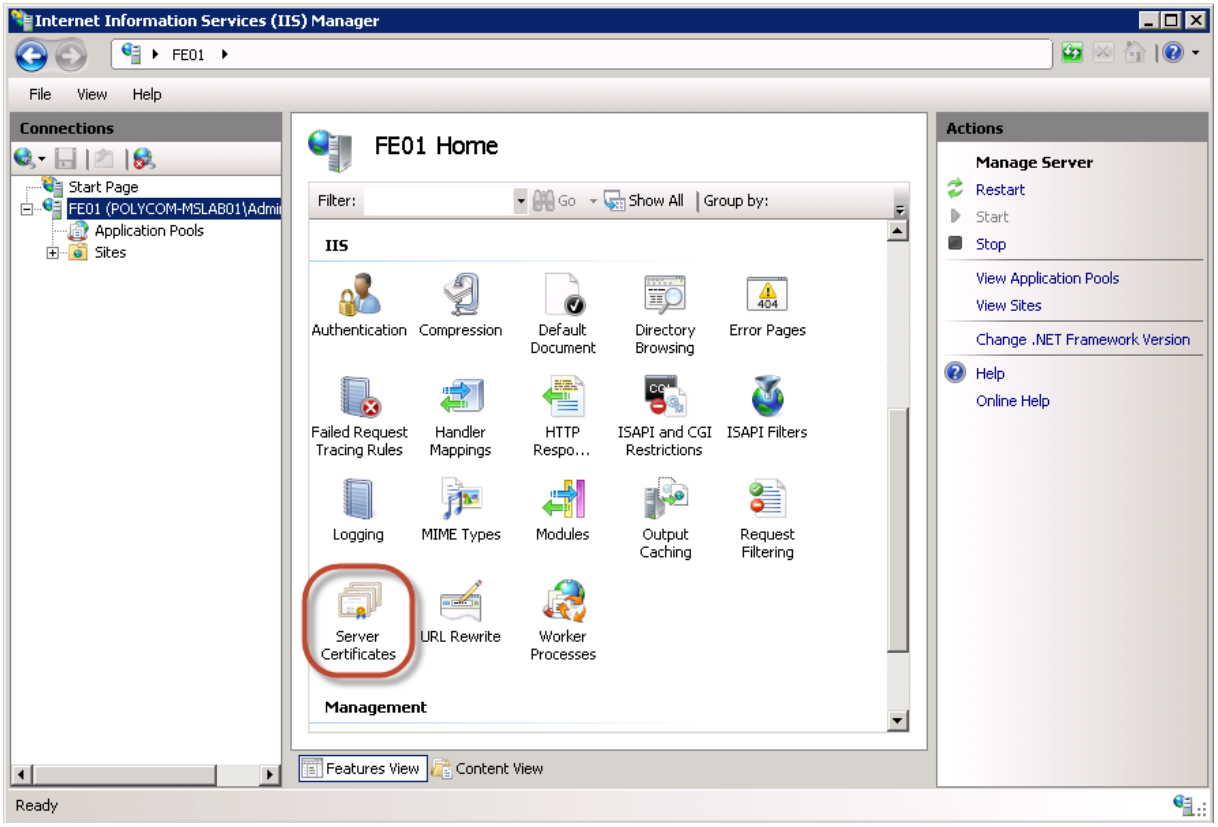
Note: For instructions on creating a MatchURI and provisioning a certificate in Skype for Business, refer to Appendix E: Configuring Static Routes in Skype for Business.

Create a Security Certificate for RealPresence DMA System

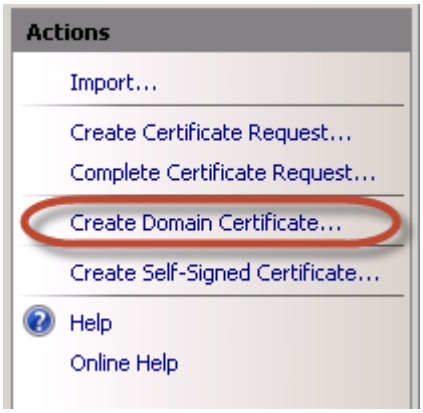
This section shows you how to create a security certificate for the RealPresence DMA system using IIS Manager 7.

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

1. On the Skype for Business 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.



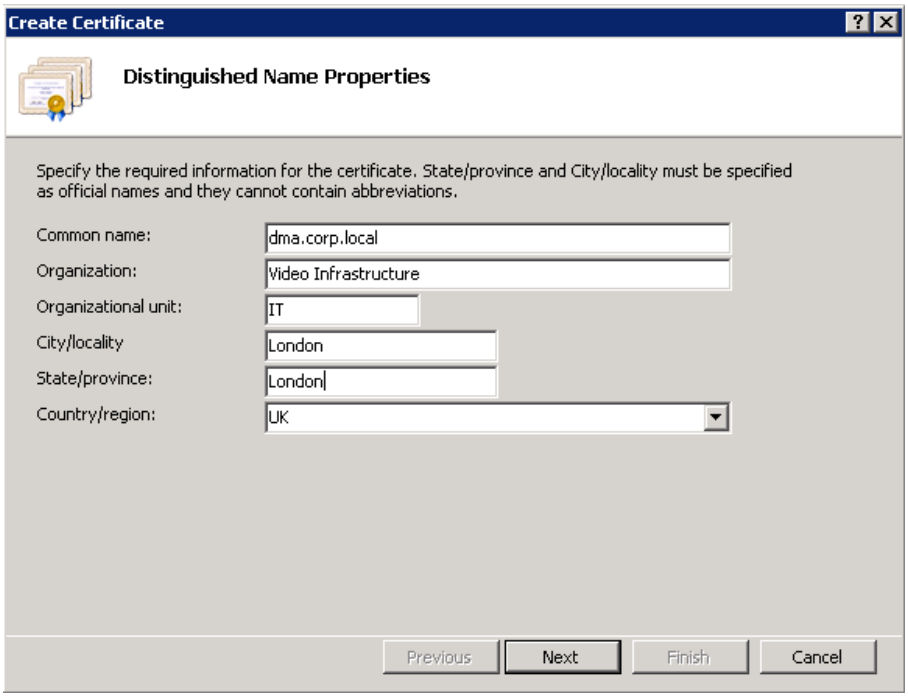
4. In the **Actions** pane (far right), select the **Create Domain Certificate**, shown next.



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.



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.

Export a Certificate for the RealPresence DMA System

After you create a security certificate for the RealPresence DMA system, export the certificate using the Microsoft Management Console.

To export the certificate using the Microsoft Management Console:

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.

Validating a Certificate on the Skype for Business Server

After creating a security certificate on a Polycom DMA system, validate the certificate on the Skype for Business Server. If you do not validate the certificate, the Skype for Business Server will be unable to open port 5061 to the Polycom DMA system, which can cause issues for matchURI dialing and for CSS gateway participants in calls using Polycom RealConnect technology.

For instructions on configuring a certificate, refer to Configure a Certificate.

Validating a Certificate for a Multicomputer Trusted Application Pool

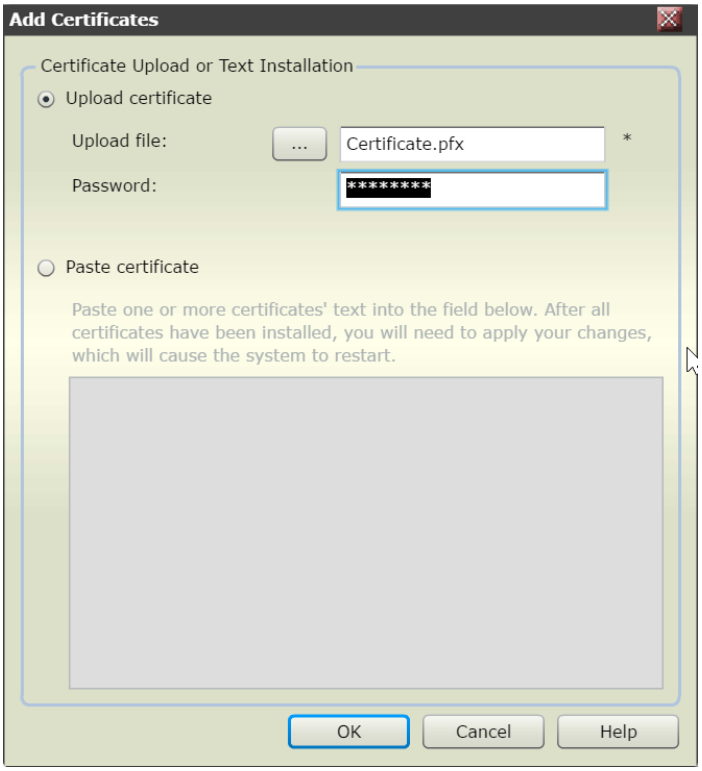
In a Skype for Business deployment, a server that is a member of a multicomputer trusted application pool must contain its computer FQDN as a subject or Subject Alternative Name (SAN) in its certificate, as well as in the FQDN of the multicomputer pool present in the SANs of the certificate. For example, in a Skype for Business topology, customerA has a multicomputer trusted application pool called *polycomKB.customer.com*, which contains a DMA with the FQDN *dmaKB.customer.com*.

Install a Certificate

You can add a Subject Alternative Name (SAN) using a PFX certificate created outside of Polycom DMA system, and install the certificate to Polycom DMA system.

To install a certificate:

1. On the Polycom DMA system, go to **Admin > Local Cluster > Certificates** and select **Upload Certificate**.
2. In **Upload File**, browse to the correct PFX certificate and enter the password.



3. Click **OK**.

Enabling Skype for Business for Polycom RealConnect

Polycom RealPresence Collaboration Server (RMX) solution and RealPresence DMA system introduce Polycom RealConnect technology for Skype for Business, a new RealPresence platform function for

Skype for Business customers. Polycom RealConnect technology enables you to dial into scheduled Skype for Business 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 Skype for Business.

The figure Skype for Business Invitation with Conference ID shows a Skype for Business invitation populated with a Conference ID, which is provided automatically by Skype for Business Server and represents the H.323 number or SIP URI you dial on the standards-based endpoint.

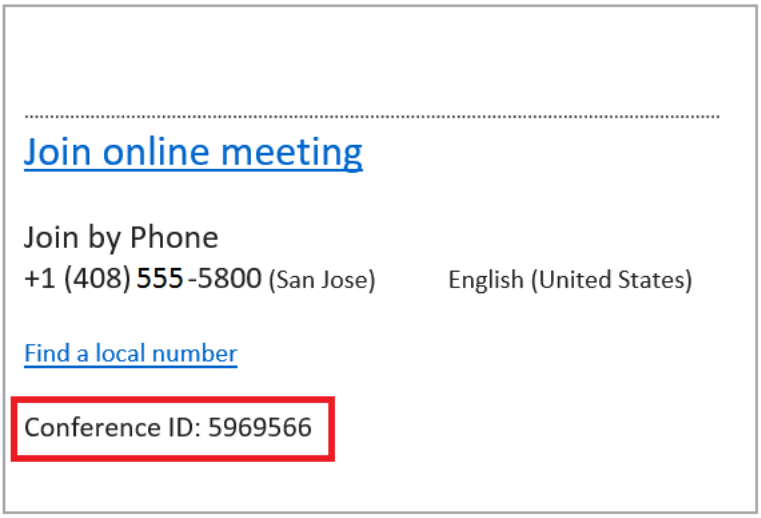
For example:

5969566

5969566@dmadomain.net

Web Info: Conference IDs are generated only when you deploy Skype for Business 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 Skype for Business dial-in conference deployment steps, refer to Microsoft's Configure dial-in conferencing in Skype for Business Server 2015.

Skype for Business invitation with conference ID

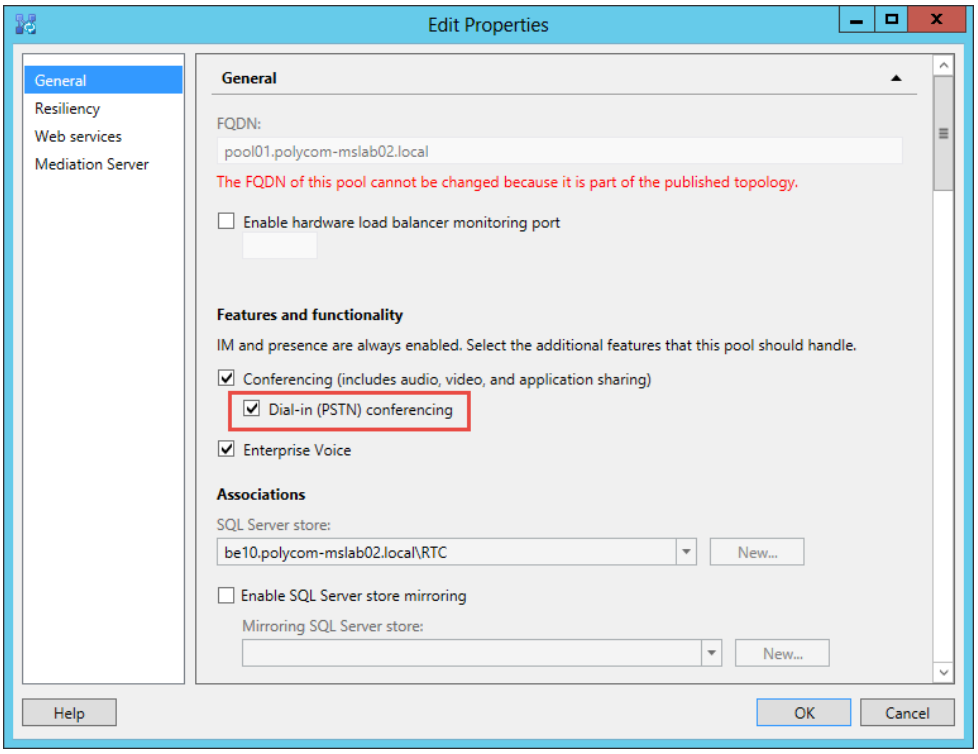


Enable Dial-in Conferencing

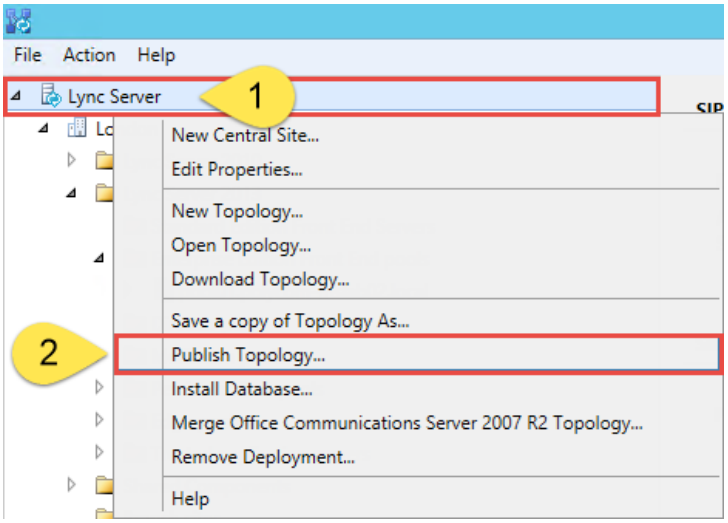
This section shows you how to enable Dial-in Conferencing.

To enable Dial-in Conferencing:

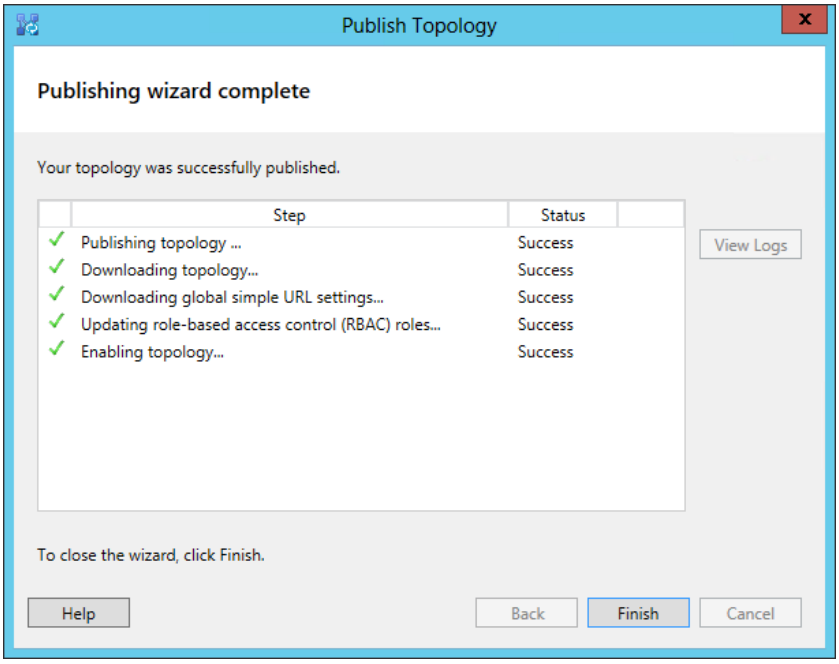
1. Install the dial-in (PSTN) conferencing component for the front end server or pool in the Skype for Business topology builder by going to **Edit Properties > General > Features and Functionality**.
2. Check **Dial-in (PSTN) conferencing** and click **OK**.



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 Skype for Business Server by running the Skype for Business bootstrapper process.

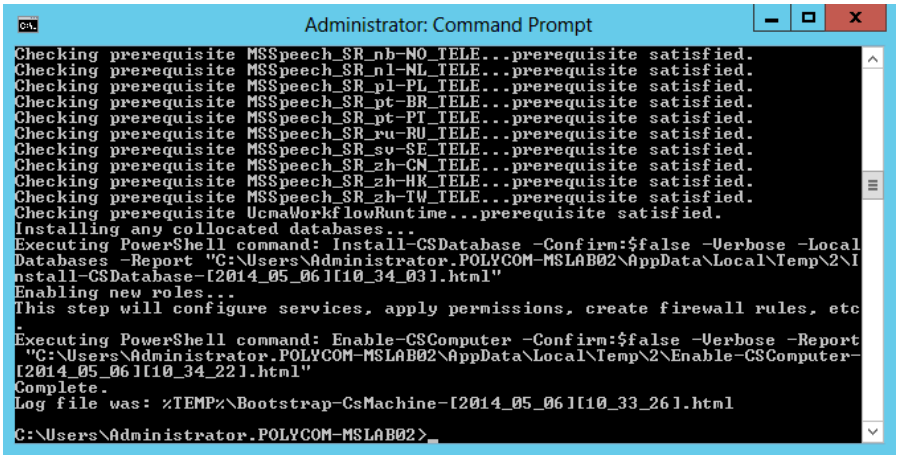
Install the Dial-In Conferencing Services

After you enable dial-in conferencing, install the dial-in conferencing services.

To install the dial-in conferencing services:

1. Open the command prompt on your front end server and execute the command:

```
C:\Program Files\Skype for Business Server 2015\Deployment\Bootstrapper.exe
```



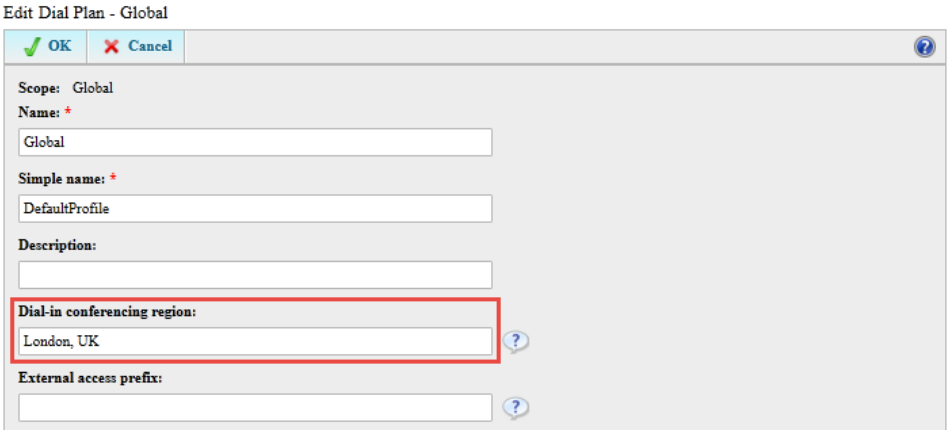
2. Install the associated service by opening the Skype for Business Server Management Shell and executing `Start-CSWindowsService`.

Configure the Dial-in Conferencing Region

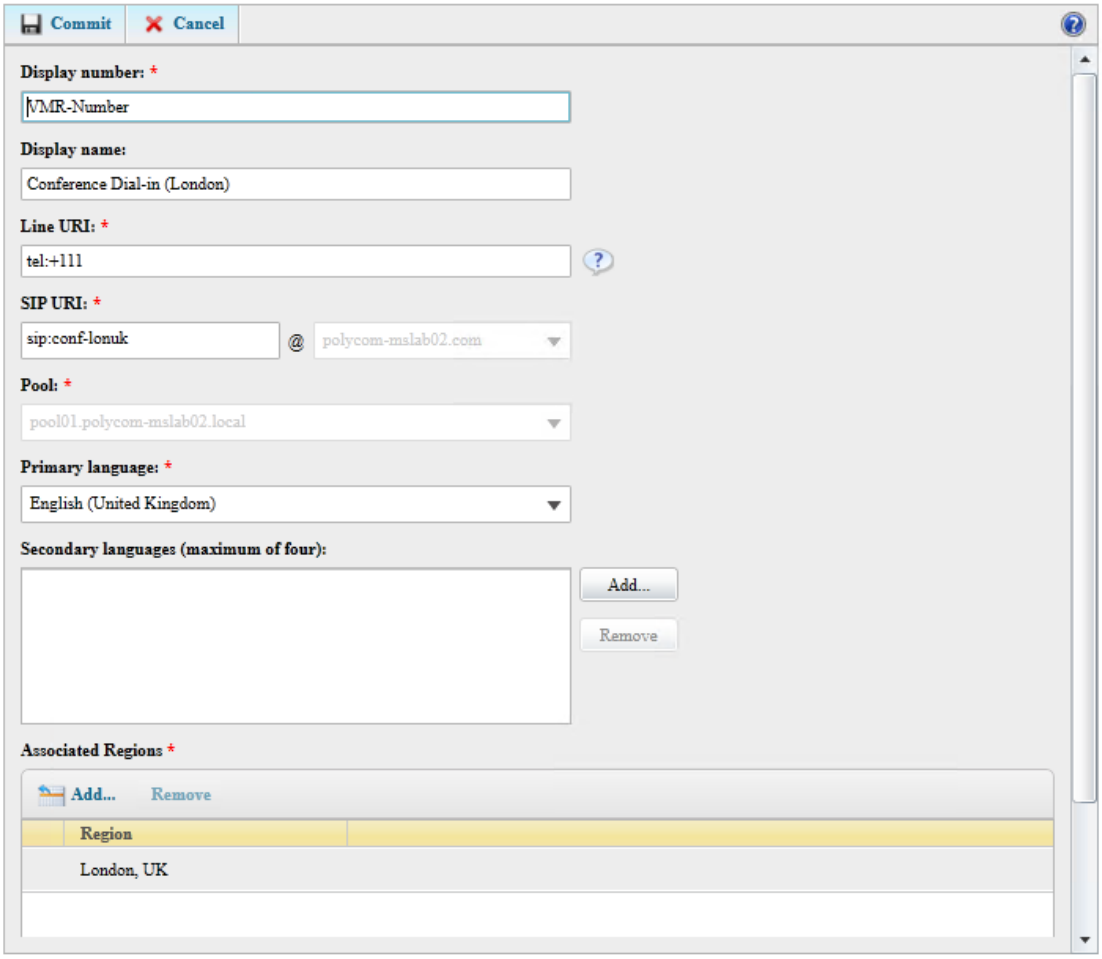
Next, configure a dial-in conferencing region. Typically, you will need to configure multiple regions and assign local access numbers. In the following example, we add a default region in order to generate an H.323 or standard SIP number that users can dial into from any standards-based room system.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

To configure the dial-in conferencing region:

1. Open the **Skype for Business 2015 Server Control Panel** and go to **Voice Routing > Edit the Global Dial Plan > Dial-in conferencing region**.



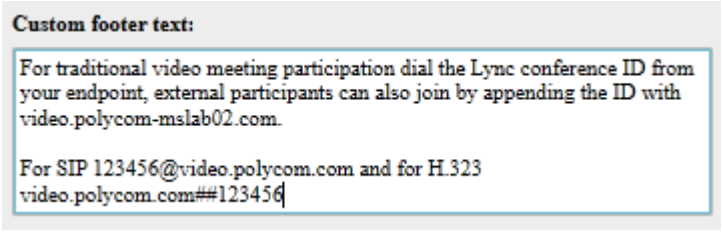
2. Specify a dial-in access number by going to **Skype for Business 2015 Server Control Panel > Conferencing > Dial-in Access Number > New** and completing the following fields:
   - **Display number** This field permits alphanumeric entry. This is typically the dial-in access number. This example uses 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.



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 **Skype for Business 2015 Control Panel**, go to **Conferencing > Meeting Configuration**.

4 Edit the default global template as shown next.



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 Skype environment now includes Conference IDs in Skype for Business-enabled meeting invitations.

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

Enabling RealPresence DMA System for Polycom RealConnect

This section shows you how to configure the RealPresence DMA system for Polycom RealConnect and includes the following major tasks:

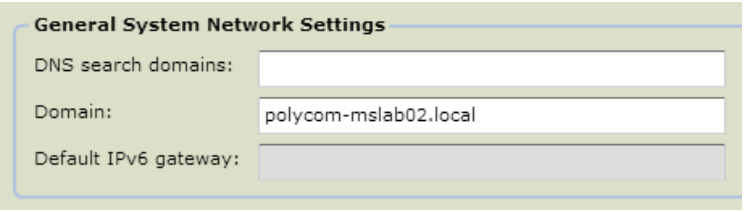
1. Configure Domain and Time
2. Enabling Multiple SIP Domains for Polycom RealConnect On-Premises
3. Add a Skype for Business Server as an External SIP Peer
4. Configure a Conference Template for Polycom RealConnect
5. Configure the Skype for Business Dial Rule
6. Create a Dial Rule to Support Polycom ContentConnect or MMCU with Soft Blades
7. Enable the Panoramic Layout for Skype for Business Calls
8. Enable Skype for Business AVMCU-to-MCU Affinity for On-Premises Polycom RealConnect Conferences

Configure Domain and Time

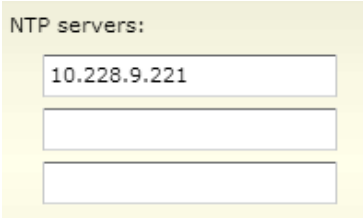
Next, specify domain and time on the RealPresence DMA system.

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.**



2. Configure the time to synchronize with the same source as the Skype for Business 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.



Enabling Multiple SIP Domains for Polycom RealConnect On-Premises

You must complete the additional steps in this section to enable Polycom RealConnect. If you have not done so already, add your Skype for Business external SIP peer for your primary domain.

Configure the Skype for Business external SIP peer for each front-end pool in each domain. For example, if your Skype for Business deployment consists of the following, you need to configure the following external SIP peers in the Polycom DMA system:

Domain: `domain1.com`

Front End pools:

- `NALA-pool.domain1.com`
- `APAC-pool.domain1.com`

Domain: `domain2.com`

Front End pools:

- `NALA-pool.domain2.com`
- `EMEA-pool.domain2.com`
- `ASIA-pool.domain2.com`

Add a Skype for Business Server as an External SIP Peer

You can add the Skype for Business Server as an external SIP peer and reference these SIP peers in dial rules when:

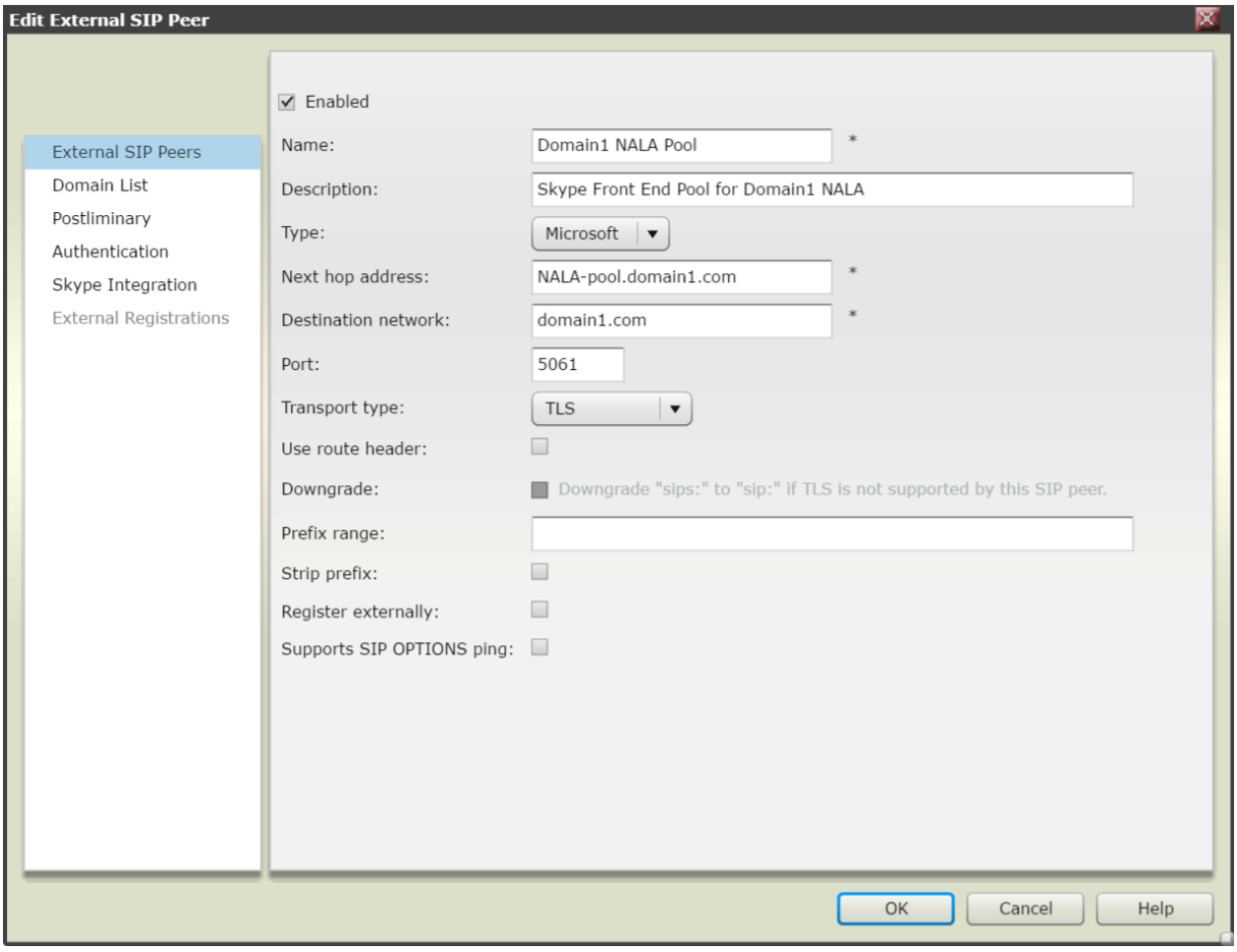
- Using Polycom RealConnect technology with an on-premises Skype for Business deployment. Refer to Configure the Skype for Business Dial Rule.
- Sharing content with Polycom ContentConnect. Refer to Create a Dial Rule to Support Polycom ContentConnect or MMCU with Soft Blades.
- Using Skype for Business AVMCU-to-MCU Affinity. Refer to Enable Skype for Business AVMCU-to-MCU Affinity for On-Premises Polycom RealConnect Conferences.

To add the Skype for Business Server as an external SIP peer:

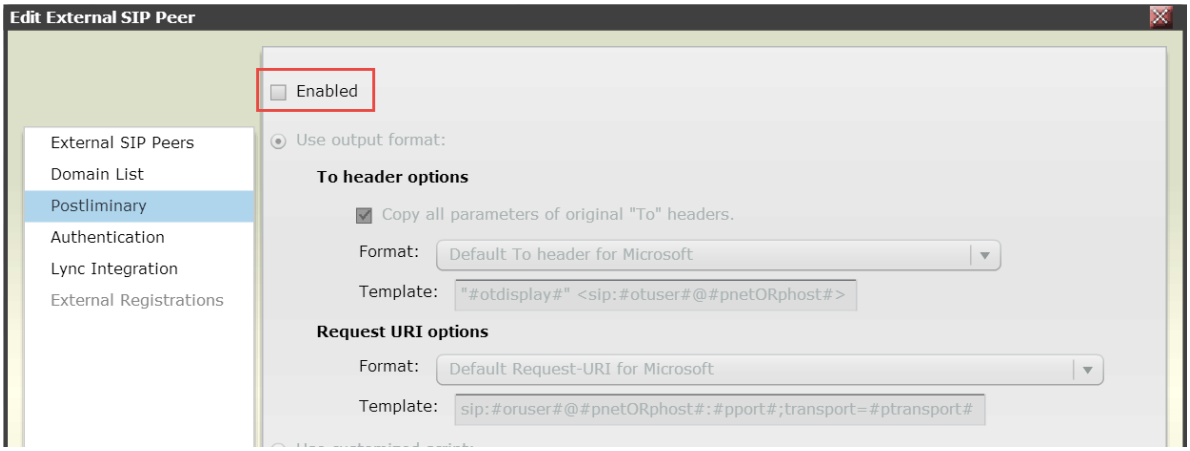
1. In the **DMA administrator** console go to **Network > External SIP Peers > Add**. Complete the following fields:
   - **Name** Enter the name you gave to this Skype for Business Front End Server or Pool. For example, `Domain1 NALA Pool`.

- **Description** Enter a description for Name field. For example, Skype Front End Pool for Domain1 NALA
- **Type** Choose **Microsoft**.
- **Next hop address** Enter the FQDN for your Front End Server or Pool. For example, `NALA-pool.domain1.com`.
- **Destination network** Enter the SIP domain used for Polycom RealConnect conferences. This is not necessarily the same as the domain extension for your Skype for Business Front End Server or your Pool. For example, `domain1.com`.
- **Port** Enter 5061.
- **Transport type** Enter TLS.

You can leave the remaining fields blank. Continue to create External SIP Peers for additional domain as shown in the following figure.



2 Ensure that the postliminary is not enabled.



Obtain the Trusted Application Service GRUU Identification

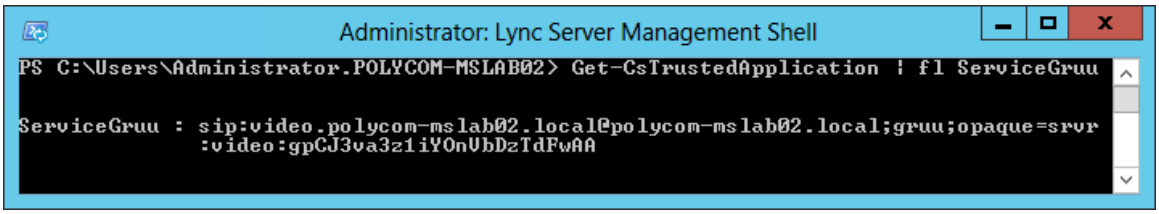
Use PowerShell to obtain the Globally Routable User Agent URI GRUU. If you are deploying multiple external SIP domains, the GRUU information can be shared as long as you are using the existing Trusted Application Pool and Application ID.

In prior releases, creating an account in Active Directory was necessary only for Skype for Business deployments with an Edge Server deployed to facilitate federated or remote worker calling. You must now enable ICE with or without Edge Server deployments.

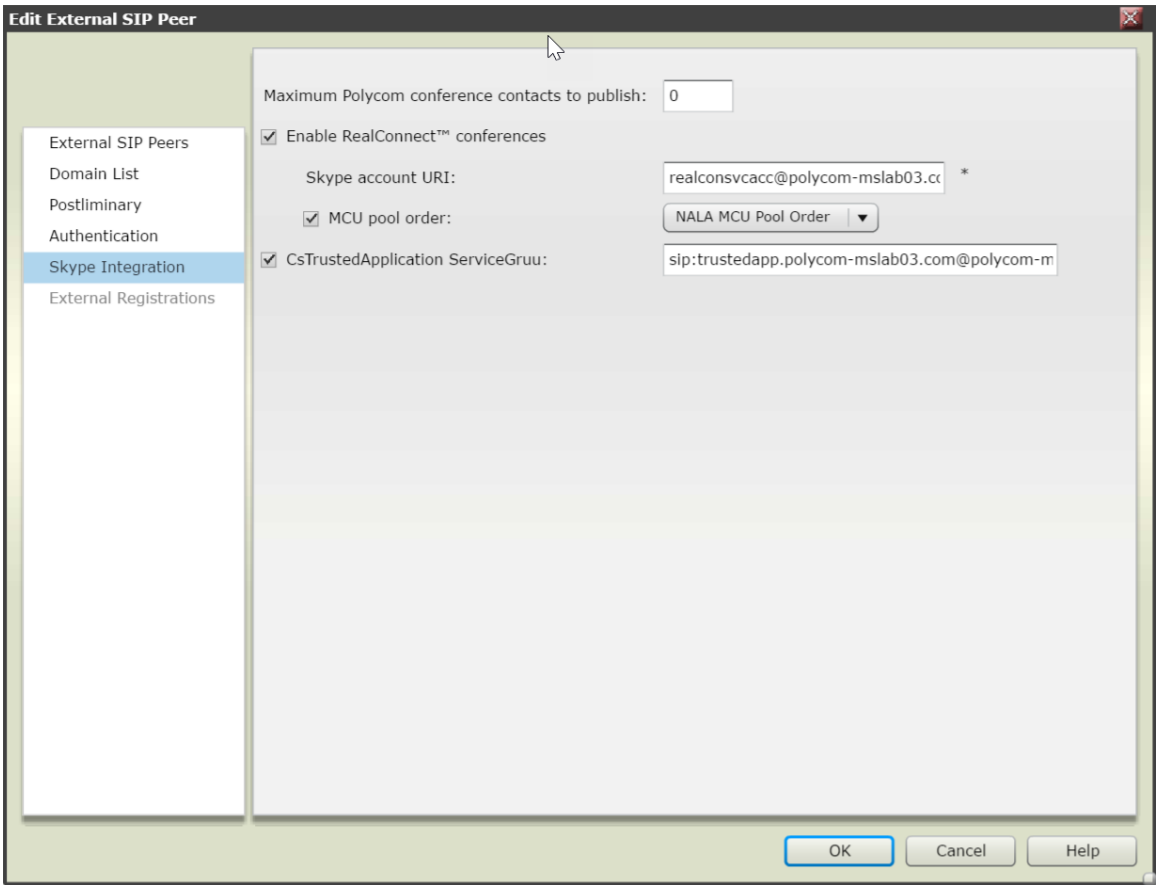
To obtain the service GRUU identification:

1. Navigate to **Start > All Programs > Skype for Business 2015 > Lync Server Management Shell** to open the Skype for Business PowerShell terminal.
2. Use the `Get-CsTrustedApplication` command to display the service GRUU information and make note of the information.

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



3 In the left window, click **Skype for Business Integration** and enter the GRUU you obtained to the **CsTrustedApplication ServiceGruu** field.

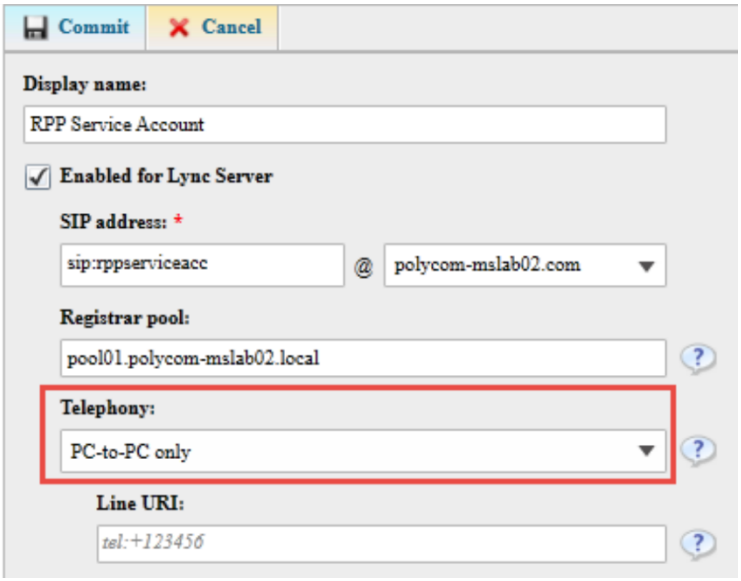


4 In **Maximum Polycom conference contacts to publish**, enter the maximum number of VMRs you are publishing presence for. This field is not required for Polycom RealConnect. Polycom recommends you set this to the maximum of 25,000.

5 Check **Enable RealConnect conferences**.

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

Edit Skype for Business Server user – RealPresence Platform service account



Configure a Conference Template for Polycom RealConnect

This section shows you how to create a RealPresence DMA system conference template for Polycom RealConnect technology.

You can have many conference templates in the system that you can use for Skype for Business and select by a dial rule. You must set the following constraints for Skype for Business conference templates:

- Conference mode (must be AVC only)
- If you are using the MMCU with soft blades, enable Microsoft Remote Desktop Protocol (RDP) content
- For Microsoft AVMCU Cascade Mode, select Resource optimized or Video optimized
- (Optional) Enable panoramic layout as shown in Enable the Panoramic Layout for Skype for Business Calls.
- Send content to legacy endpoints

To configure a RealPresence DMA system conference template for Polycom RealConnect:

1. Create the template with the name RealConnect Template.
2. On the **Polycom MCU General Settings** tab, set **Conference Mode** to AVC only.
3. On the **Polycom MCU General Settings** tab, select a value for the Microsoft AVMCU cascade mode: **Resource optimized** or **Video optimized**.
4. On the **Polycom MCU Video Quality** tab, select **Send content to legacy endpoints**.
5. Click **Ok**.

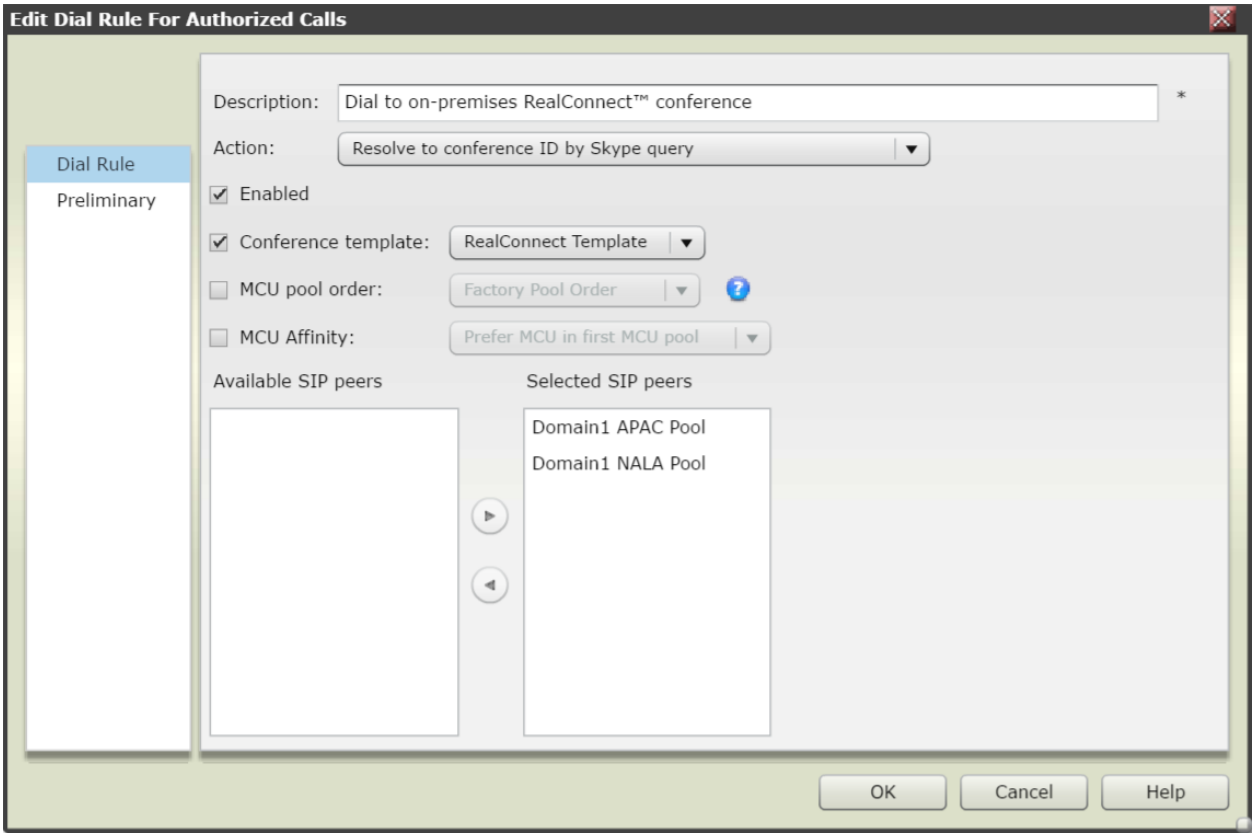
Configure the Skype for Business Dial Rule

Next, create a dial rule to assign to Polycom RealConnect Skype for Business conferences.

To configure a dial rule:

1. Go to the **DMA Admin screen > Call Server > Dial Rules**.
2. Highlight **Dial to on-premises RealConnect conference** and select **Edit**.

   The Description field displays *Dial to on-premises RealConnect Conference*.



3. Select **Enabled** to enable the dial rule.
4. Select **Conference Template** and in the drop-down menu, select a conference template you created in Configure a Conference Template for Polycom RealConnect.
5. From **Available SIP peers** select any of the SIP peers you created in Add a Skype for Business Server as an External SIP Peer to use for Polycom RealConnect conferences.
6. Click **OK.**

Create a Dial Rule to Support Polycom ContentConnect or MMCU with Soft Blades

Create a dial rule to support Polycom ContentConnect or MMCU with soft blades.

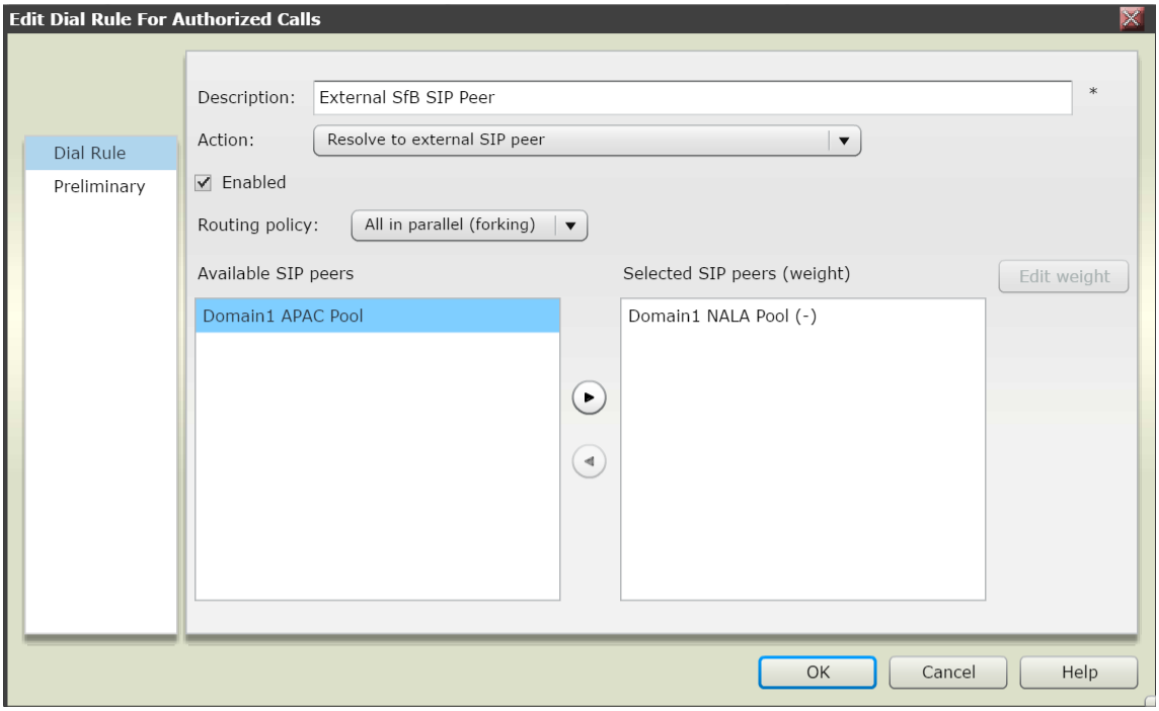
Note: The MMCU with soft blades is an alternative to the Microsoft transcoding functionality of Polycom ContentConnect. If you are using the MMCU with soft blades to transcode content, do not use Polycom ContentConnect.

To create a dial rule to support Polycom ContentConnect or the MMCU with soft blades:

1. On RealPresence DMA system, go to **Admin > Call Server > Dial Rules,** click **Add**.

   The Edit Dial Rule for Authorized Calls dialog displays.

2. In **Action**, select **Resolve to external SIP peer** and enter a description, for example, 'External Skype for Business SIP Peer'.



3. Add a SIP peer you created in Enabling Multiple SIP Domains for RealConnect On-Premises.

   The available SIP peer you assigned displays in Selected SIP peers.

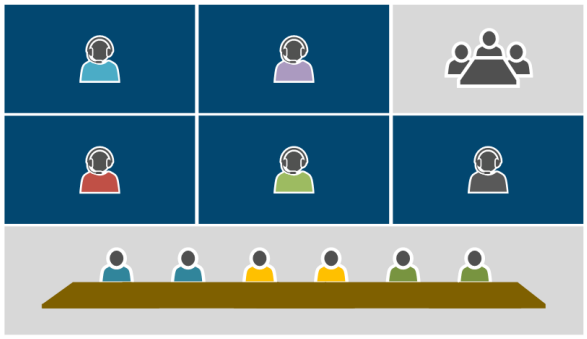
4. Select **Enabled** to enable the dial rule.
5. Select the conference template you created in Configure a Conference Template for Polycom RealConnect.
6. Select **Send content to legacy endpoints**.
7. Click **OK.**
8. Ensure that the dial rule displays in the last position.
9. Repeat this procedure for each SIP peer you created previously.

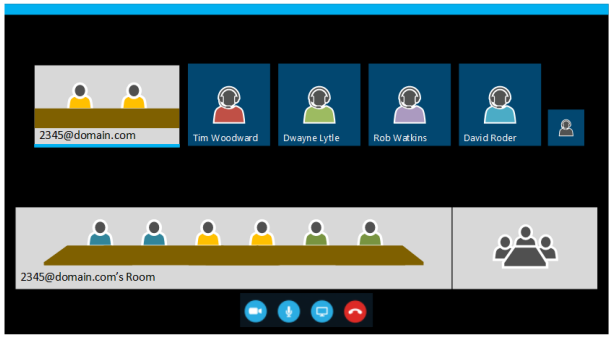
Enable the Panoramic Layout for Skype for Business Calls

When using RealPresence Collaboration Server version 8.7.1 or later, the Skype for Business client can display a panoramic video strip containing all participants in an immersive telepresence room, a Polycom® RealPresence Centro™, or an additional four standards-based endpoints during video conferences with the active speaker displaying in Gallery View.

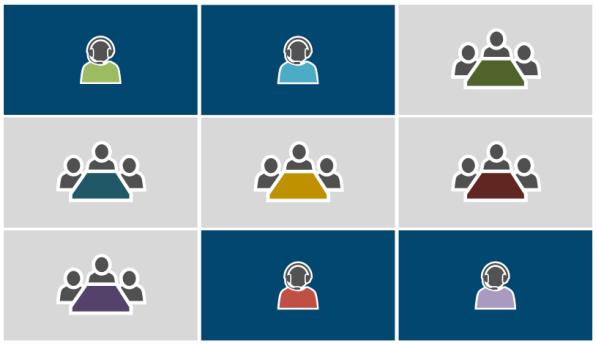
The following figures illustrate the standard and immersive scenarios. The left-side figures illustrate the viewpoint from a standards-based endpoint; the right-side figures illustrate the viewpoint from the Skype for Business client.

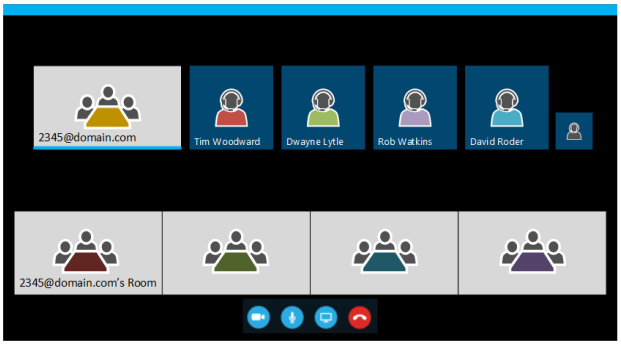
Immersive Video Teleconferencing – Panoramic Layout with Polycom RealConnect





Standard Video Teleconferencing – Panoramic Layout with Polycom RealConnect





The following procedure shows you how to enable the panoramic layout.

Note: To use panoramic layout with Microsoft environment conferences, you must use Polycom® RealPresence® Collaboration Server version 8.7.1 or later.

To enable the panoramic layout:

1. In the conference template you created in Configure a Conference Template for Polycom RealConnect, select **Polycom MCU General Settings > Advanced Settings**.
2. Click to select the checkbox for **Enable MS panoramic layout**.

Enable Skype for Business AVMCU-to-MCU Affinity for On-Premises Polycom RealConnect Conferences

Skype for Business AVMCU-to-MCU Affinity minimizes the use of WAN bandwidth by using co-located Polycom MCUs with their corresponding Skype front end pools.

By default, when a RealConnect conference starts, the Polycom MCU is selected based on the MCU pool order specified in the dial rule *dial to on-premises RealConnect conference*. You can override the MCU pool order you configured in the dial rule by associating a different MCU pool order with specific Skype for Business front end pools. Overriding this dial rule allows you to select Collaboration Server solution MCUs that are geographically close to specific front end pools. If the RealConnect conference is hosted on an AVMCU within a front end pool with an associated MCU pool order, that MCU pool order is used.

To enable the Skype for Business AVMCU-to-MCU Affinity, ensure that you define a distinct external SIP peer for each Skype for Business front end pool. For instructions, refer to Add a Skype for Business Server as an External SIP Peer.

Repeat the following procedure for each front end pool.

To enable Skype for Business AVMCU-to-MCU Affinity:

1. In **Network > External SIP Peers**, add or edit the external SIP peer that corresponds to a specific front end pool.
2. Verify that the next hop address specifies the FQDN for the front end pool.
3. Select the Skype Integration tab.
4. Verify that **Enable RealConnect™ conferences** is selected.
5. Verify that the Skype account URI is configured.
6. To override the MCU pool order that is specified in the resolve to conference ID by Skype query dial rule, click the checkbox for the MCU pool order field and select an MCU pool order. You may need to define MCU pool orders that contain the MCU pools and MCUs that are preferred for this front end pool. Note also that the MCU pool order must contain all the MCUs that are acceptable for use for RealConnect conferences hosted on an AVMCU in this front end pool.

Enabling RealPresence DMA System for Presence Publishing

As of RealPresence DMA system 6.1, you can publish Skype for Business 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 Skype for Business 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 Skype for Business 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. 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 Front End Server.

Note: 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 Skype for Business.

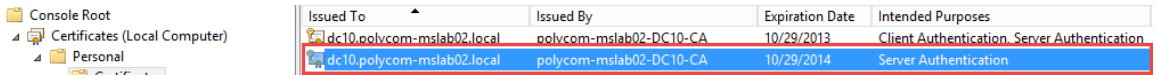
If a Server Authentication certificate is not already present within the personal certificate store on the Domain Controller, you must first enable remote PowerShell to create an SSL certificate, which is required for RealPresence DMA system and all domain controllers. You can check for a server authentication certificate.

Check for a Server Authentication Certificate

Check for a server authentication certificate.

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**.



- 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 RealPresence Distributed Media Application (DMA).

  If you want to request and obtain a certificate from your enterprise CA, 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.

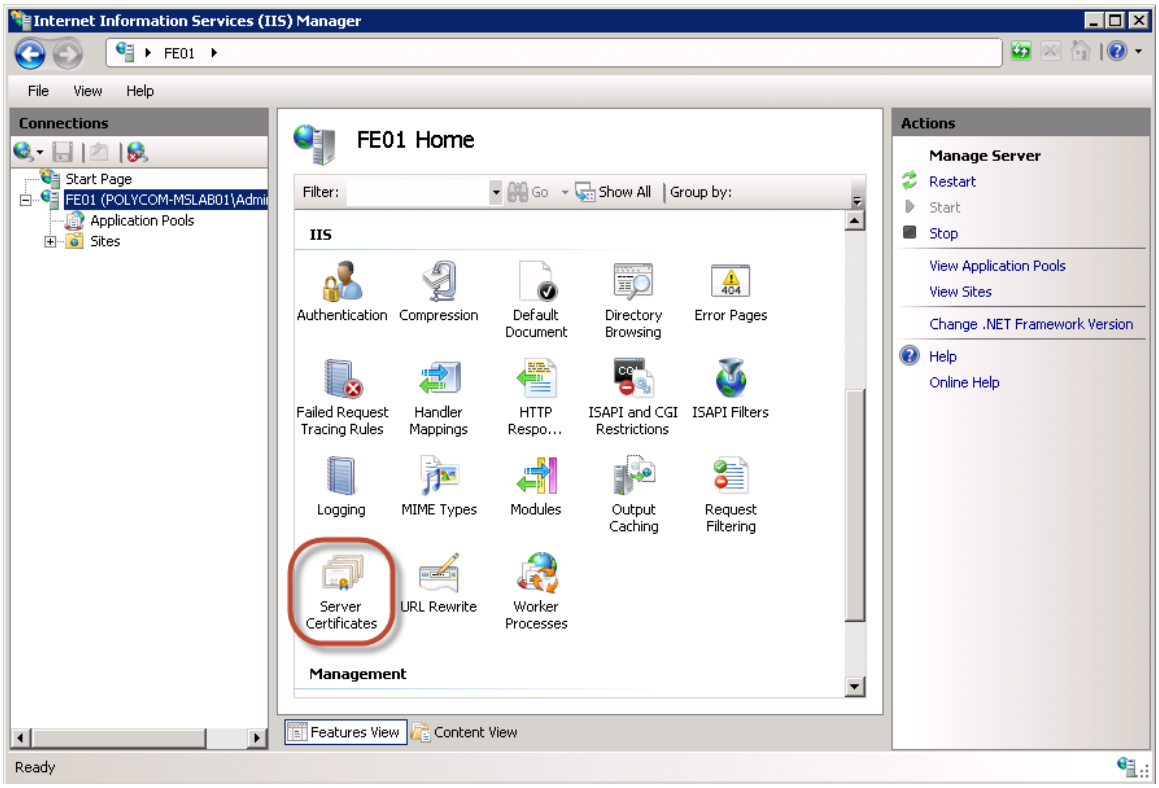
Create a Security Certificate for Windows Remote Management using IIS Manager 7

This section shows you how to create a security certificate for Windows Remote Management using IIS Manager 7.

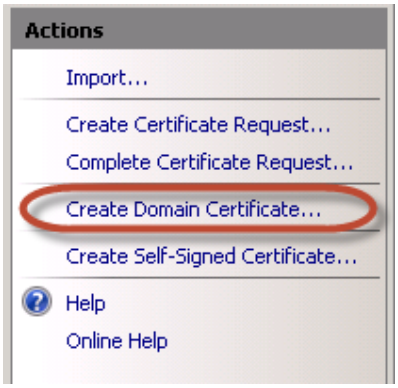
To create a security certificate using IIS Manager 7:

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.



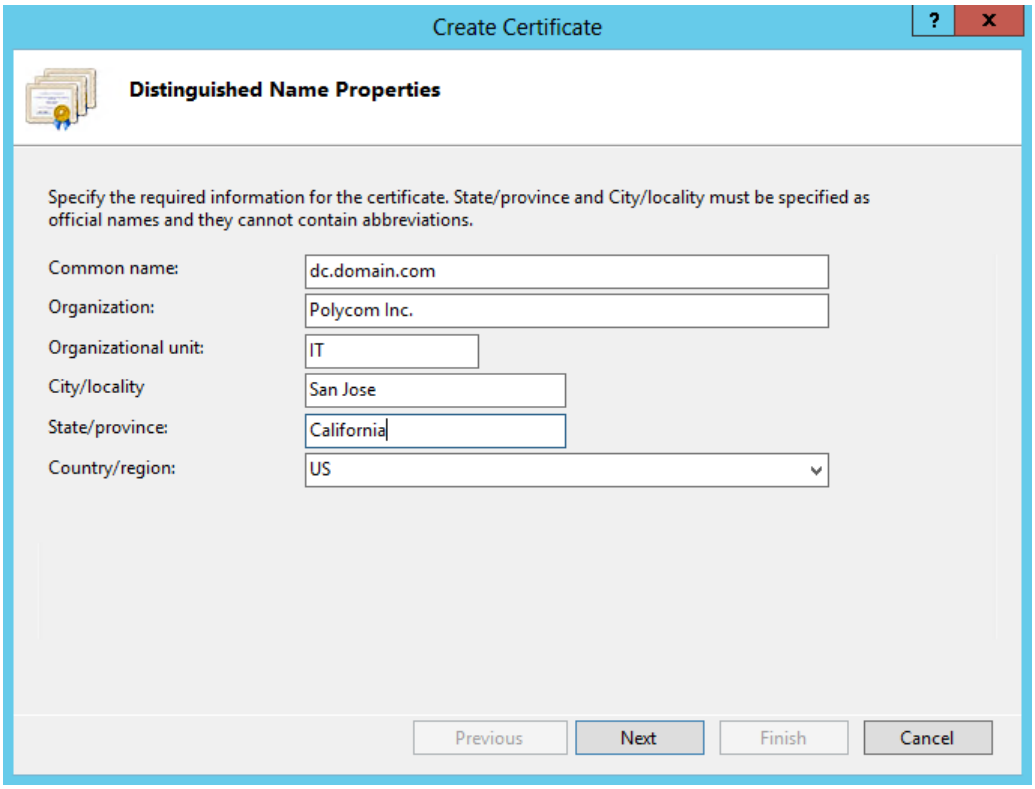
4 In the **Actions** pane (far right), select **Create Domain Certificate**, shown next.



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.

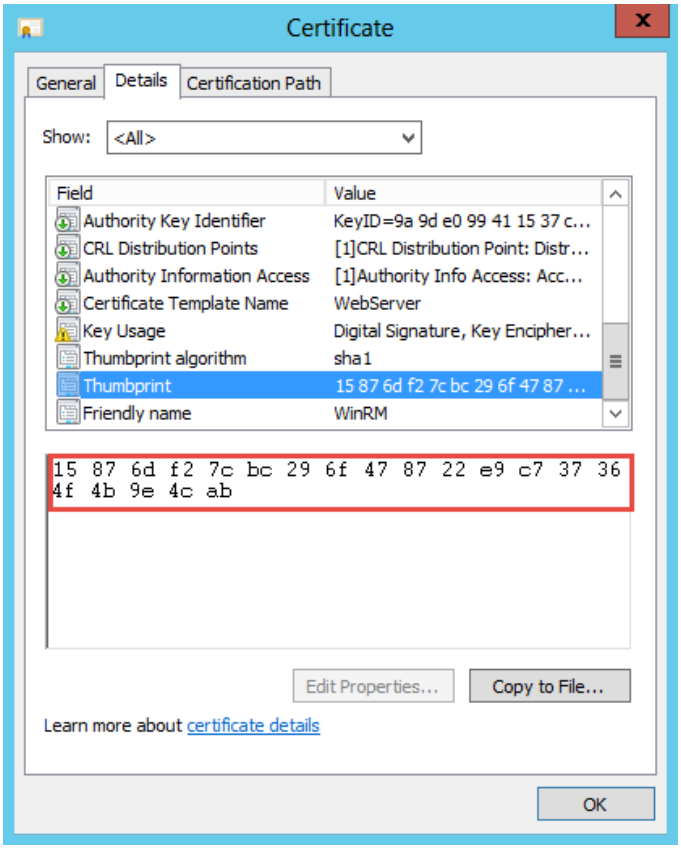


6 Click **Next**.

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, shown next.



Create a Windows Remote Management Listener with the Corresponding Certificate

After you create a security certificate, 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 Skype for Business 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 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 Fe1.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.

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
```

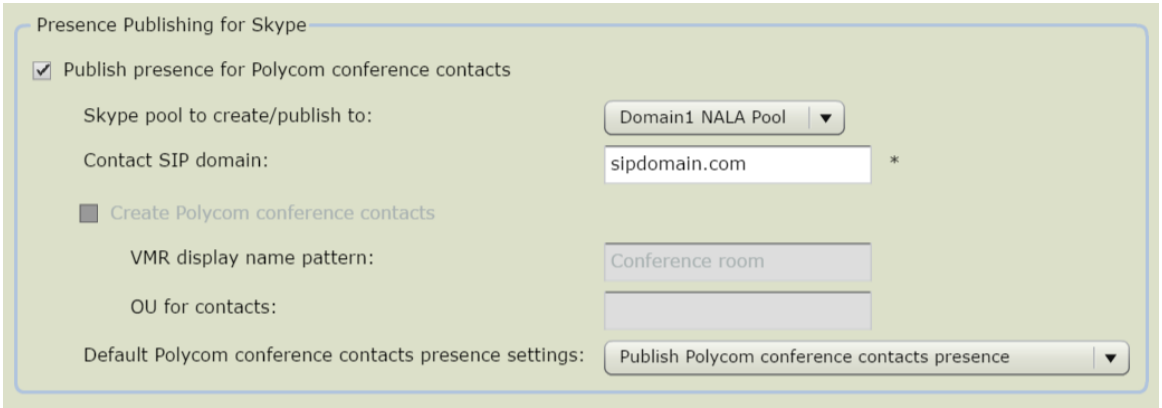
Publish Presence for Skype for Business VMR Contacts

You can publish presence for VMR contacts.

To publish presence for VMR contacts:

1. On the RealPresence DMA system, go to **Admin > Conference Manager > Conference Settings**.
2. Under **Presence Publishing for Skype**, select **Publish Presence for Polycom conference contacts** and complete the following fields:
   - In **Skype pool to create/publish to:**, select the External SIP peer for Skype pool where the VMR contacts reside.
   - In **Contact SIP domain:**, 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 Skype for Business administrator.



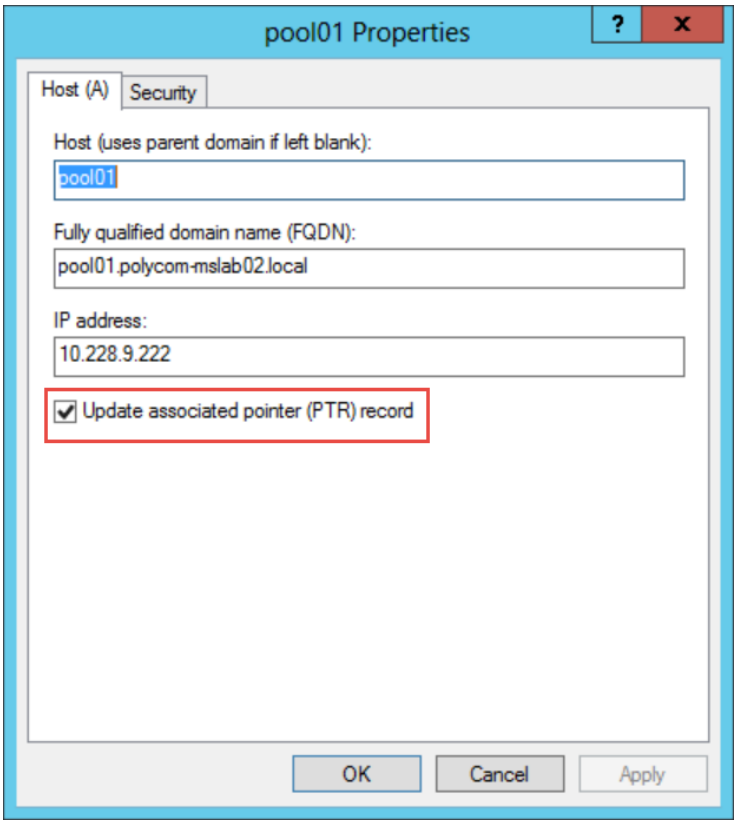
3 If you want to automatically create Polycom conference contacts, select **Create Polycom conference contacts**. This option is available only if you have configured the RealPresence DMA system to integrate with Microsoft Active Directory and the Domain field to indicate the Active Directory domain you want the DMA system to create and publish contacts. If you do not select this option, you must create contacts manually. Complete the following fields:

   - In **VMR display name pattern**, enter a VMR display name pattern you want to use as a naming convention for all contact names.

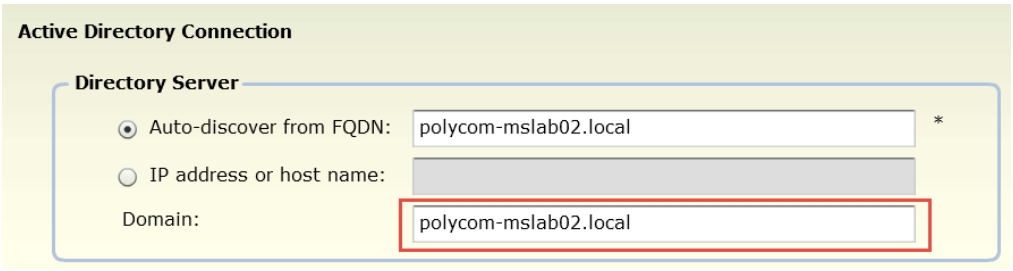
4 (Optional): The Organizational Unit (OU) you enter here assigns an individual Active Directory container or organizational unit in the order that RealPresence DMA system contacts are situated independently from Active Directory Users and Groups. If you do not enter an OU, the RealPresence DMA system 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. For instructions on creating an organizational unit, refer to Create an Organizational Unit

5 If you are deploying Enterprise Skype for Business Pools with manual records, ensure that reverse lookup is possible by selecting **Update associated pointer (PTR) record**, as shown next.

   When you set RealPresence DMA system to automatically create VMRs with Skype for Business and you create Skype for Business-enabled publish presence contacts within Active Directory, DMA uses PTR records to perform discovery for Active Directory and Skype for Business Servers.



6 Go to **Admin > Integrations > Active Directory Connection**, and in the **Domain** field, enter the FQDN of the active directory domain where you create contacts for your Active Directory domain. Complete this field during Active Directory integration.

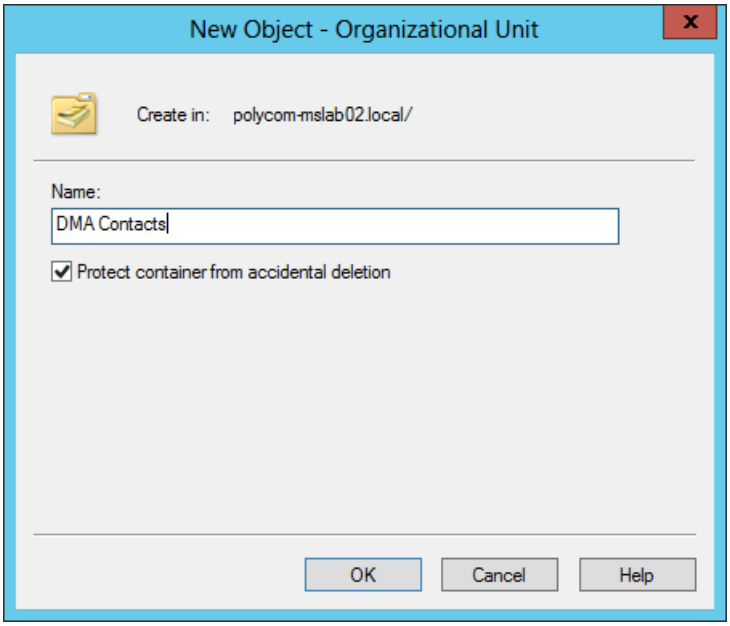


Create an Organizational Unit

After you publish presence for VMR contacts, create an organizational unit (OU).

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.

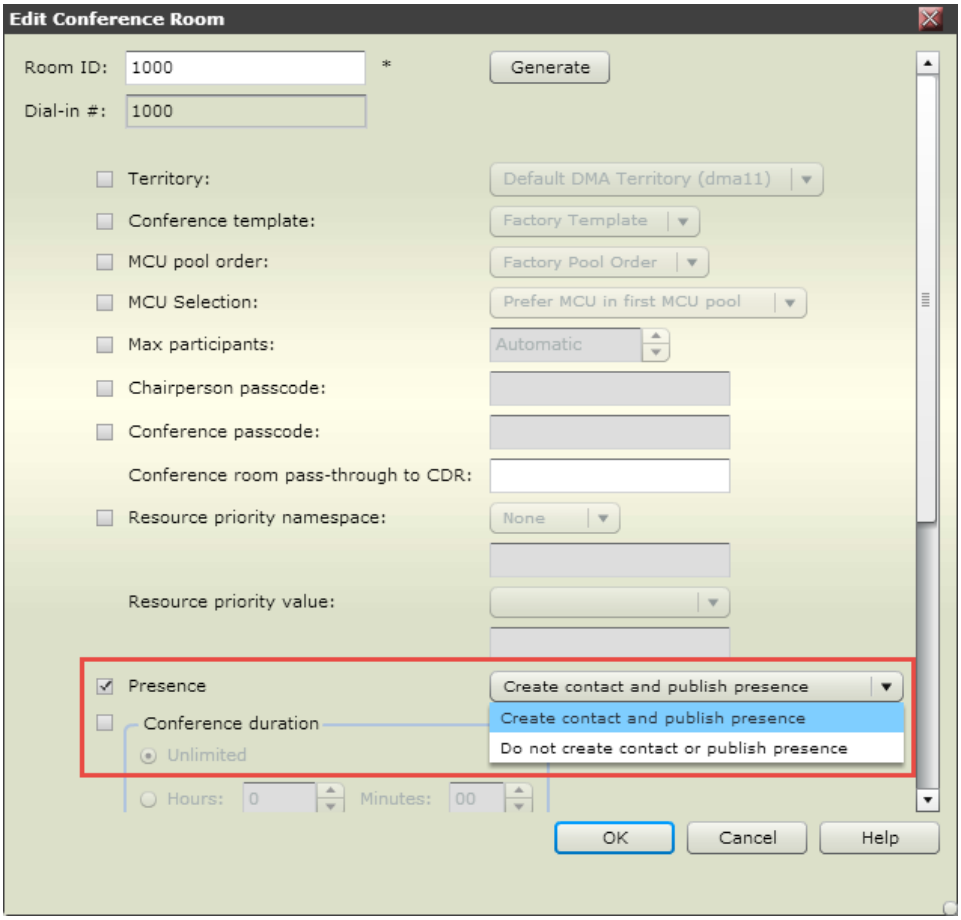


Managing Presence for Virtual Meeting Rooms

After configuring presence publishing, you can manage presence publishing for a locally defined room.

To manage Presence publishing for a locally defined room:

1. Go to **Access User > Users > Manage Conf Rooms**. Here you can 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**.



3. Click **OK**.

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 environment. To configure RealPresence DMA system to work with Skype for Business, refer to the section Deploying Polycom RealPresence DMA Systems.

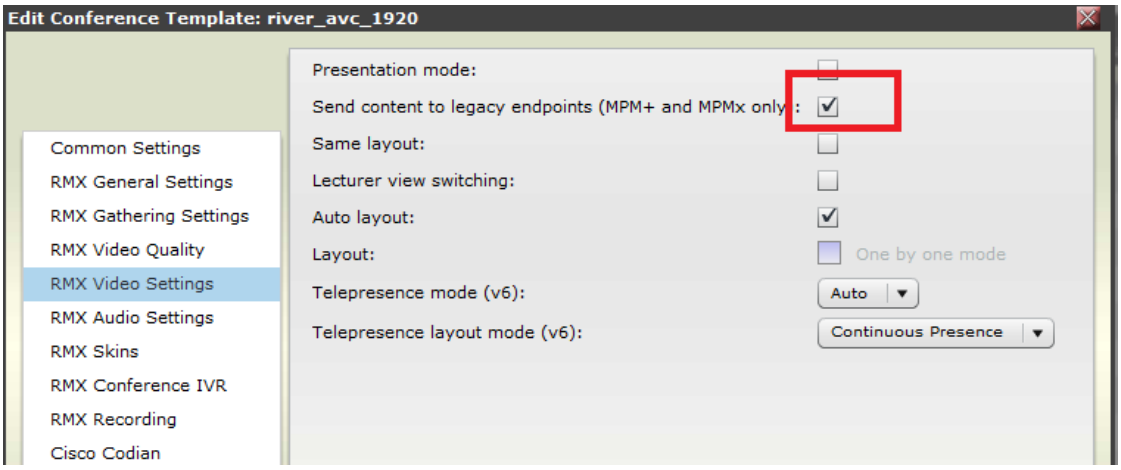
For your RealPresence DMA system setup, consider the following:

- 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.

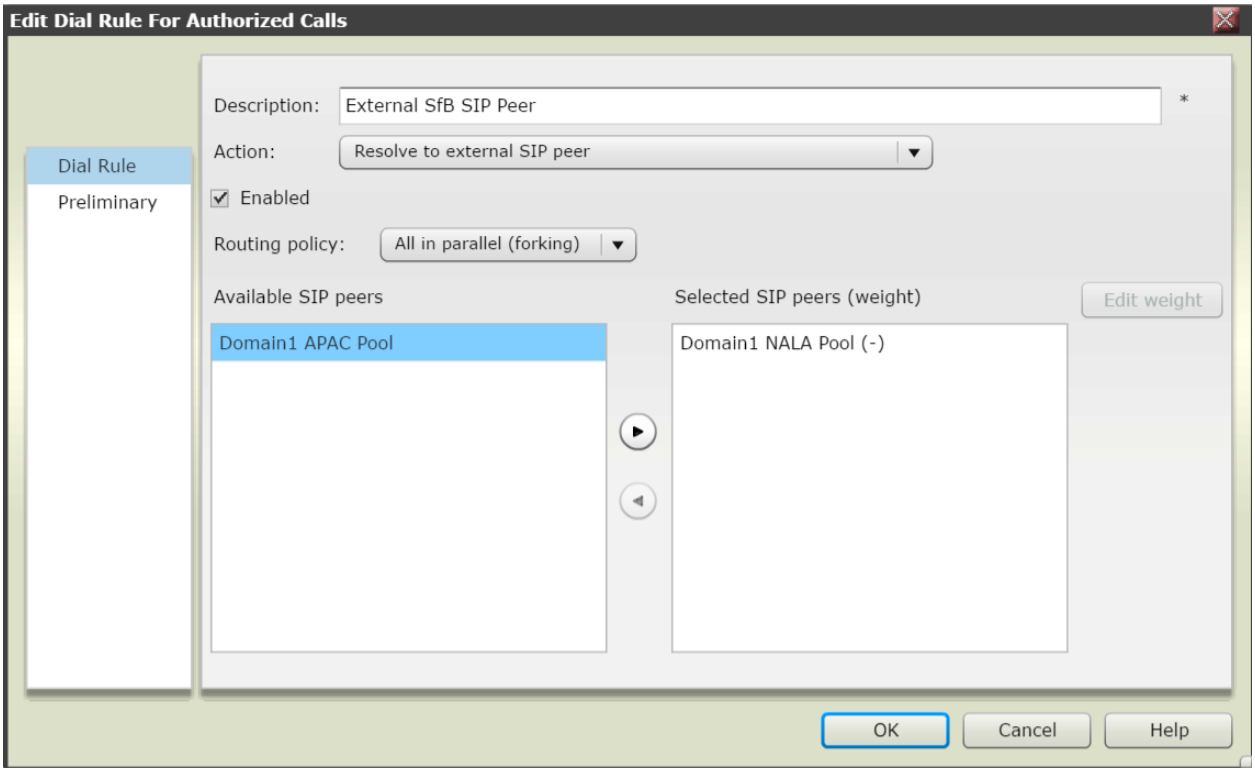
To configure RealPresence DMA system for Polycom ContentConnect software:

1. Ensure that the postliminary is not enabled.
2. For the conference template you created in Configure the RealPresence DMA System Skype for Business Conference Template, 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 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 Skype for Business SIP peer
   - **Action** Resolve to external SIP peer
   - **Preliminary Enabled** No
   - **Enabled** Enabled
   - Select one of the external SIP peers you created in the section Add a Skype for Business Server as an External SIP Peer.
4. If your Skype for Business deployment has multiple pools or multiple domains, add a dial rule for each external SIP peer that corresponds to a pool and domain.



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

Dial rules for authorized calls:

Order	Description	Action	Preliminary Enabled	Enabled
#1	Dial by conference room	Resolve to conference room	No	Enabled
#2	Dial registered endpoints by alias	Resolve to registered endpoint	No	Enabled
#3	Dial by virtual entry queue ID	Resolve to virtual entry queue	No	Enabled
#4	Dial to on-premises RealConnect™ confe	Resolve to conference ID by Skype quer	No	Enabled
#5	Dial services by prefix	Resolve to service prefix	No	Enabled
#6	Dial external networks by H.323 URL, E	Resolve to external address	No	Enabled
#7	Dial endpoints by IP address	Resolve to IP address	No	Enabled
#8	Dial to RealConnect conference by exter	Resolve to Skype Conference ID by Con	No	Disabled
#9	External SfB SIP Peer	Resolve to external SIP peer	No	Enabled

Deploying Polycom RealPresence Media Suite

When you incorporate Polycom RealPresence Media Suite Software in a Microsoft environment, you can connect to a Skype for Business or Lync meeting directly to record video, audio, and content. RealPresence Media Suite can also integrate with RealPresence DMA systems to record Polycom RealConnect meetings.

To deploy a RealPresence Media Suite in a Microsoft environment, you need to configure settings on the Skype for Business or Lync Server and RealPresence Media Suite.

Configuring Skype for Business Server for Use with a RealPresence Media Suite

Complete the following tasks to configure Skype for Business Server with a RealPresence Media Suite system:

1. Configuring a RealPresence Media Suite FQDN on the DNS Server
2. Configure the Microsoft PowerShell to Create the Trusted Application
3. Configure Microsoft PowerShell to Update the Topology
4. Define a Static Route for the RealPresence Media Suite Using Microsoft PowerShell

Configuring a RealPresence Media Suite FQDN on the DNS Server

To register with Skype for Business, the RealPresence Media Suite SIP signaling domain must be accessible by the DNS server used by the Skype for Business Server. You need to configure a DNS A record for the FQDN of the RealPresence Media Suite SIP signaling domain.

The RealPresence Media Suite and the Skype for Business Server must both resolve the RealPresence Media Suite host record identically, regardless of the domain you select to store the DNS Host record.

Configure the Microsoft PowerShell to Create the Trusted Application

Create the trusted application using the Microsoft PowerShell.

To create the trusted application:

1. Navigate to **Start > All Programs > Skype for Business 2015 > Skype for Business Server Management Shell** to open the **PowerShell** terminal.
2. Use the `New-CsTrustedApplication` command to set up a trusted application for the RealPresence Media Suite.

```
New-CsTrustedApplication -ApplicationId ms20696
-TrustedApplicationPoolFqdn ms20696.sfb2015.com -Port 5061
```

The parameters are defined as follows:

- **ApplicationId**—A descriptive name for the application. Must be unique within your Skype for Business deployment.
- **trustedApplicationPoolFQDN**—The FQDN of the application pool, in this example, *ms20696.sfb2015.com*.
- **port**—The SIP port. The default SIP port number is 5061.

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

3 Use the `New-CsTrustedApplicationPool` command to create a new pool that will contain the computers that host trusted applications.

```
New-CsTrustedApplicationPool -Identity ms20696.sfb2015.com -Registrar
Registrar:lync2015.sfb2015.com -site 1 -ComputerFqdn
ms20696.sfb2015.com
-ThrottleAsServer $true -TreatAsAuthenticated $true
```

The parameters are defined as follows:

- **Identity**—The FQDN of the new pool.
- **Registrar**—The service ID or FQDN of the Registrar service for the pool.
- **Site**—The Site ID of the site on which this pool is homed.
- **ComputerFqdn**—Creating a trusted application pool will automatically create a trusted application computer that is part of that pool. By default, the computer will receive the same FQDN as the pool.
- **ThrottleAsServer**—Set this parameter to false to throttle connections between the servers within the pool and trusted applications as clients.
- **TreatAsAuthenticated**—Determines whether authentication is required for trusted applications connecting to servers within the pool.

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

Configure Microsoft PowerShell to Update the Topology

You must use Microsoft PowerShell to update the topology.

To update the topology:

1 Navigate to **Start > All Programs > Skype for Business 2015 > Skype for Business Server Management Shell** to open the Skype for Business PowerShell terminal.

2 Use the `Enable-CsTopology` command to update the Skype for Business topology.

Define a Static Route for the RealPresence Media Suite Using Microsoft PowerShell

You need to define a static route for your RealPresence Media Suite solution using PowerShell. Route changes you make take effect immediately.

To define a static route:

1. Navigate to **Start > All Programs > Skype for Business 2015 > Skype for Business Server Management Shell** to open the Skype for Business PowerShell terminal.
2. Use the `New-CsStaticRoute` command to set up a static route for the RealPresence Media Suite.

   ```
   $route = New-CsStaticRoute -TLSRoute -destination "ms20696.sfb2015.com"
   -port 5061 -matchuri "ms20696.sfb2015.com" -usedefaultcert $true
   ```

   where `ms20696.sfb2015.com` is the FQDN of the RealPresence Media Suite server SIP signaling domain and ms20696.sfb2015.com is the name of the Trusted Application Pool you created.

   For more information about the `New-CsStaticRoute` command see Microsoft New-CsStaticRoute.
3. Set the routing configuration. By configuring the static route, matched URI dialing is enabled. The following example sets the route to be global:

   ```
   Set-CsStaticRoutingConfiguration -identity global -route @{Add=$route}
   ```
4. 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 Media Suite solution is now set as a trusted host, and calls from a Skype for Business client to a SIP address in the RealPresence Media Suite's domain will be routed through that system.

Configuring Your RealPresence Media Suite for Skype for Business

This section outlines the following four steps that configure a RealPresence Media Suite with Skype for Business Server:

1. Ensuring DNS is Configured Properly
2. Create a Security Certificate for the RealPresence Media Suite
3. Configure Signaling Type
4. Configure a Virtual Recording Room for Skype for Business Calls

Ensuring DNS is Configured Properly

To configure DNS properly, ensure that:

- You have all FQDNs of the system you are creating a certificate for.
- All of the FQDNs are in the primary DNS server of the environment and resolve correctly to the RealPresence Media Suite.

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

Create a Security Certificate for the RealPresence Media Suite

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

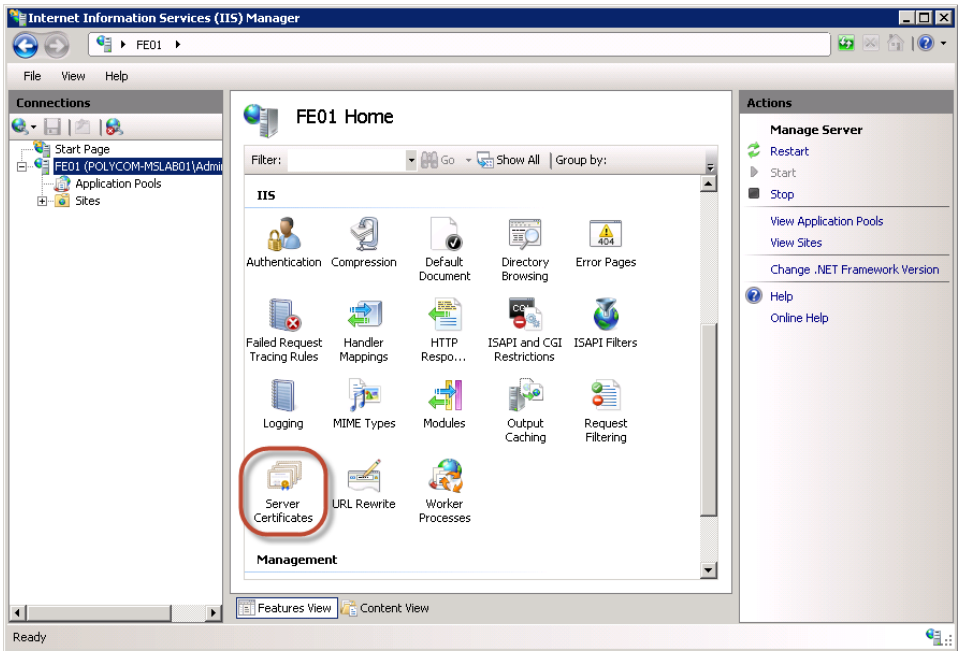
- You can purchase and install a certificate from a commercial Trusted Root CA such as VeriSign or Thawte. Use the procedures in the RealPresence Media Suite documentation for Certificate Management to create a Certificate Signing Request and to install the certificate(s) you receive from the CA.
- Request 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 Media Suite Administrator Guide 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 Skype for Business 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 Media Suite. 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 Media Suite Administrator Guide* for your model at RealPresence Media Suite on Polycom Support.

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.

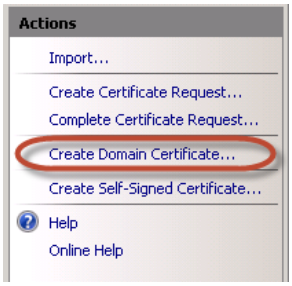
To create a security certificate for the RealPresence Media Suite system using IIS Manager 7:

1. On the Skype for Business 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 Media Suite name. This name must match what is in the DNS.

6 Click **Next**.

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

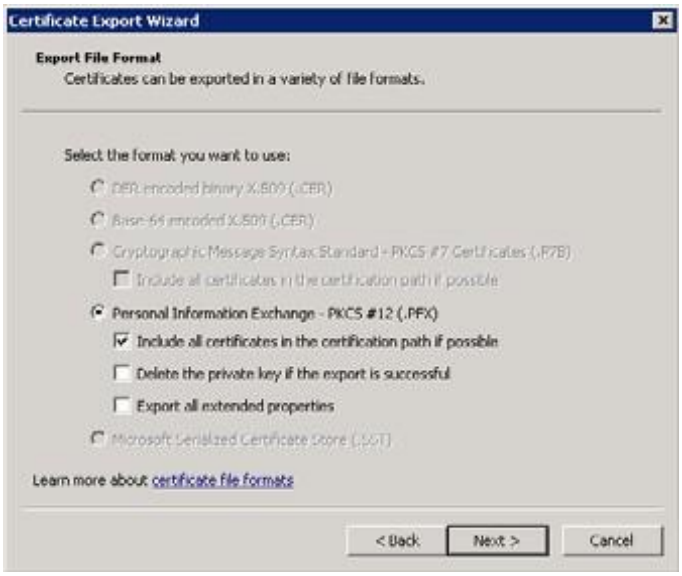
8 Click **Finish**.

Export Security Certificate

After creating a security certificate for RealPresence Media Suite, export the certificate using the Microsoft Management Console.

To use the Microsoft Management Console to export the certificate:

1. Open **Microsoft Management Console**.
2. 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**.
3. Click **OK**.
4. Browse to **Certificates (Local Computer) > Personal > Certificates**.
5. Right-click the created certificate and select **All Tasks > Export** to view the Certificate Export wizard.
6. 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**.
7. In the **File to Export** panel, enter a path where you want to save the new file, for example, `c:\temp\ MediaSuitecert.pfx`.

8 Once the `.pfx` file is on your computer, you can upload it to the RealPresence Media Suite system and install it, using the procedures in the RealPresence Media Suite system's online help for Certificate Management.

Configure Signaling Type

The next step in configuring a RealPresence Media Suite with Skype for Business Server is to configure signaling type for communicating with Skype for Business Server.

To configure the signaling type:

1 Log in to the RealPresence Media Suite Admin Portal.

2 Go to **Configuration > Signaling Settings > SIP**.

3 Select **SIP** tab.

4 Select **Microsoft Skype for Business** as **SIP Server Type**, and configure the Skype for Business server address, port, and domain name.

Configure a Virtual Recording Room for Skype for Business Calls

The next step in configuring a RealPresence Media Suite with Skype for Business is to configure a virtual recording room (VRR).

To configure the VRR for Skype for Business call:

1 Log in the RealPresence Media Suite Admin Portal.

2 Go to **Template > VRRs > Add**.

3 Configure the VRR settings, as shown in the following table.

Parameter	*Description*
VRR Name	Specify a unique name to identify the VRR. You can also use the default name generated by the system.
VRR Number	Specify a number to identify the VRR. You can directly dial the VRR to record by adding the VRR number when dialing the RealPresence Media Suite system. The number you enter must be unique and comprised of 4-8 digits. You can also use the number automatically generated by the system. Note: The initial digit of the VRR number cannot be zero.
Enable Register to Skype for Business	Specify whether register VRR to Skype for Business.
Skype for Business Register Name	Specify a Skype for Business or Lync user combined with the VRR.
Description	If necessary, you can enter additional VRR information, such as the owner and usage, in order to improve identification and classification management when there are many VRRs.

Parameter	*Description*
Recording Template	Specify the recording template. The template defines the basic recording link parameters.
Transcoding Template	After recording is done, the system will do offline transcoding according to the transcoding templates configured here. Multiple offline transcoding outputs are allowed. Only qualified transcoding templates will apply. If the template parameters are higher than the recorded raw parameters, then the template will be ignored. For example, if recording raw resolution (e.g. 4CIF) is less than the transcoding template (e.g. 720p), then this transcoding template will be ignored. Note: If the recording template disable the live streaming, the transcoding template is required for playing back video correctly.
Sites	Select sites for VRR. After the sites are selected, the live stream using the VRR will be pushed to these sites.
Live Streaming Server	You can check configured live streaming server information, including the publish point template, stream alias, and streaming lists.
Email Address (separated by ‘,’)	Once the live streaming is started or the VRR recorded video has completed its format conversion and is ready for viewing, the system sends an email message to the address set here.

4. Click **OK**. When a user dials out from Skype for Business to RealPresence Media Suite, the user can choose different recording templates by inviting different registered users to the Skype for Business meeting after configuring the VRR and integrating the Skype for Business user with the VRR.

For more about configuring RealPresence Media Suite to integrate with Skype for Business environment, refer to *Polycom RealPresence Media Suite Administrator Guide* at RealPresence Media Suite on Polycom Support.

Configure Your RealPresence Media Suite for Polycom RealConnect

To deploy a RealPresence Media Suite Software with Polycom RealConnect technology, register the RealPresence Media Suite Software to RealPresence DMA system.

To register the RealPresence Media Suite to RealPresence DMA system:

1. In the RealPresence Media Suite Admin Portal web page, go to **Configuration > Signaling Settings**.
2. Select one of the following signaling types from **Call Preference** on User Portal down-drop list.

- Select **H.323 only** to prevent users from setting SIP as the signaling type by mistake from the User Portal.
- Select **SIP and H.323** to enable users to specify a signaling type when they start a recording or live event from the User Portal.
- Select **SIP only** to disable peer-to-peer (P2P) recording.

3 Depending on the signaling type you selected, do one of the following:

- For H.323, enter the DMA address in the **Gatekeeper Address** field.
- For SIP, select **Generic** in **SIP Server Type**, and enter the DMA address in the **Server Address** field and the port in the **Server Port** field.

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

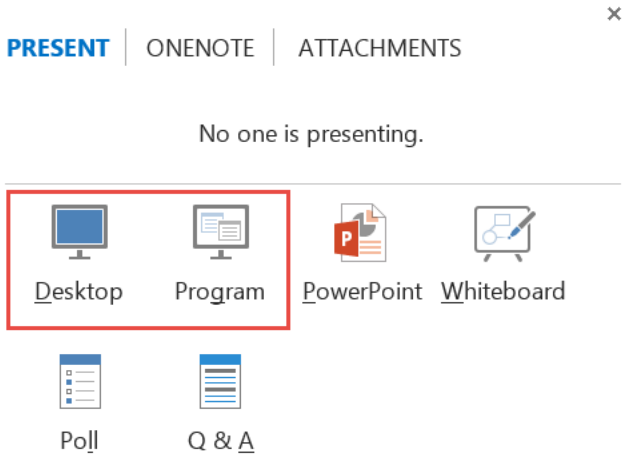
Deploying Polycom ContentConnect Software

This section explains how to configure Polycom ContentConnect software solution components with Skype for Business. 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 ContentConnect on Polycom Support.

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

Gateway Mode facilitates content sharing only between standards-based video room systems and Skype for Business 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 Skype for Business 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 Skype for Business clients, only a Microsoft Edge server is required.

Required Polycom ContentConnect software components for Skype for Business

Component
Management Systems and Recorders
Microsoft Active Directory Server
Gatekeepers, Gateways, and MCUs
Skype for Business
Microsoft Lync Server 2013
Polycom RealPresence Distributed Media Application (DMA) 7000
Polycom RealPresence Collaboration Server (RMX) Software MCU/1500/1800/2000/4000 (8.5 or higher)
Microsoft Endpoints
Gateway Mode Skype for Business client installed on Windows, Mac, mobile platforms (iOS, Android, Windows), and Skype for Business 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 *Install the RealPresence Content Sharing Server Components* in the *Polycom RealPresence Content Sharing Suite Administrator Guide* on ContentConnect.

Optional Components

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

Optional Polycom ContentConnect software components for Skype for Business

Component
Firewall, Border Controllers
Microsoft Edge Server
Polycom RealPresence Access Director
Acme Packet® Net-Net Enterprise Session Director (ESD)
Recorders
Polycom RealPresence Media Suite

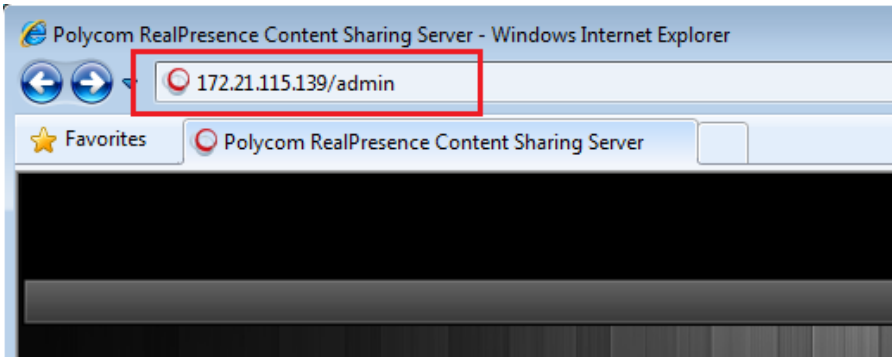
Component
Load Balancers Polycom has tested the following load balancer: F5 BIG-IP LTM 1600 and BIG-IP 10.2.1.297.0

Access 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.



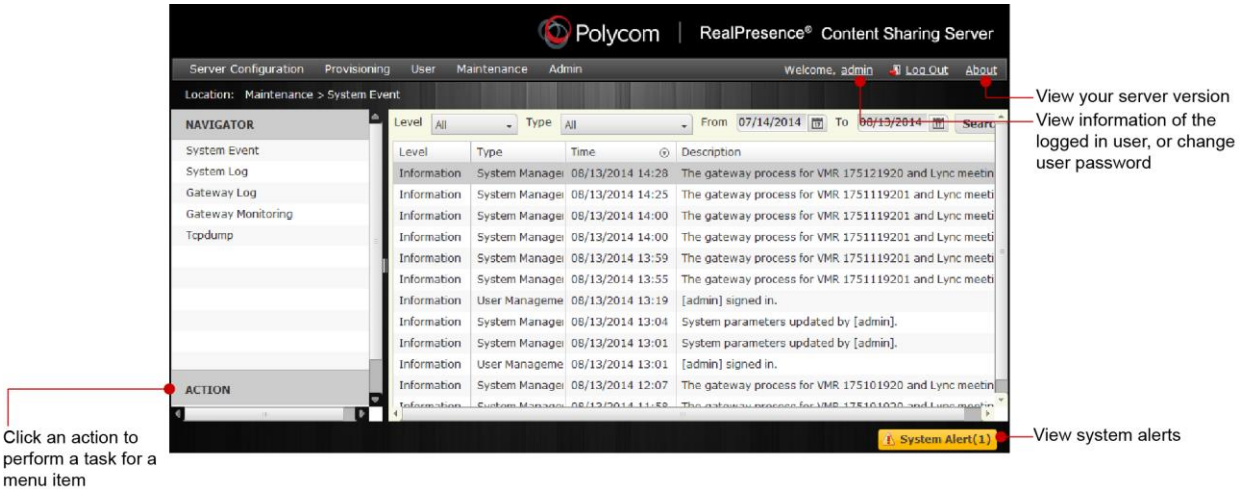
2. Press **Enter**.

   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. For information on default user names and passwords, see the *Polycom RealPresence Content Sharing Suite Administrator Guide* at ContentConnect 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.

Configuring 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 ContentConnect on Polycom Support.

Configure Polycom ContentConnect Software Server Running Mode

Polycom ContentConnect software server works in two modes: Gateway and Add-On. This guide provides steps required to configure Gateway Mode and does not address Add-on Mode.

- Gateway Mode
  - Skype for Business clients don't need to install the Polycom RealPresence Content Add-on for Skype for Business 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.
  - Only H.264 content is supported on legacy endpoints in the Gateway mode.
- Add-On Mode
  - All Skype for Business clients must install the Polycom RealPresence Content Add-on for Skype for Business 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.

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 Skype for Business Service** installed already, it will be disabled.
6. Click **Save**.

Configure Server Information

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

To configure server information settings:

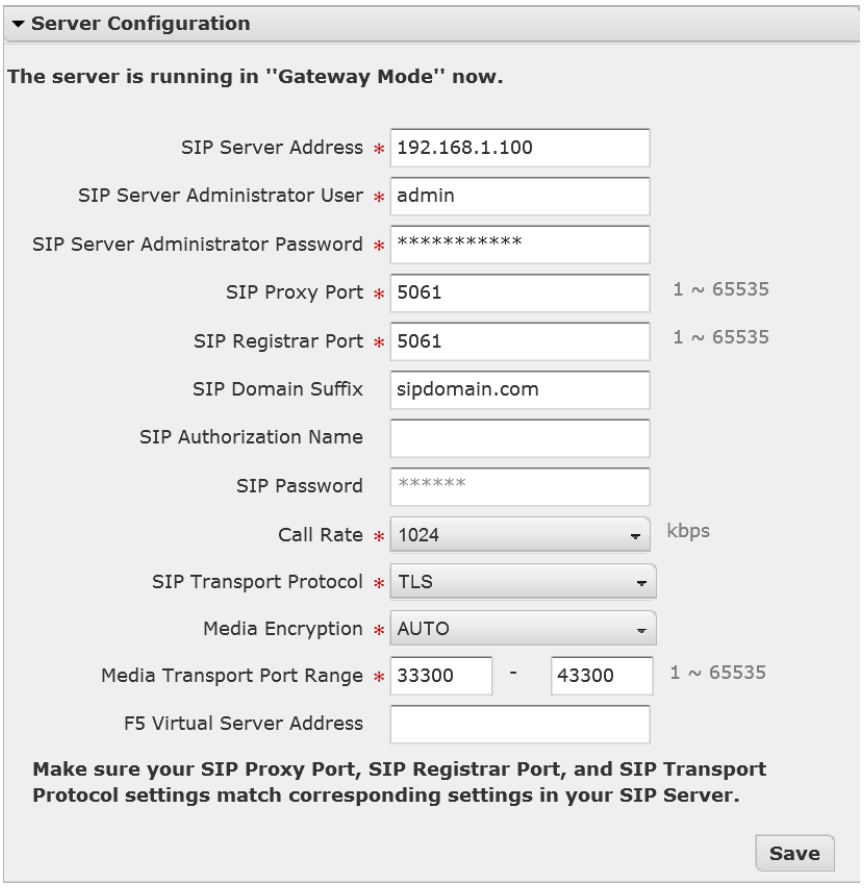
1. Log in to the Content Sharing Server Web Configuration Tool.
2. Select **Server Configuration > Server**.
3. Enter the following information:
   - **SIP Server Address** The IP address or host name of the RealPresence DMA system.
   - **SIP Server Administrator User** The user name of a RealPresence 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 Skype for Business 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



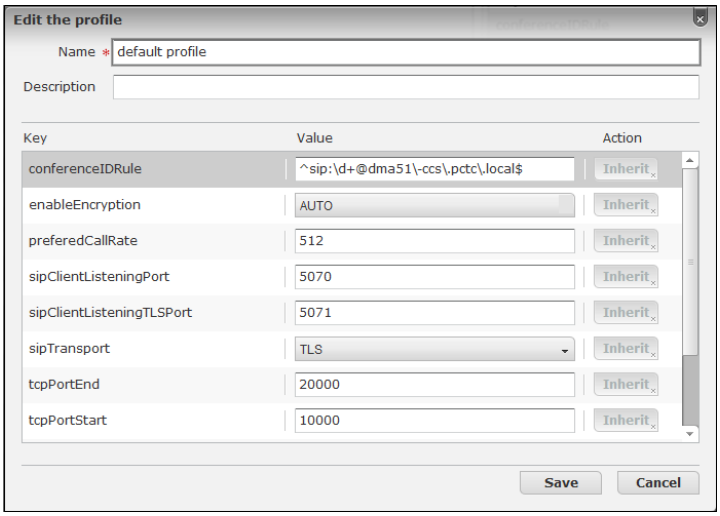
(Optional) Configure the Polycom ContentConnect Software Provisioning Profile

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 the Polycom ContentConnect provisioning profile:

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.



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 Skype for Business-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 Skype for Business client. For example, for 123456@dma51-ccs.pctc.local, the route dma51-ccs.pctc.local has been created in Skype for Business.

     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 Skype for Business 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

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

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

Appendix B: Exchange Calendar Polling Information

This appendix provides information on 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: Skype for Business Client and Server Support

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

Note: On RealPresence DMA systems do not support dialing from Skype for Business clients to virtual entry queues (VEQs).

Skype for Business client and Server Support for Features

Feature	*Client*	*Server*	*Comments*
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 – Skype for Business 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 Skype for Business 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

Mode	*Product*	*Resources Used and Licenses Required*
Polycom RealConnect technology (Polycom ContentConnect software Gateway Mode)	RealPresence DMA system	• No concurrent call license for the SVC cascaded connections with Skype for Business 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	• 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)	• One Polycom ContentConnect software license per conference • One Polycom ContentConnect software license web client
Polycom ContentConnect software (Add-on mode)	RealPresence DMA system	• One concurrent license per Skype for Business client • One concurrent call license per Polycom ContentConnect software Skype for Business add-on
	RealPresence Collaboration Server (RMX) solution	• Each Skype for Business client consumes video resources depending on the video resolution • One audio port for content for each Polycom ContentConnect software Skype for Business Add-on or web client
	Polycom ContentConnect software	• One Polycom ContentConnect software license per Skype for Business (with add-on) on VMR • One Polycom ContentConnect software license per Polycom ContentConnect software web client

Appendix E: Configuring Static Routes in Skype for Business

In Skype for Business Server 2015 and Lync Server 2013, 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.

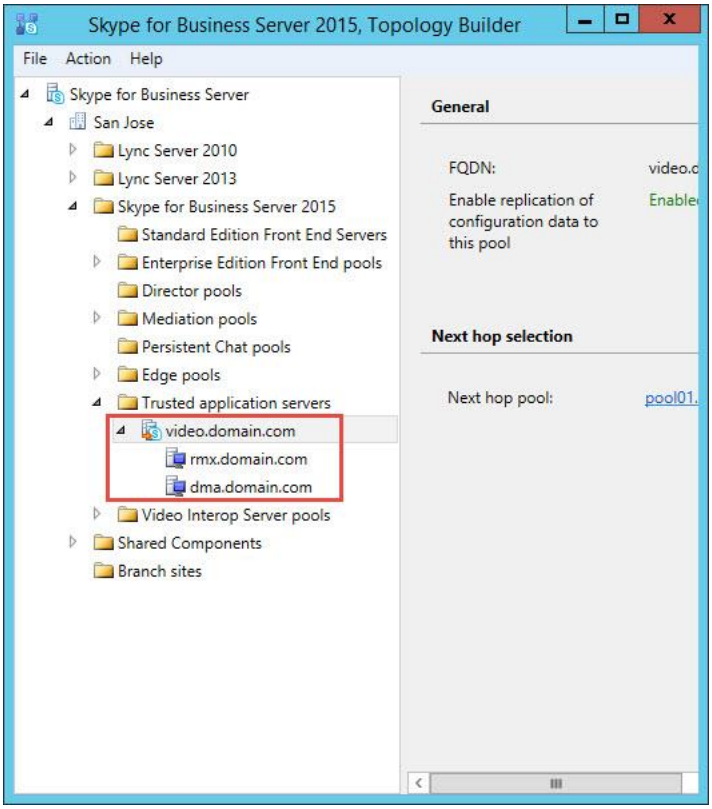
You do not require static routes or VMRs to deploy Polycom RealConnect technology as the Polycom DMA system automatically creates VMRs with the same number as the Skype for Business conference ID.

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.



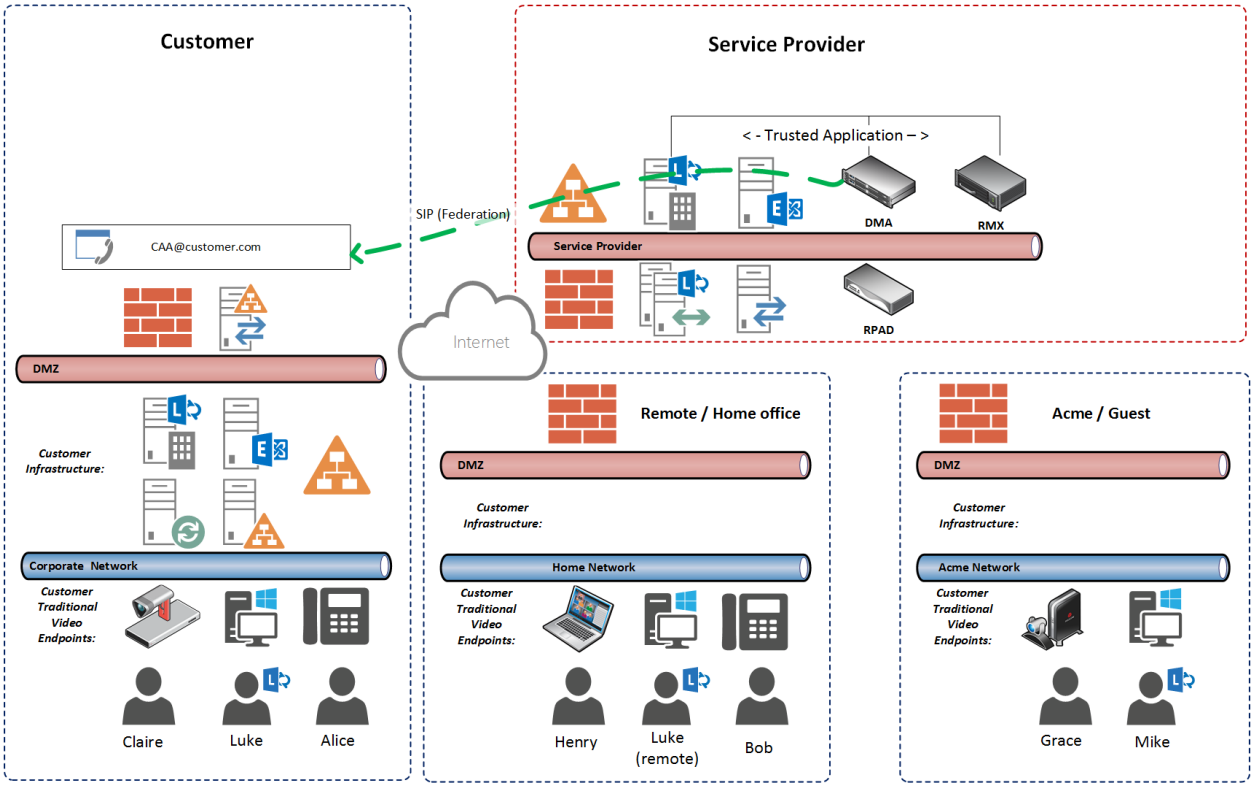
TLS Security

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.

Appendix F: Polycom RealConnect for Service Providers

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

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

RealPresence System and Skype for Business for Polycom RealConnect

Polycom RealPresence Collaboration Server (RMX) solution, RealPresence DMA, and Polycom ContentConnect systems introduce Polycom RealConnect technology for Skype for Business, a new RealPresence platform function for Skype for Business customers. Polycom RealConnect technology enables you to dial into scheduled Skype for Business 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 Skype for Business.

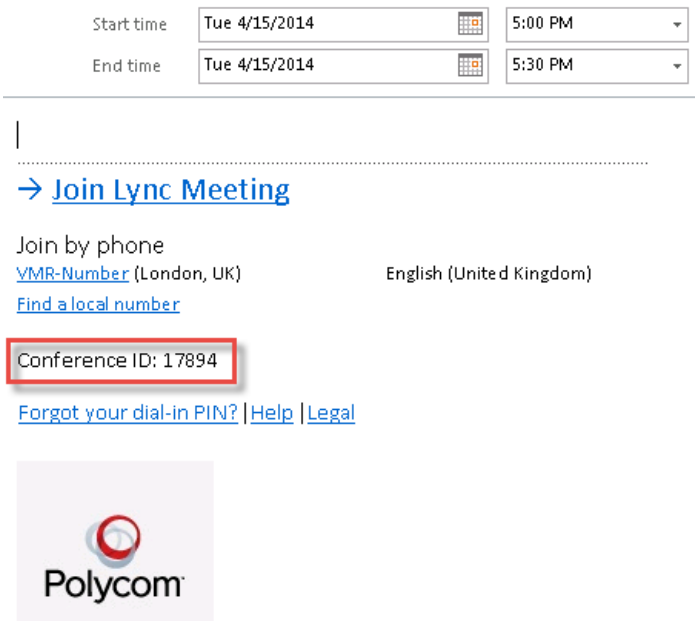
Conference IDs are generated only when you deploy Skype for Business Dial-in Conferencing and are enabled when PSTN dial-in conferencing capabilities are also enabled. However, you can use a dummy dial-in access number. For full Skype for Business dial-in conference deployment steps, refer to Microsoft's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

The figure Skype for Business Invitation with Conference ID shows a Skype for Business invitation populated with a Conference ID, which is provided automatically by the customer's respective Skype for Business 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*

Skype for Business invitation with conference ID

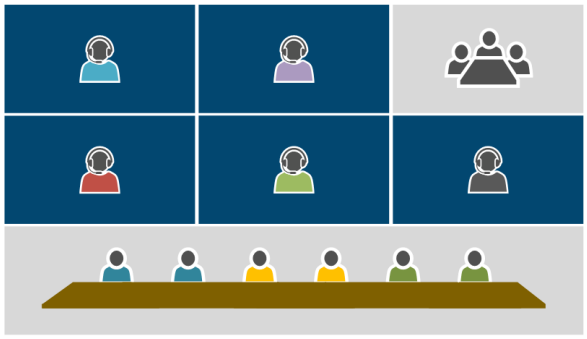


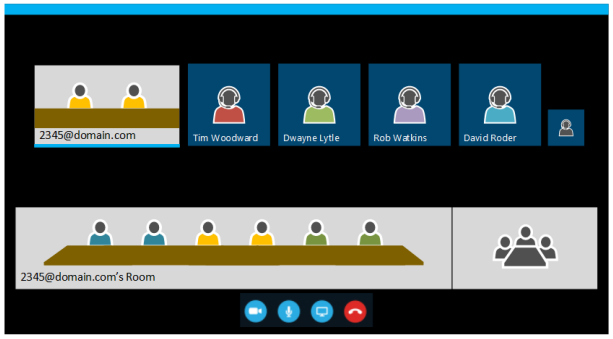
Enable the Panoramic Layout for Skype for Business Calls

When using RealPresence Collaboration Server version 8.7.1 or later, the Skype for Business client panoramic strip can display a video strip containing all participants in an immersive telepresence room, a Polycom® RealPresence Centro™, or an additional four standards-based endpoints during video conferences with the active speaker displaying in Gallery View.

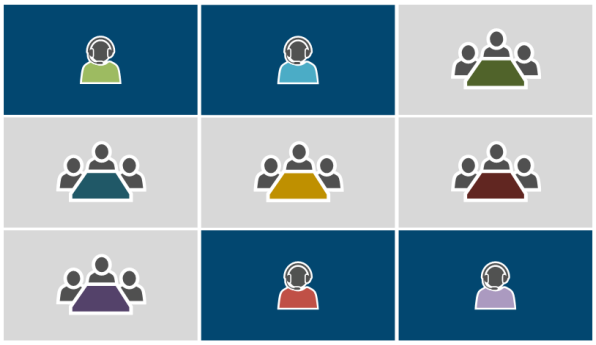
The following figures illustrate the standard and immersive scenarios. The left-side figures illustrate the viewpoint from a standards-based endpoint; the right-side figures illustrate the viewpoint from the Skype for Business client.

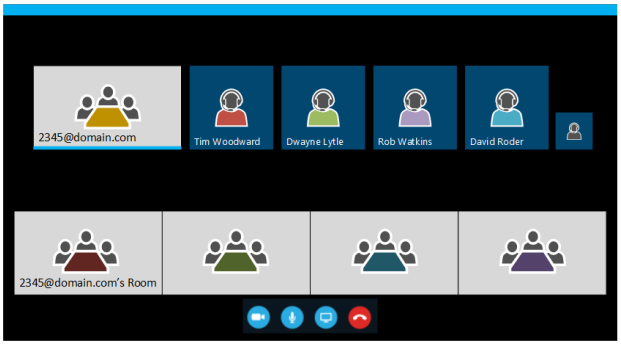
Immersive Video Teleconferencing – Panoramic Layout with Polycom RealConnect





Standard Video Teleconferencing – Panoramic Layout with Polycom RealConnect





The following procedure shows you how to enable the panoramic layout.

Note: To use panoramic layout with Microsoft environment conferences, you must have version 8.7.1 or later of the Polycom® RealPresence® Collaboration Server.

To enable the panoramic layout:

1. In the conference template you created in Configure a Conference Template for Polycom RealConnect, select **Polycom MCU General Settings > Advanced Settings**.
2. Click to select the checkbox for **Enable MS panoramic layout**.

This Appendix includes the following sections:

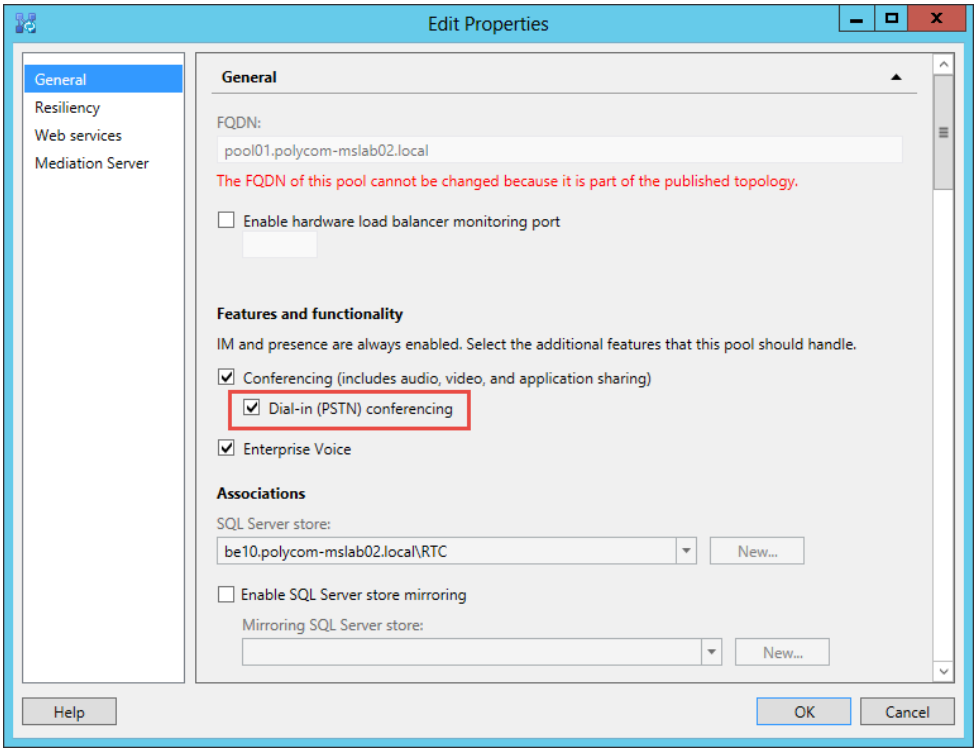
Deploy Skype for Business Dial-in Conferencing

This section is for customers enabling Dial-in Conferencing on Skype for Business. If you require more details, refer to Microsoft TechNet.

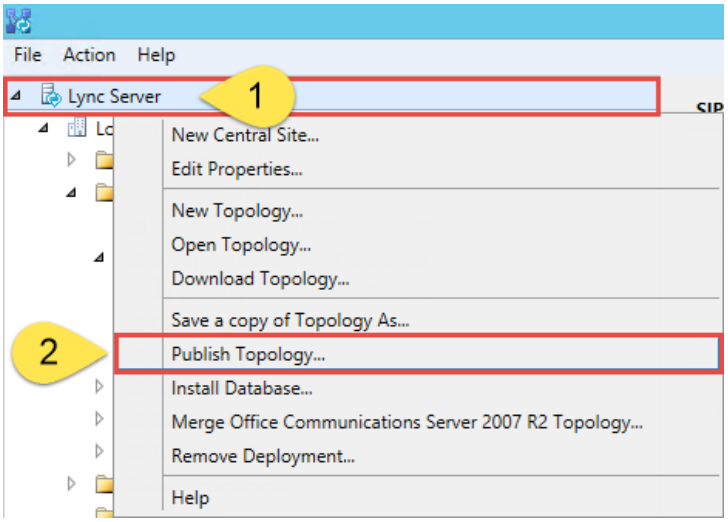
The customer must first enable dial-in conferencing.

To enable Dial-in Conferencing:

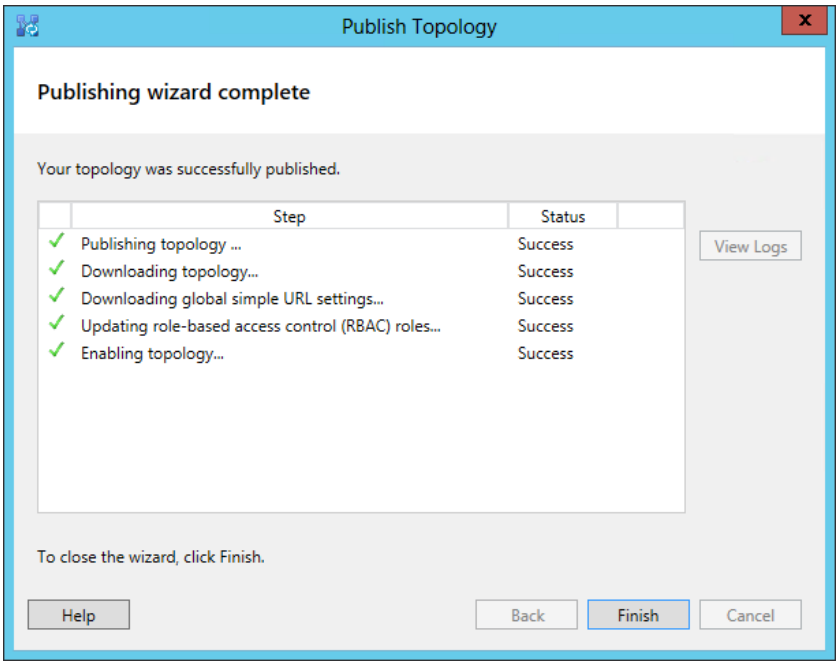
1. In the Skype for Business topology builder, install the dial-in (PSTN) conferencing component for the Skype for Business front end server or pool by going to **Edit Properties > General > Features and Functionality**.
2. Select **Dial-in (PSTN) conferencing** and click **OK**.



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 Skype for Business Server by running the Skype for Business bootstrapper process.

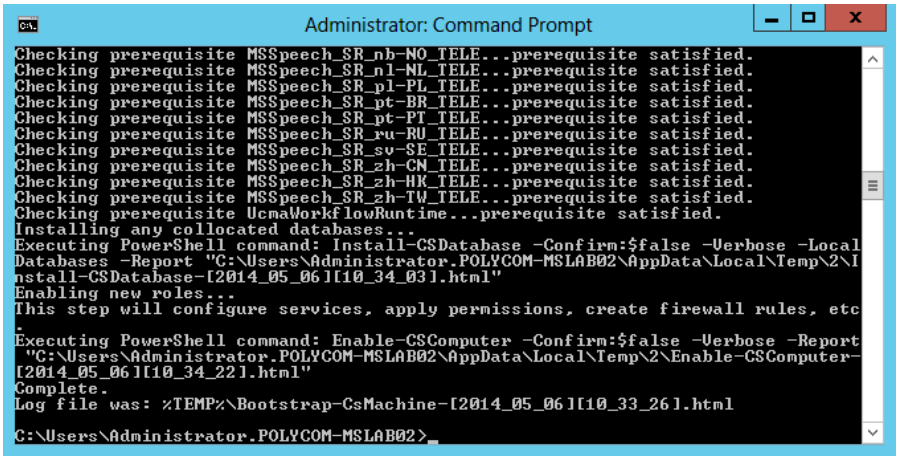
Deploy the Dial-In Application

After you enable dial-in conferencing, deploy the application.

To deploy the application:

1. On your Skype for Business front end server, open the command prompt and execute the command:

```
%Program Files%\Skype for Business Server 2015\Deployment\Bootstrapper.exe
```



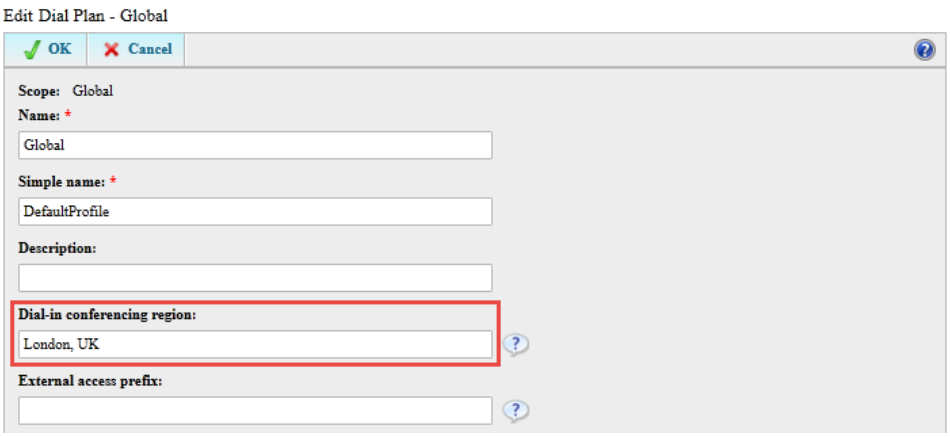
2. Install the associated service by opening the Skype for Business Server Management Shell and executing `Start-CSWindowsService`.

Configure a Dial-in Conferencing Region

After deploying the application, 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.

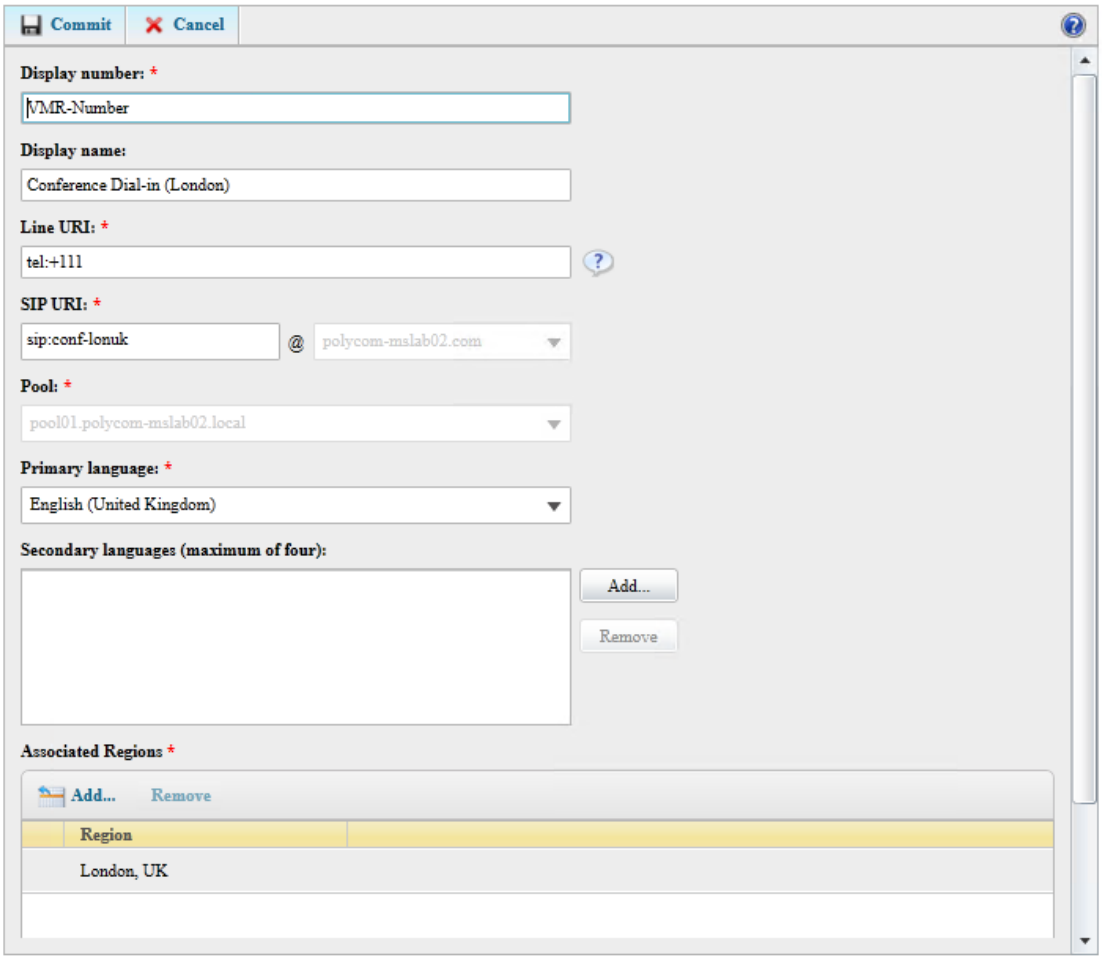
To configure the dial-in conferencing region:

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



2 Specify a dial-in access number by going to **Skype for Business Server Control Panel > Conferencing > Dial-in Access Number > New** and completing the following fields:

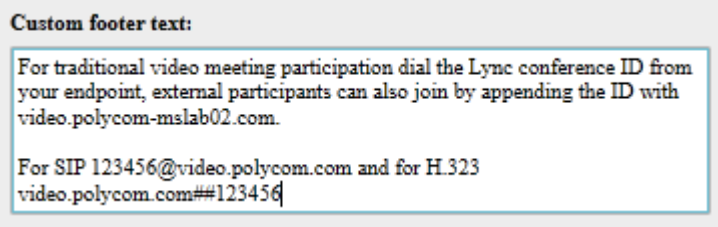
- **Display number** This field permits alphanumeric entry. This is typically the dial-in access number. This example uses the VMR or Conference ID and is labelled here as VMR-Number.
- **Display name** Choose a display name. Typically, this name matches the region.
- **Line URI** The line URI will not 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 Skype for Business 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.



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 Skype for Business Control Panel, go to **Conferencing > Meeting Configuration**.

4 Edit the default global template as shown next.



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 Skype for Business environment now includes Conference IDs in Skype for Business-enabled meeting invitations.

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 Certificate 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.

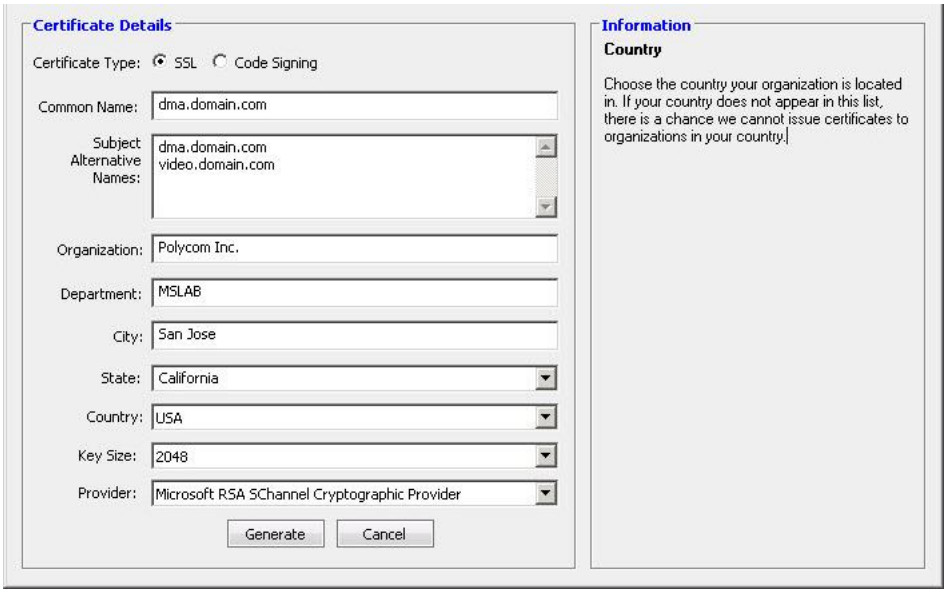
2 In **Certificate Details**:

a Set **Certificate Type** to SSL.

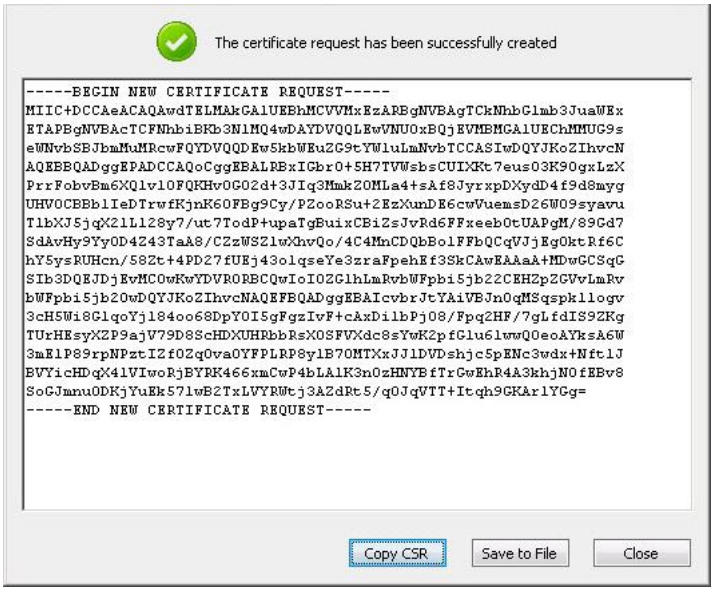
b Enter your common name domain in **Common Name**.

c In **Subject Alternative Names**, duplicate the common name domain and add the MatchURI.

d Click **Generate**.

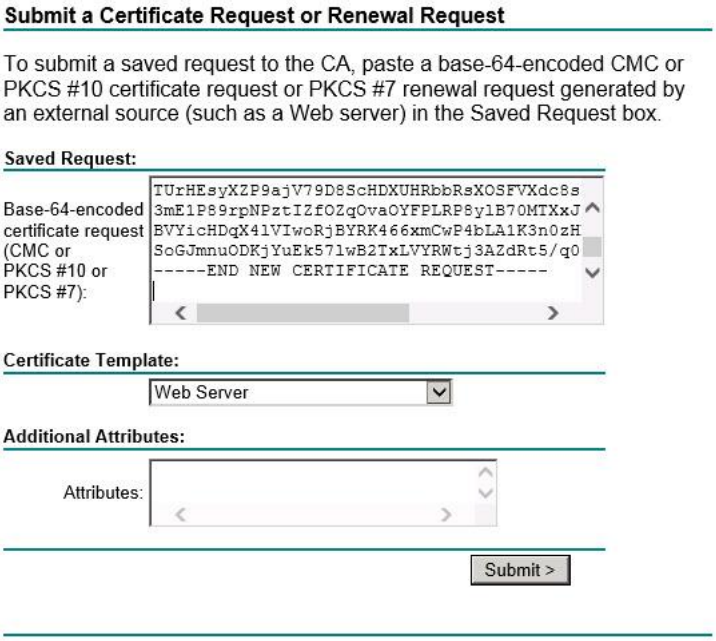


3 Click **Save to File** after the certificate request is generated.



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.**

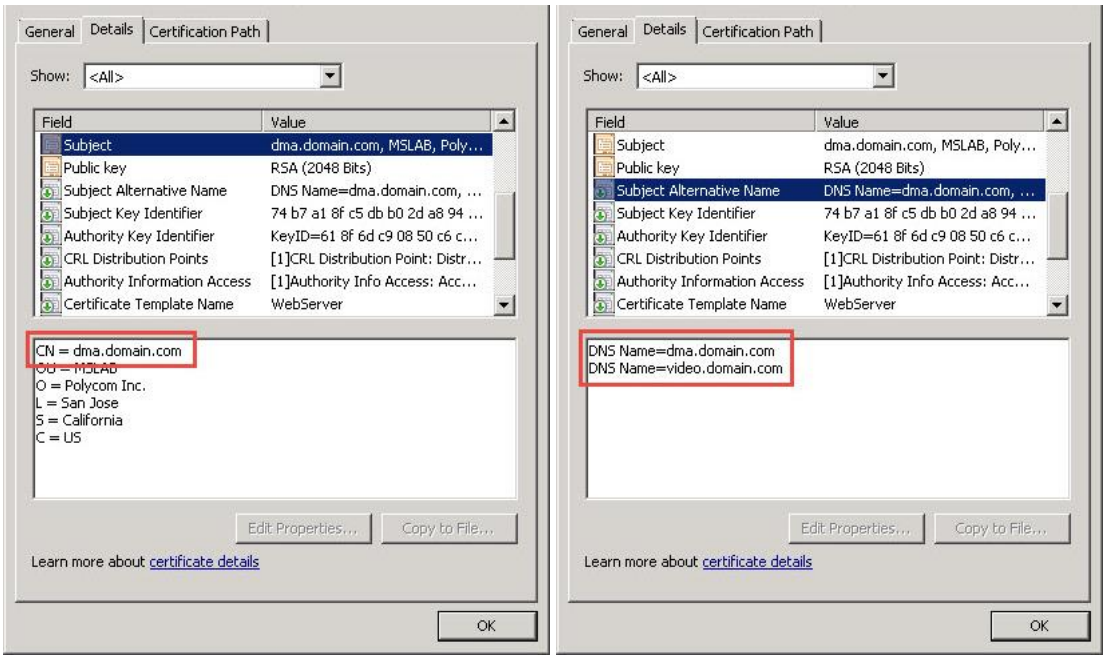


6 Download the certificate.

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

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.

Deploying Polycom RealPresence Collaboration Server (RMX) Solution for Skype for Business

This section outlines the steps service providers must complete to integrate Polycom RealPresence Collaboration Server (RMX) solution with Skype for Business Server. You must add a DNS entry, and create and install a security certificate. You also need to add a static route on the Skype for Business Server for the RealPresence Collaboration Server (RMX) solution to use, and enable Skype for Business 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 Skype for Business Server Edge Server.

Note that Microsoft Presence is available only with Skype for Business and Lync Server 2013.

To set up the RealPresence Collaboration Server (RMX) solution for use in a Skype for Business Server environment, you must configure RealPresence Collaboration Server (RMX) solution for SIP, create security certificates, and ensure encryption settings.

Complete the following steps:

1. Setting Up the RealPresence Collaboration Server (RMX) System for Security and SIP
2. Creating and Installing a Security Certificate for the Polycom RealPresence Collaboration Server (RMX) System
3. Configure Encryption
4. Configuring Skype for Business Server for use with a Polycom RealPresence Collaboration Server (RMX) System

Setting 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:

1. Configure the RealPresence Collaboration Server (RMX) IP Network Service
2. Create the RealPresence Collaboration Server (RMX) FQDN (SIP signaling IP address) in DNS

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 Skype for Business 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 Skype for Business Front End server or Pool name and the server domain name.
10. If not selected by default, change the **Transport Type** to **TLS**.

Create the RealPresence Collaboration Server (RMX) FQDN (SIP Signaling IP address) in DNS

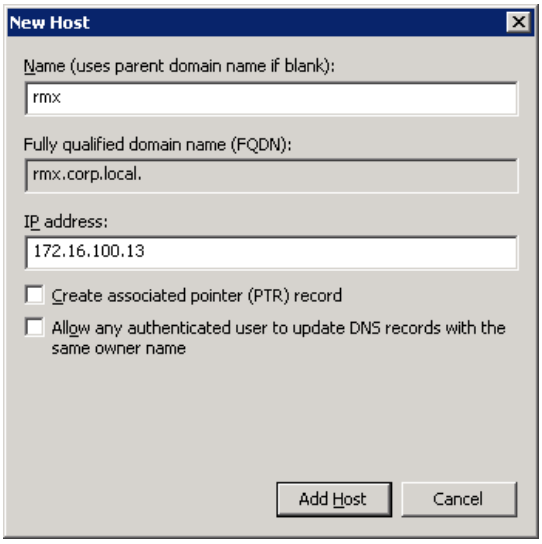
To register with Skype for Business Server, the RealPresence Collaboration Server (RMX) SIP signaling domain must be accessible via the DNS server used by the Skype for Business Server. You need to configure a DNS A record for the FQDN of the RealPresence Collaboration Server (RMX) SIP signaling domain.

The RealPresence Collaboration Server (RMX) solution and the Skype for Business 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**.

Creating and Installing 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 Skype for Business 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.

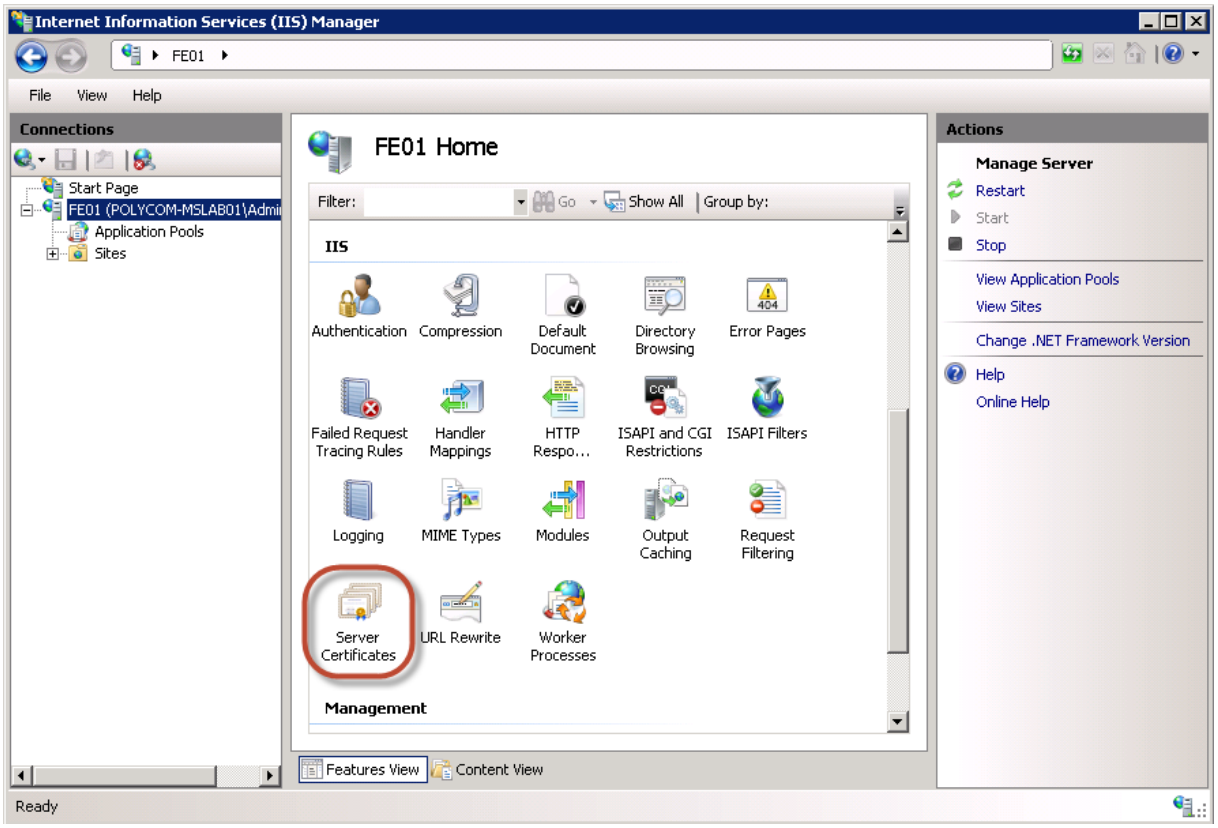
- If your organization permits the submission of certificate requests directly to the enterprise's CA server, you can use the Internet Information Services (IIS) Manager on the Skype for Business Server to download an export file of the certificate to your computer for later installation on the Polycom RealPresence Collaboration Server (RMX) solution. This procedure is described next.

Create a Security Certificate for RealPresence Collaboration Server

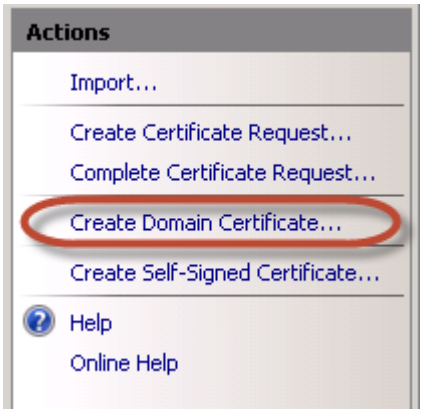
This section shows you how to create a security certificate for the RealPresence Collaboration Server.

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

1. On the Skype for Business 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.



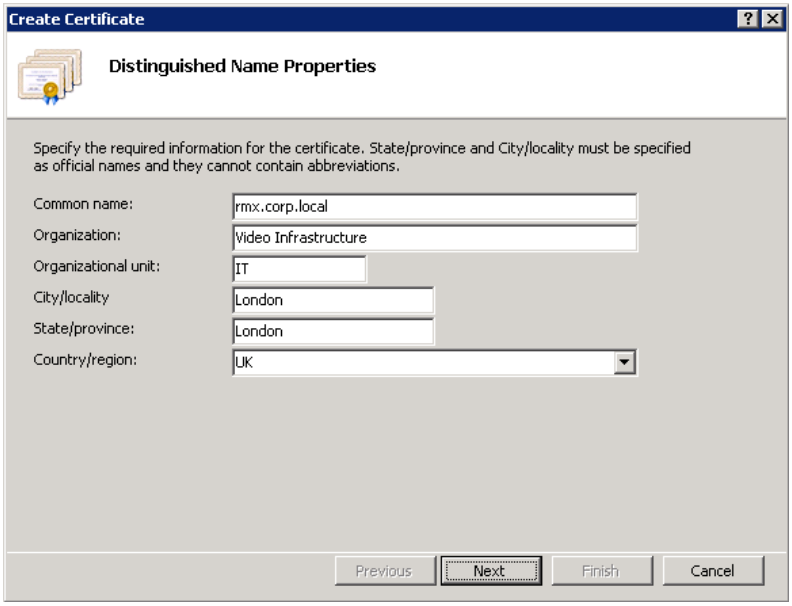
4 In the **Actions** pane on the far right, select **Create Domain Certificate**.



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.



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.

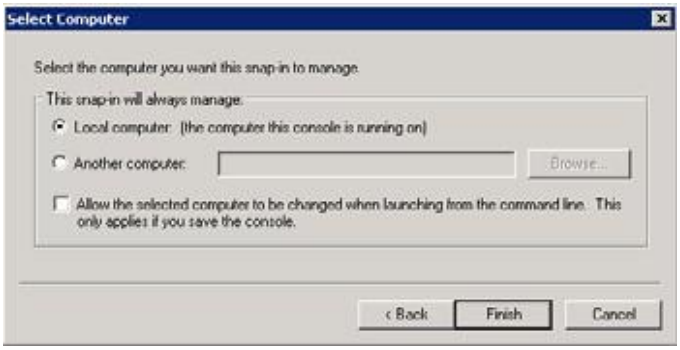
Export the Certificate

After you create the security certificate, export the certificate using the Microsoft Management Console.

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

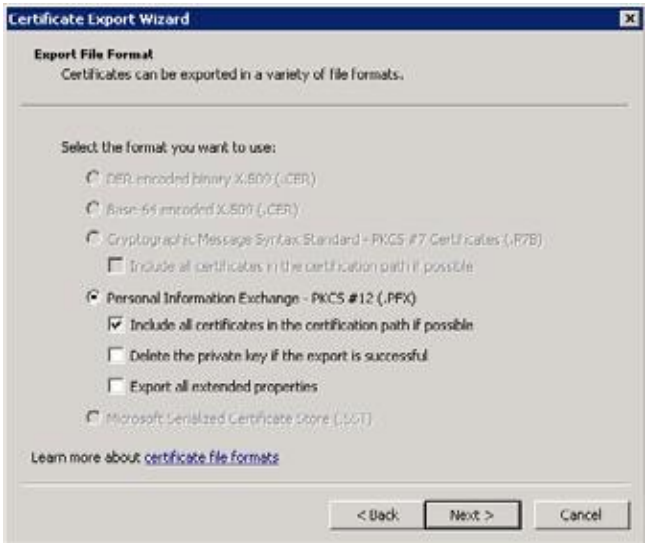
1. Open **Microsoft Management Console** and add the Certificates snap-in.
   a. Choose **File > Add/Remove Snap-in**.
   b. Select **Certificates** from the Available Snap-ins area and click **Add**.
   c. On the **Certificates snap-in** dialog, select **Computer Account** and click **Next**, as shown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

Install the certificate on RealPresence Collaboration Server (RMX) system.

To install the certificate:

» 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 Skype for Business 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 Skype for Business clients, consider changing your Skype for Business Server encryption settings to support encryption rather than require encryption.

As a best practice, Polycom recommends using Microsoft PowerShell commands to update the Cr Server encryption settings. For more details on using PowerShell, see Skype for Business 2015 Management Shell.

To configure Skype for Business Server encryption:

1. Use the following Skype for Business PowerShell command to determine the current encryption setting for Skype for Business Server:

```
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 Skype for Business PowerShell command to change your encryption setting to support encryption:

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

3. Verify your encryption settings:

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

Configuring Skype for Business Server for use with a Polycom RealPresence Collaboration Server (RMX) System

The Polycom 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 Skype for Business Server.

In Microsoft environments, SIP domains often match the email domain. As an alternative, you can use a separate SIP domain for your Skype for Business 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.

Polycom recommends using Skype for Business PowerShell commands to perform the following tasks. For detailed documentation on using Skype for Business PowerShell, see Skype for Business 2015 Management Shell.

Define Your Trusted Application Pool Using Skype for Business Topology Builder

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 > Skype for Business Server 2015 > Skype Server Topology Builder** to open the Skype for Business 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.

Create the Trusted Application Using Skype for Business PowerShell

This step creates the trusted application using the Skype for Business PowerShell.

To create the trusted application:

1 Navigate to **Start > All Programs > Skype for Business Server 2015 > Skype for Business Server Management Shell** to open the Skype for Business 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 Skype for Business 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 TechNet 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 Skype for Business deployment.

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

Note: 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

Use Skype for Business PowerShell to Update the Topology

This step shows you how to use Skype for Business PowerShell to update the topology.

To update the topology:

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

```
Enable-CsTopology
```

Enabling 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 Skype for Business Server.)

Note: Federation and CAC are supported only for Polycom endpoints and devices registered to a Skype for Business Server.

Required Ports

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

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

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

Microsoft Required Ports

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

Setting 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.

Obtain the Trusted Application Service GRUU Identification

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

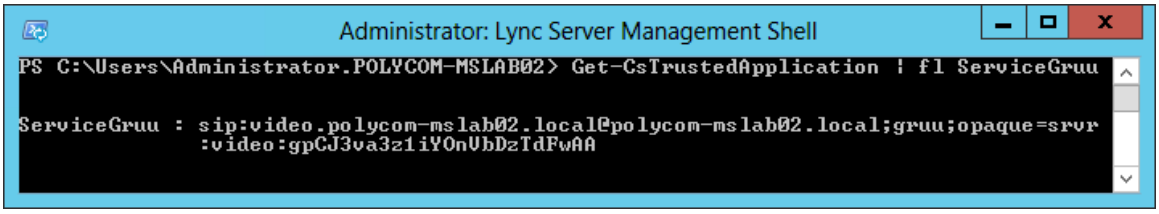
If you are deploying multiple RealPresence Collaboration Servers, the Globally Routable User Agent URI (GRUU) information can be shared as long as the existing Trusted Application Pool and Application ID are used.

In prior releases, creating an account in Active Directory was necessary only for Skype for Business deployments with an Edge Server deployed to facilitate federated or remote worker calling. You must now enable ICE with or without Edge Server deployments.

To obtain the service GRUU identification:

1. Navigate to **Start > All Programs > Skype for Business Server 2015 > Skype for Business Server Management Shell** to open the Skype for Business 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
   ```



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 you obtained without the prefix *sip:*. For example, use:

   ```
   video.polycom-mslab02.local@polycom-
   mslab02.local;gruu;opaque=srvr:video:gpCJ3va3z1iYOnVbDzTdFwAA
   ```

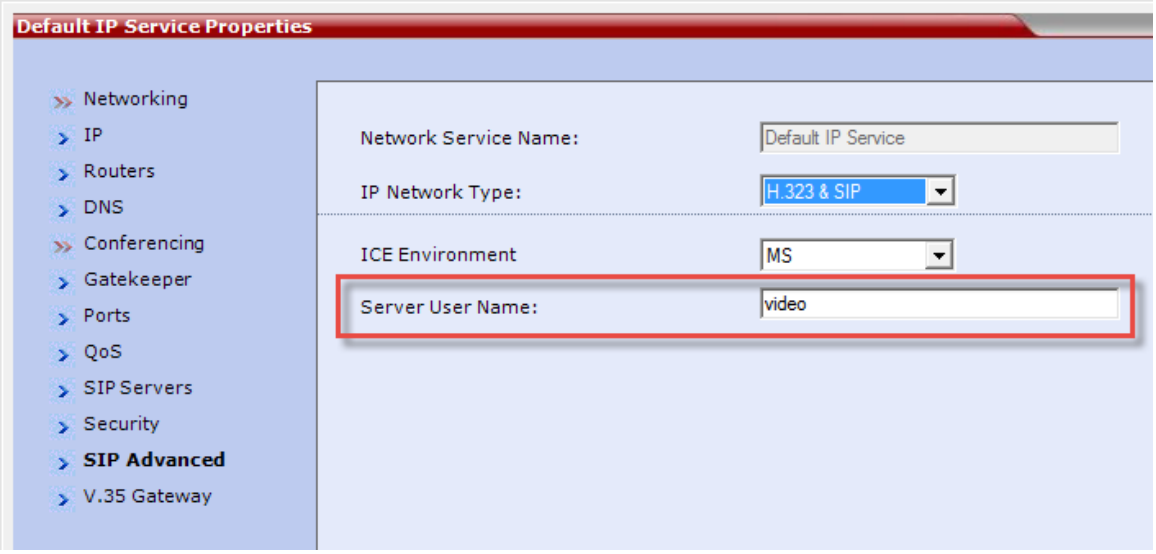
Configure the RealPresence Collaboration Server (RMX) System for Edge Server Support

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

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.

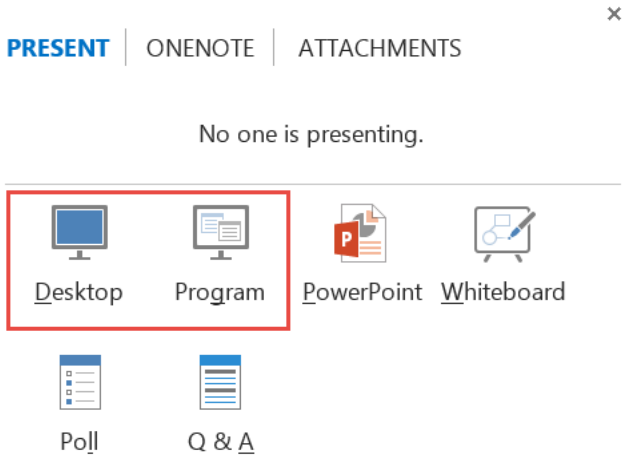
   The system lists the ICE servers it is connected to, the connection status, and the status of the firewall detection in the RealPresence Collaboration Server (RMX) solution.

Deploying Polycom ContentConnect Software

This section explains how to configure Polycom ContentConnect software solution components with Skype for Business. 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-BFCP content gateway, fully transcoding RDP and BFCP H.264 content streams.

Because Gateway Mode facilitates RDP-BFCP transcoding, not all Skype for Business sharing modalities are supported. When sharing content via Skype for Business, 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 Skype for Business 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 Skype for Business clients, only an Edge server is required.

Required Polycom ContentConnect software components for Skype for Business

Component
Management Systems and Recorders
Microsoft Active Directory Server
Gatekeepers, Gateways, and MCUs
Skype for Business
Microsoft Lync Server 2013
Polycom RealPresence Distributed Media Application (DMA) 7000
Polycom RealPresence Collaboration Server (RMX) Software MCU/1500/1800/2000/4000 (8.5 or higher)

Component
Microsoft Endpoints Gateway Mode Skype for Business client installed on Windows, Mac, mobile platforms (iOS, Android, Windows), and Skype for Business 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 Skype for Business Server.

Optional Polycom ContentConnect software components for Skype for Business

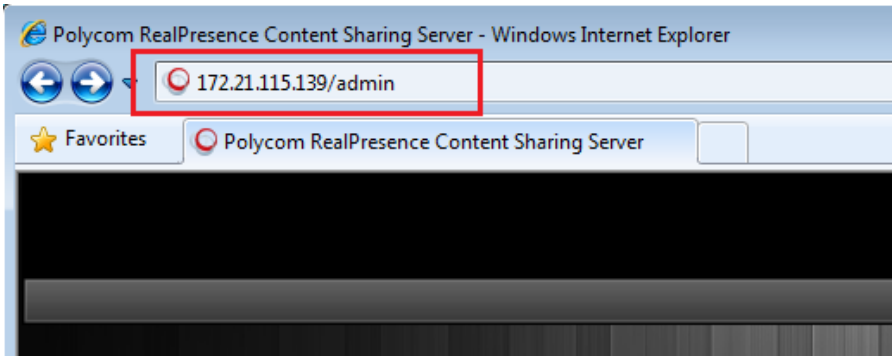
Component
Firewall, Border Controllers Edge Server Polycom RealPresence Access Director Acme Packet® Net-Net Enterprise Session Director (ESD)
Recorders Polycom RealPresence Media Suite
Load Balancers Polycom has tested the following load balancer: F5 BIG-IP LTM 1600 and BIG-IP 10.2.1.297.0

Access 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.



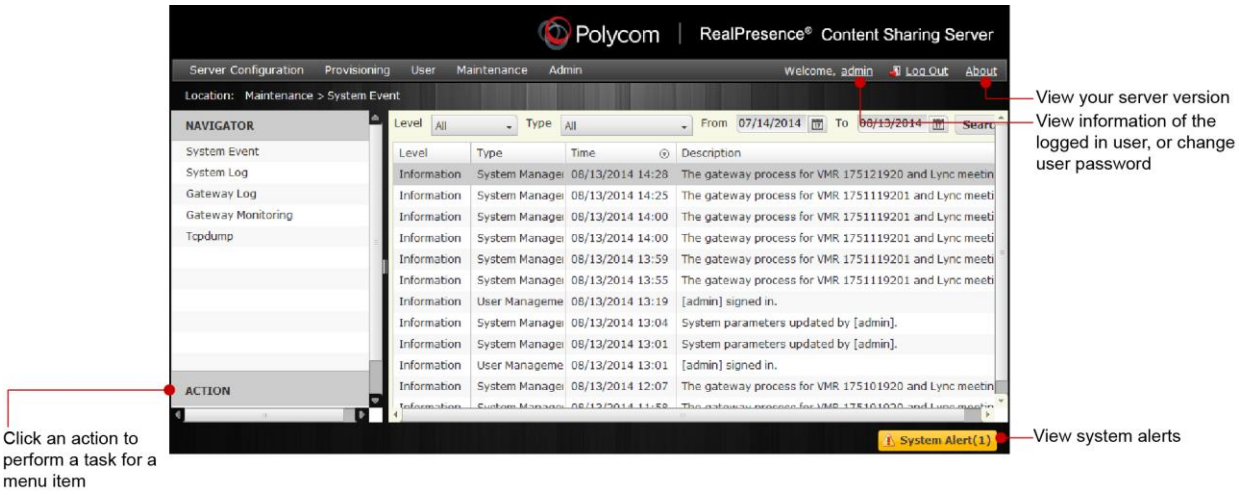
2. Press **Enter**.

   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.

Configuring 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 and Add-On. This guide provides steps required to configure Gateway Mode and does not address Add-on Mode.

- 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. Skype for Business clients don't need to install the Polycom RealPresence Content Add-on for Skype for Business 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.
  - Only H.264 content is supported on legacy endpoints in the Gateway mode.
- Add-On Mode
  - All Skype for Business clients must install the Polycom RealPresence Content Add-on for Skype for Business 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.

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 Skype for Business Service** installed already, it will be disabled.

6 Click **Save**.

Configure Server Information

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

To configure server information settings:

1 Log in to the Content Sharing Server Web Configuration Tool.

2 Select **Server Configuration > Server**.

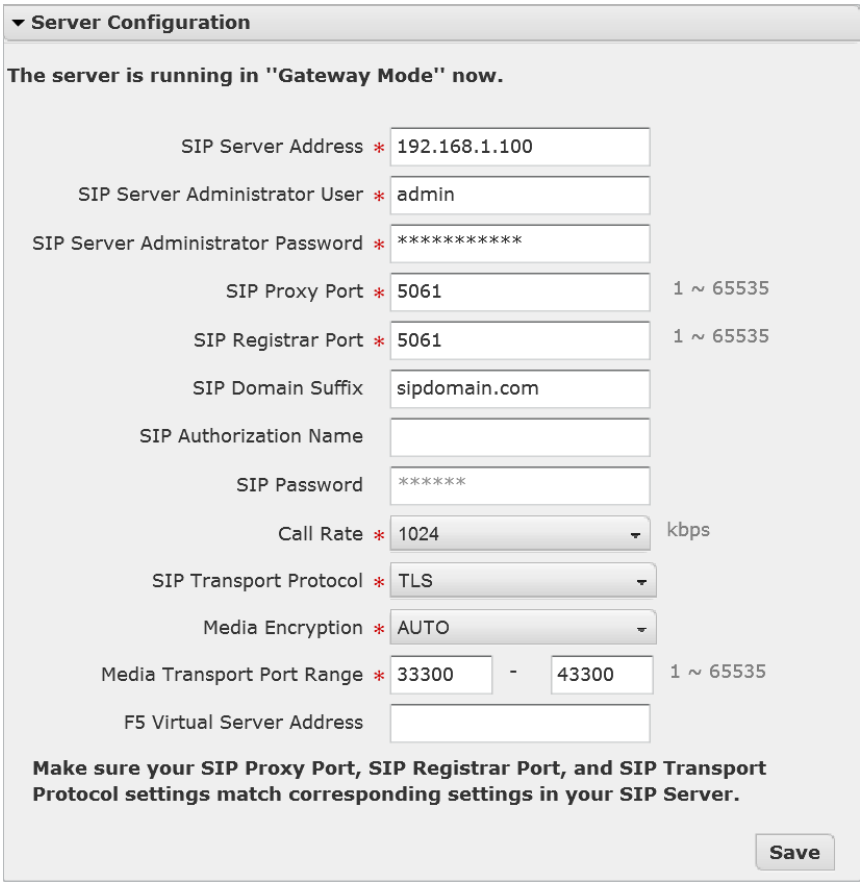
3 Enter the following information:

- **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 Skype for Business 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



Configuring RealPresence DMA System for Skype for Business

Complete the five tasks in this section to configure a RealPresence DMA system with Skype for Business Server.

Ensuring 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

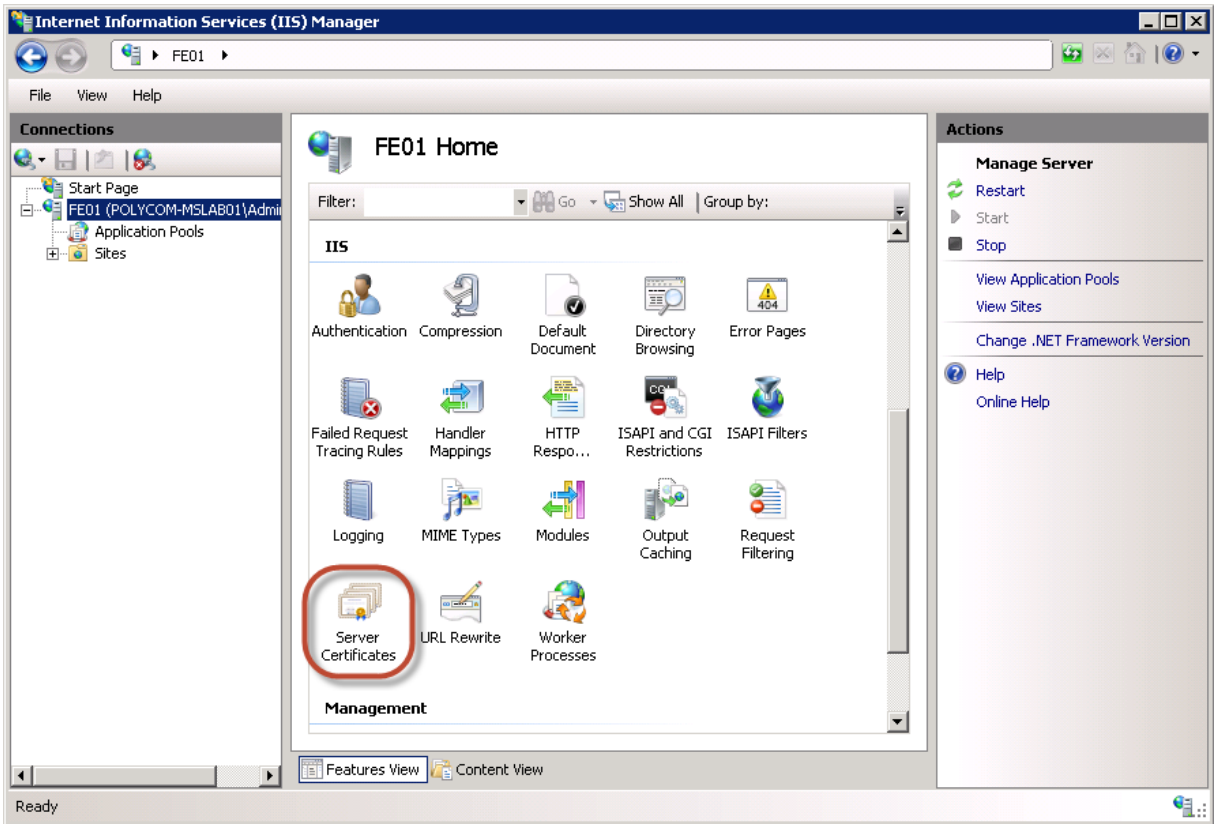
The second step in configuring a RealPresence DMA system with Skype for Business Server is to install a security certificate on the RealPresence DMA system so that Skype for Business Server trusts it. You can purchase or install a certificate or request and obtain a certificate from your enterprise CA,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

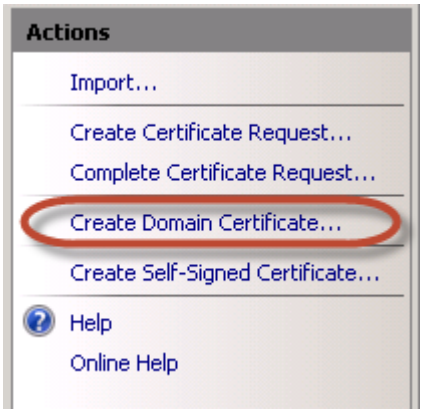
To create a security certificate for the RealPresence DMA system using IIS Manager 7:

1. On the Skype for Business 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.



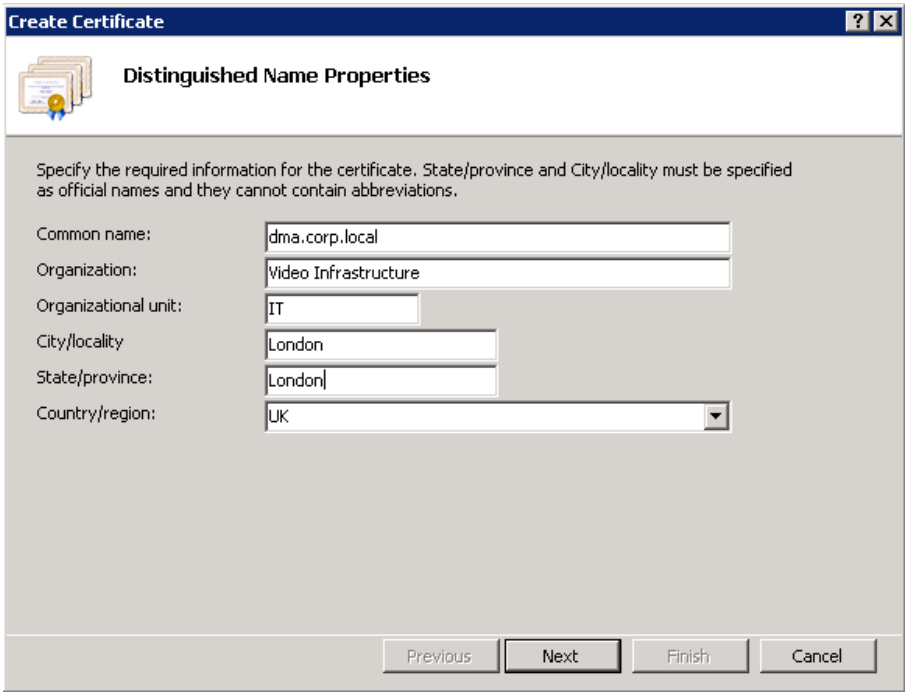
4 In the **Actions** pane (far right), select the **Create Domain Certificate**, shown next.



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.



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.

Export a Security Certificate

After you create a security certificate, use the Microsoft Management Console to export the certificate.

To use the Microsoft Management Console to export the 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**.

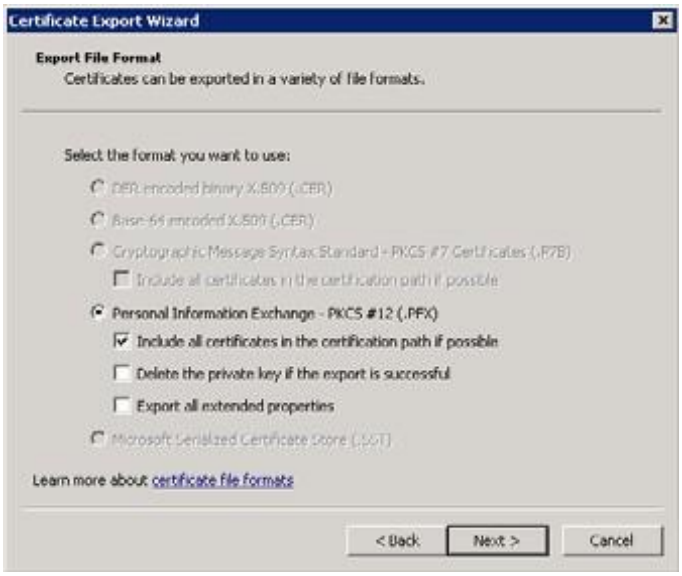
4 Right-click the created certificate and select **All Tasks > Export** to view the Certificate Export wizard.

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.

Configure a RealPresence DMA System SIP Peer for Skype for Business Server

In the RealPresence DMA system, configure Skype for Business Server an external SIP peer. This allows SIP calls routed from the RealPresence DMA system to reach devices registered to the server.

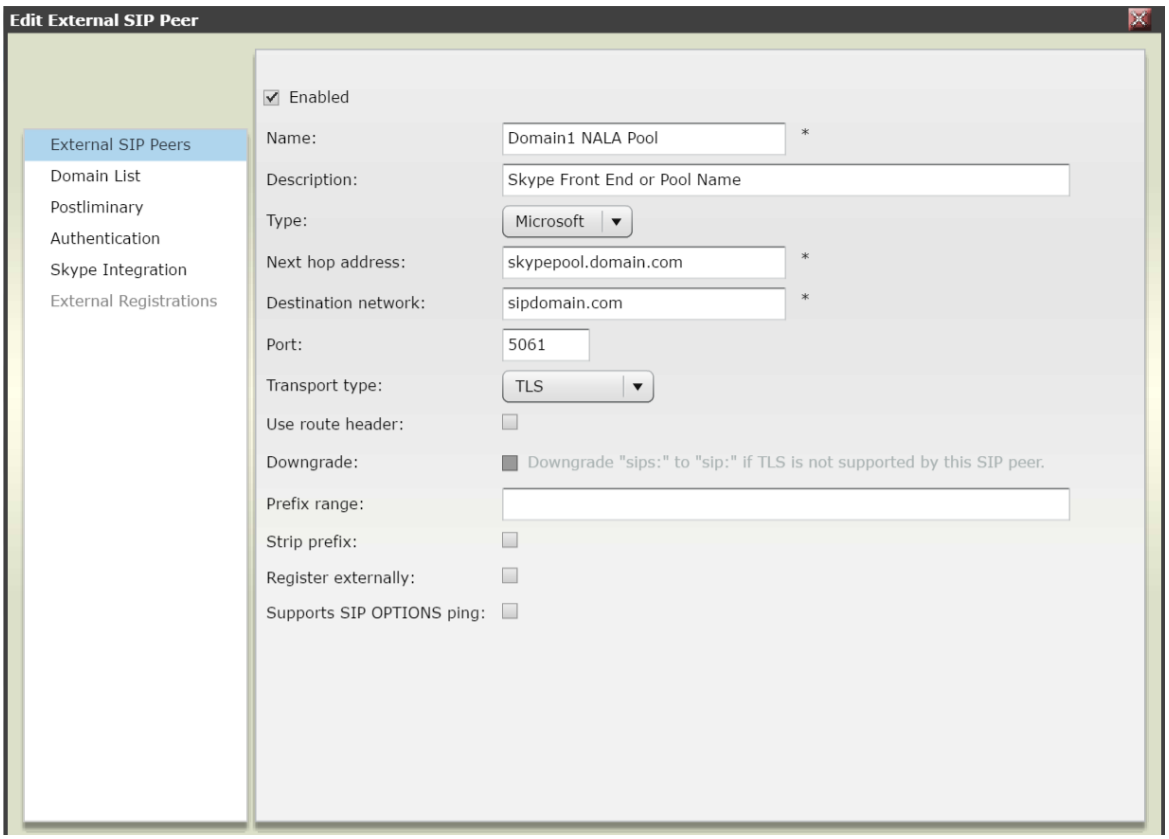
To configure the RealPresence DMA system as a SIP Peer for Skype for Business calls:

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.



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 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 Front End Server or your Pool.

8 In the **Port** field, enter the SIP port to use. Skype for Business 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**.

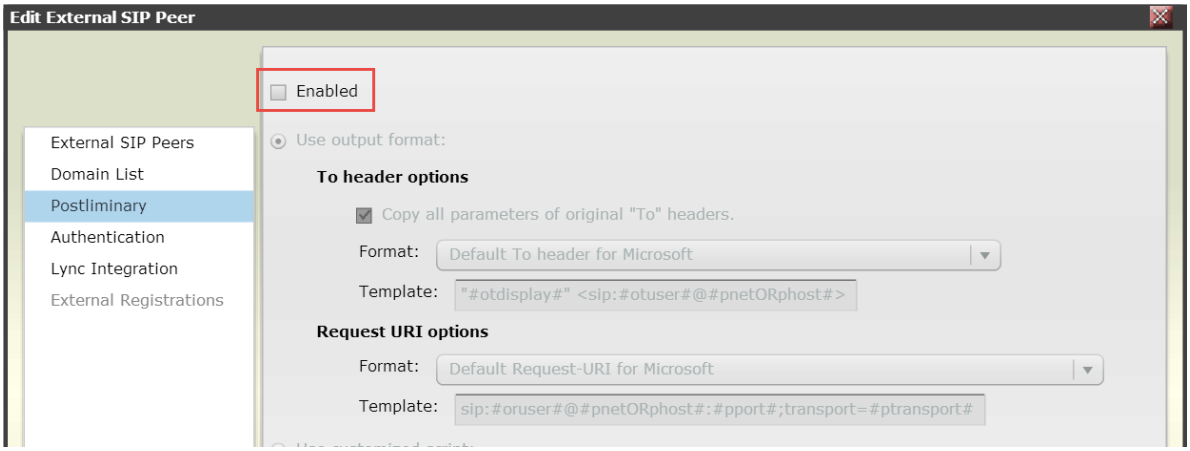
12 In the **Transport Type** drop-down list, select **TLS**.

13 Go to the **Skype for Business Integration** tab, check **CsTrustedApplication ServiceGruu**, and enter the GRUU information you obtained in the section 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 Skype for Business Server.

As shown in the following illustration, do not enable the postliminary script, which by default handles the Polycom ContentConnect gateway.



Next, complete the Skype for Business 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.

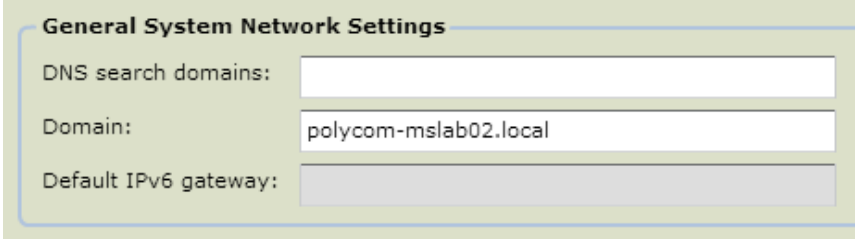
Configure RealPresence DMA system network settings to match the Skype for Business Server, specifically, Time and Domain. You need to configure the domain to match the extension you gave to the RealPresence DMA system DNS name.

Specify a Domain and Time on the RealPresence DMA System

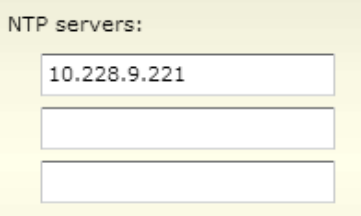
Next, specify domain and time on the RealPresence DMA system.

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.**



2 Configure the time to synchronize with the same source as the Skype for Business 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.



Configure the RealPresence DMA System Skype for Business Conference Template

Next, service providers must create a conference template that is assigned to Polycom RealConnect 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 Skype for Business Server which allocated it, a prefix is added to the conference ID to enable the DMA to identify remote Polycom RealConnect conferences.

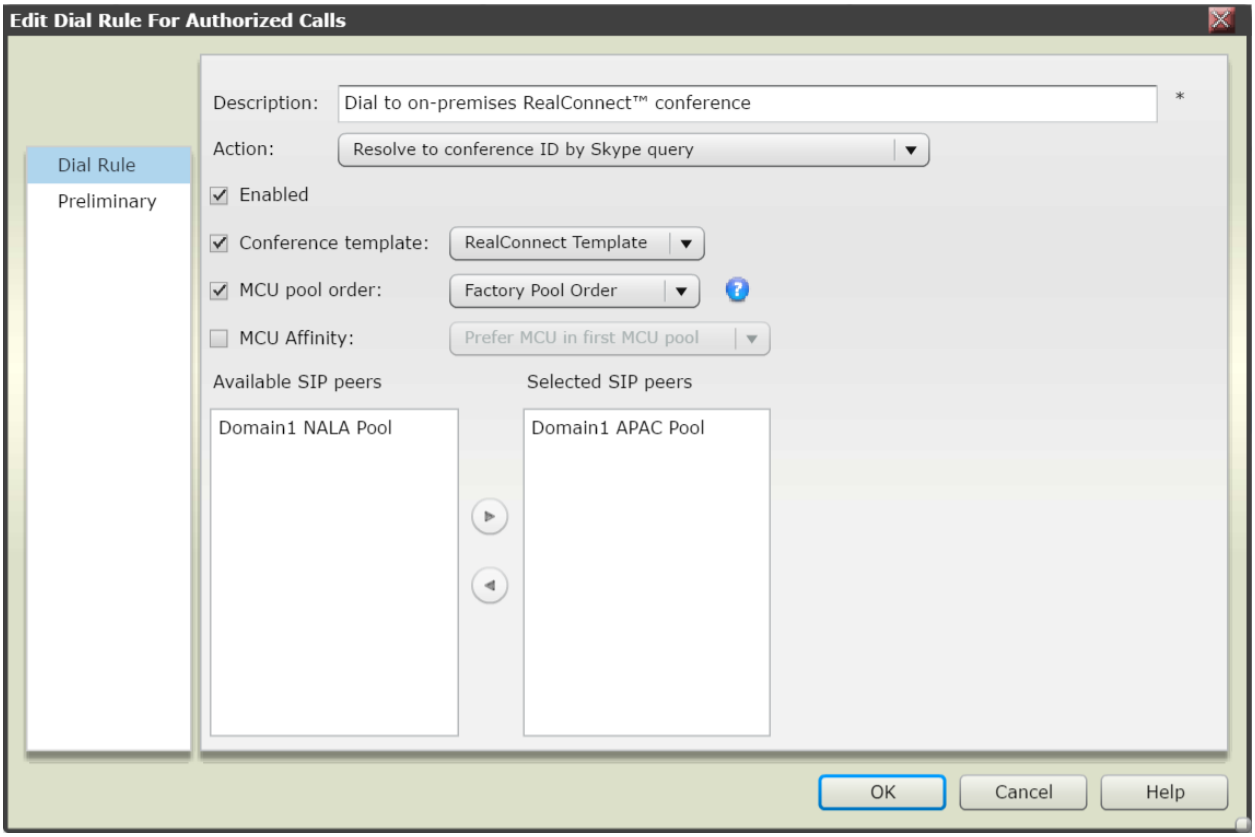
The Skype for Business service administrator of an organization hosting Skype for Business meetings, can add the respective organization prefix into the Outlook meeting invites sent by meeting organizers. This insertion requires the Skype for Business service administrator to configure the added text only once, via the Skype for Business 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 Skype for Business 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.**

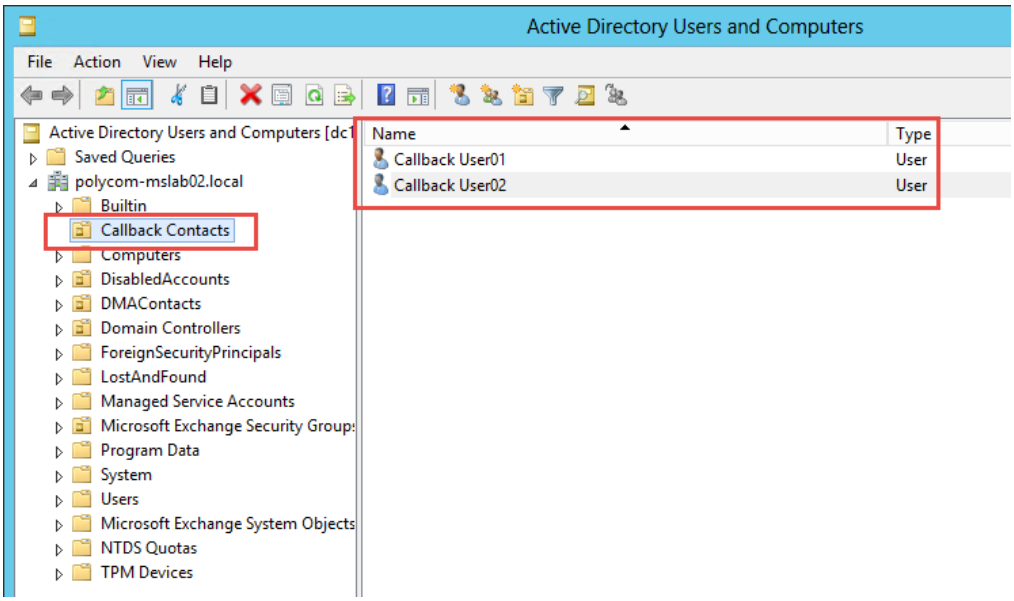
Polycom RealConnect configuration is complete.

Configure the Directory Server and Domain

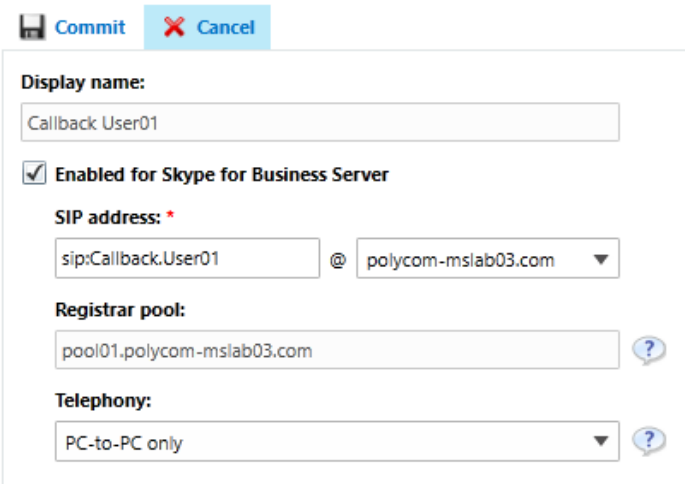
Next, configure the directory server and domain using the Active Directory domain and not the SIP domain.

To configure the directory server and domain:

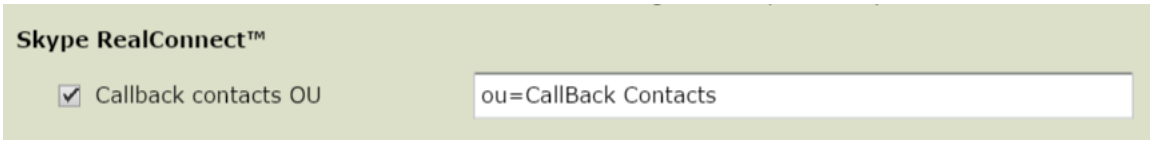
1. If you are deploying an external Skype for Business system, configure a ‘Callback contacts’ Active Directory Organizational Unit that contains Skype for Business-enabled contacts that establish federated Skype for Business conferences. The following example illustrates a container created from the root domain `Polycom-mslab02.local`.



2. Enable callback Skype for Business accounts for telephony between computer endpoints and enable dial out via federation.



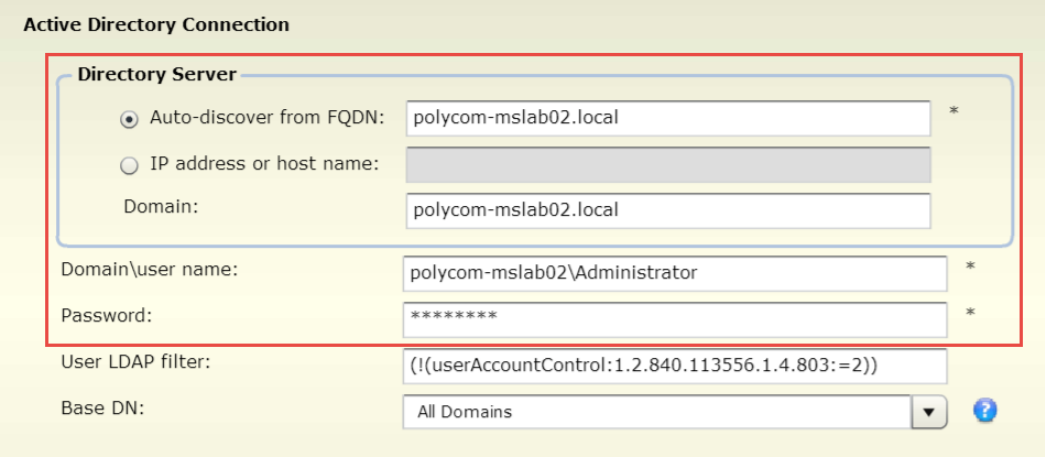
3. Configure the following container within the Active Directory Integration page on the DMA system.



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**.

To ensure you can dial each customer's conference auto attendant via federation, log into one of the callback user accounts in Skype for Business



Configure a Connection to the Federated Deployment

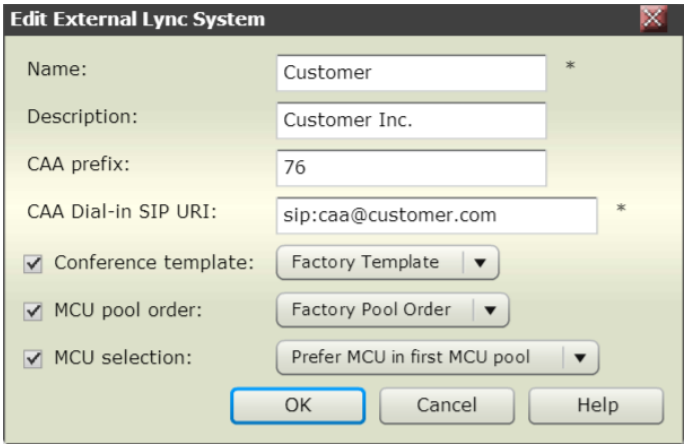
After you configure the directory server and domain, configure the connection to the remote federated deployment.

To add the remote Skype for Business deployment:

1 In the DMA system manager go to **Admin > Conference Manager > External Skype for Business 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 Skype for Business meetings. You can configure an external Skype for Business system with or without a specific prefix. Note however that you can define only one external Skype for Business system without a prefix.

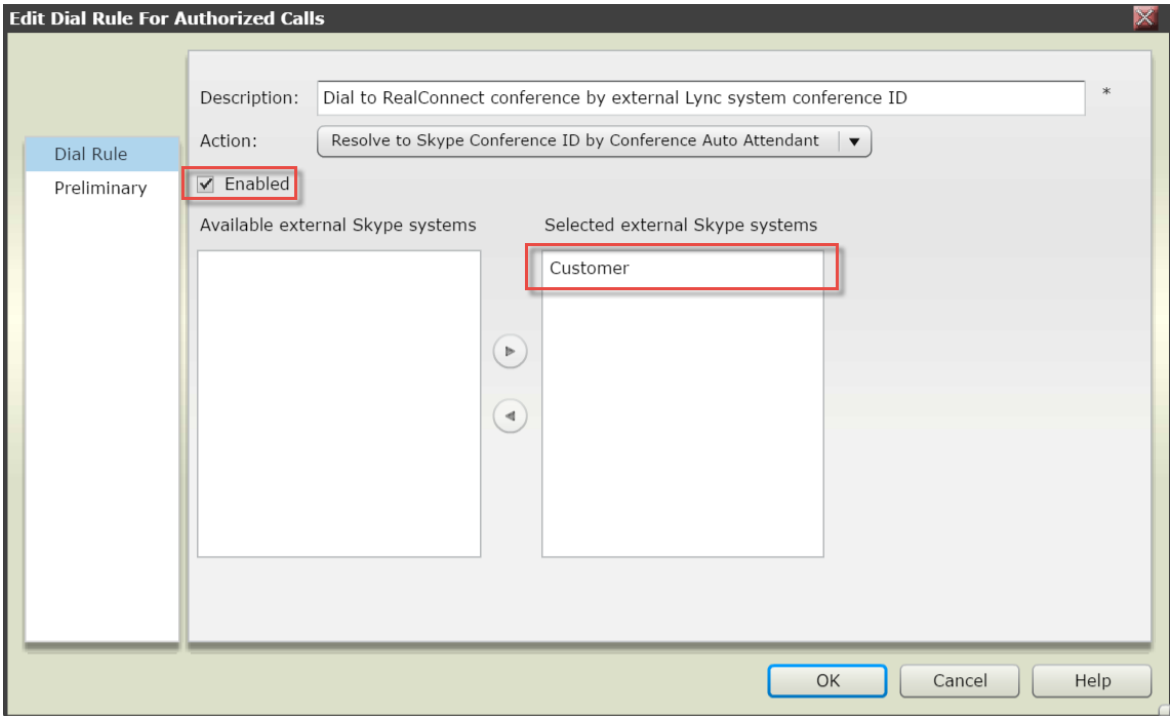


4 Enable a corresponding dial rule named ‘Dial to RealConnect conference by external Skype for Business system conference ID’’, shown next.

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 Confere	No	Enabled
#9	External Lync SIP Peer	Resolve to external SIP peer	No	Enabled

5 Add the external Skype for Business 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><SkypeConferenceID>@<Domain>
- 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:

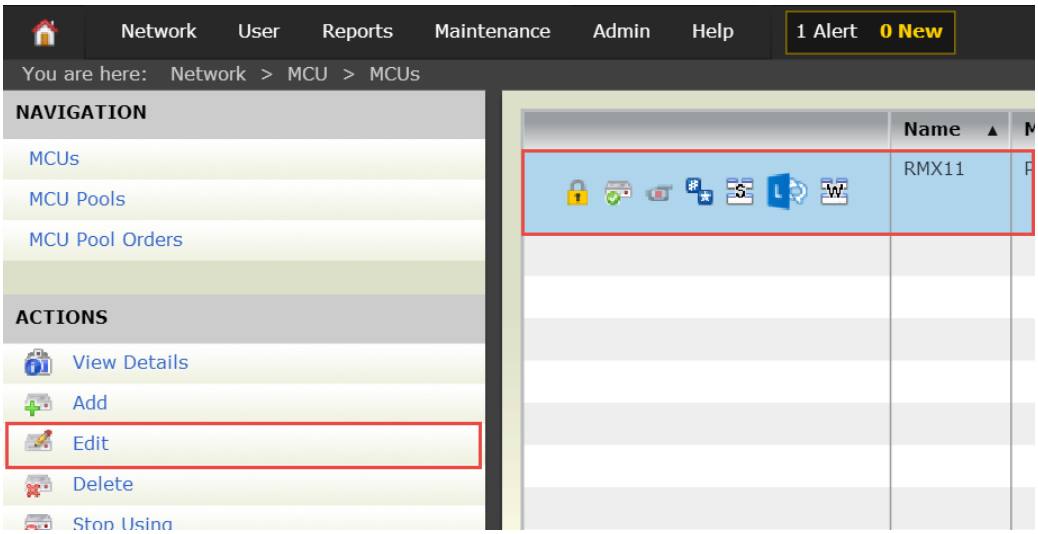
If you are using SIP-registered VTCs, when you create a VEQ, you do not need to dial a prefix and users can dial the Skype for Business Conference ID directly.

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:

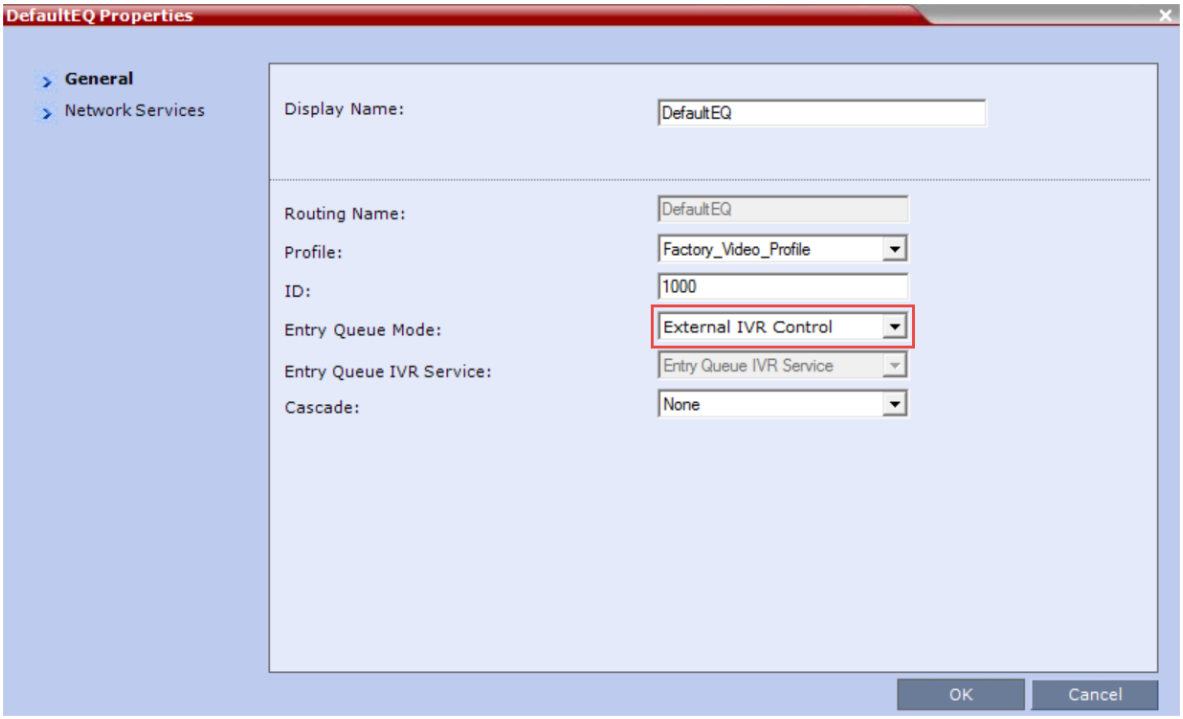
1 In the existing MCU, go to **Network > MCU > MCUs**, select the existing MCU, and click **Edit > OK**.



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**.



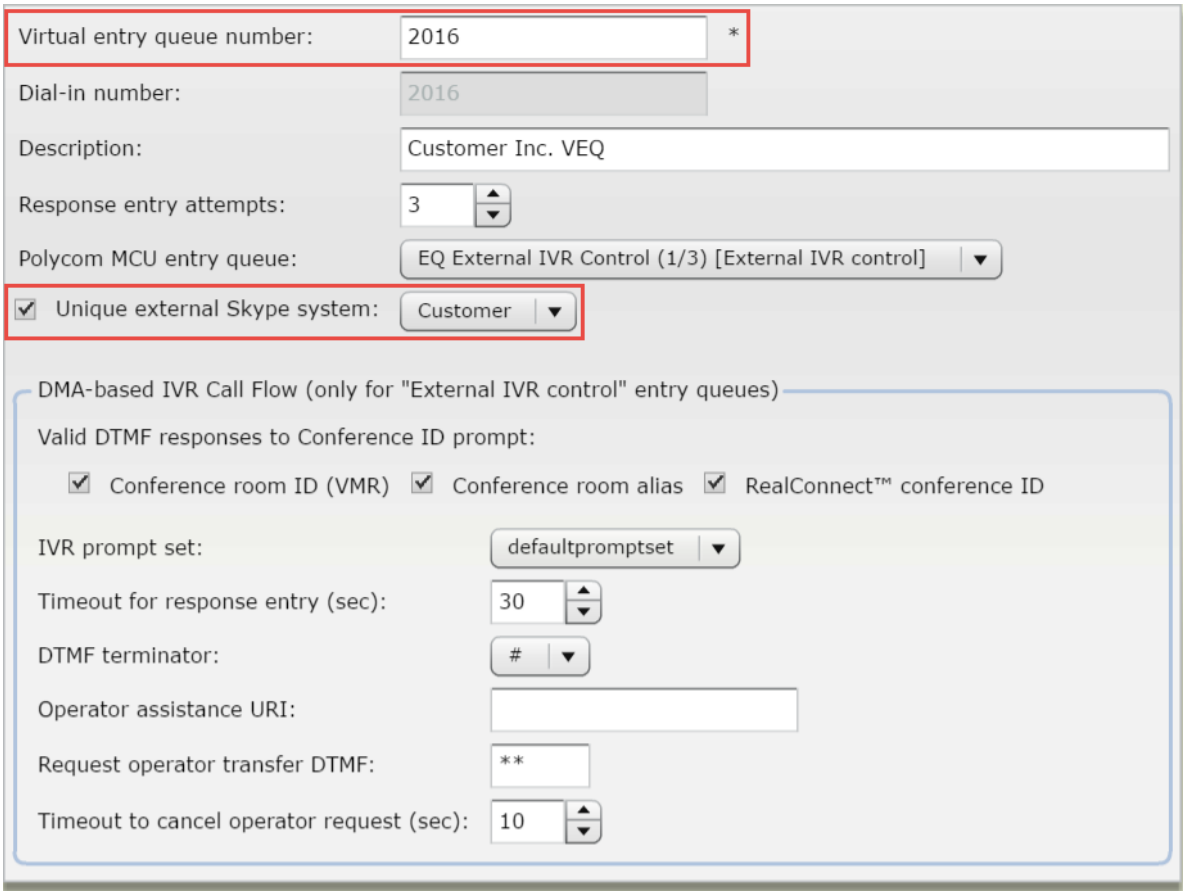
Configure the RealPresence DMA System

After you enable VEQ on one or more of your MCUs integrated with the RealPresence 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 **2016**.

3 Enable **Unique external Skype system**, set to the external Skype for Business system you specified previously, shown here as **Customer**, and click **OK**.



Appendix G: Deploying in Secure/Federal Environments

Use this appendix as a reference to this Solution Deployment Guide when deploying the Polycom Microsoft solution in a secure environment. This appendix points to:

- Restrictions and limitations of the solution in a secure environment
- Product-specific configurations
- Additional steps to complete and steps in this Solution Deployment Guide to ignore

Additional Skills and Resources for Secure Environments

Administrators require the following additional background, skills and resources when deploying this solution in a secure federal environment:

- Knowledge of local security policies enforced in the secure environment
- UCR and applicable Security Technical Implementation Guide (STIG) requirements
- Applicable Polycom documentation for each Polycom product you are installing and deploying in a secure environment. You can locate Polycom supporting documentation at Documents & Downloads on Polycom Support or contact your Polycom representative.

Feature Restrictions/Limitations in Secure Federal Environments

This Polycom solution for Microsoft is subject to the following restrictions when deployed in federal secure environments:

- No support for remote/federated users
- No support for Polycom ContentConnect software server
- No support for Polycom HDX systems (UC APL version 2.7.3.2 does not support Skype for Business integration)

Product-Specific Configuration Guidelines

Configuration guidelines vary when deploying Polycom products in a federal secure environment. This section indicates specific configuration guidelines for each product you are installing and deploying in a federal secure environment.

RealPresence Group Series Systems

Complete the initial installation of Group Series systems as outlined in the *Polycom RealPresence Group Series for Maximum Security Environments – Deployment Guide*.

The following lists exceptions in this Polycom for Microsoft Solution Deployment Guide when deploying RealPresence Group Series systems:

- Do not configure Calendaring Services (no Click-to-Join) for RealPresence Group Series systems
- Do not enable connection with remote/federated users
- Polycom® Touch Control is not supported
- Do not enable conference room access for remote and federated users for RealPresence Groups Series systems.

Polycom HDX Systems

Polycom HDX systems are not supported for deployment with Microsoft Skype for Business or Lync Server in secure federal environments.

Polycom ITP Systems

Polycom ITP systems are not certified for use in a secure federal environment.

Polycom RealPresence Collaboration Server (RMX) Systems

Complete the initial installation of RealPresence Collaboration Server (RMX) systems for secure environments and follow local policies and procedures for creating and installing identity certificates on the Collaboration Server (RMX) systems.

The following lists exceptions in this Polycom for Microsoft Solution Deployment Guide when deploying Collaboration Server:

- No support for integration with a Microsoft Edge Server
- No support for integration with Polycom ContentConnect

Polycom RealPresence DMA Systems

Complete the initial setup of Polycom DMA systems and follow local policies and procedures for creating and installing identity certificates on the Polycom DMA system.

The following lists exceptions in this Polycom for Microsoft Solution Deployment Guide when deploying Polycom DMA systems:

- No support for remote/federated users

Troubleshooting

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

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 Skype for Business Server deployment, you must enable Polycom HDX or RealPresence Group Series system users for remote access and federation as shown in Enabling Federation in your Skype for Business Environment.

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.
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.