Polycom® Unified Communications for Cisco Environments
Contents

About This Guide ..................................................................................................................... 6

Conventions Used in this Guide .............................................................................................. 6
Terms and Writing Conventions .............................................................................................. 6
Information Elements ............................................................................................................. 7
Typographic Conventions ..................................................................................................... 8

Chapter 1: Get Started ......................................................................................................... 9

Required Skills ....................................................................................................................... 9
Frequently Asked Questions ................................................................................................... 10
What’s New? ........................................................................................................................... 10
Get Help and Support Resources ......................................................................................... 10
The Polycom Community ...................................................................................................... 11

Chapter 2: Polycom Unified Communications with Cisco Interoperability .......................... 12

Supported Deployment Models .............................................................................................. 12
Direct Registration of Polycom RealPresence Systems with Cisco Unified CM .................. 12
Direct Secure Registration of Polycom RealPresence Systems with Cisco Unified CM .......... 12
Polycom RealPresence Platform SIP Integration with Cisco Unified CM .......................... 13
Polycom RealPresence Platform Integration with VCS ......................................................... 13
Polycom RealPresence Platform SIP Integration with Cisco CUBE SP Edition .................. 13

Chapter 3: Direct Registration of Polycom RealPresence Systems with Cisco Unified CM .... 14

Deployment Model Advantages ............................................................................................. 14
Supported Products for Deployment ...................................................................................... 14
Deployment Architecture ...................................................................................................... 16
Design Considerations .......................................................................................................... 16
Cisco Unified Communications Manager Considerations .................................................. 16
Polycom Immersive Telepresence Systems Considerations ............................................... 17
Share Content in Telepresence Environments ..................................................................... 17
License Devices ..................................................................................................................... 18

Register a Polycom RealPresence Immersive, Room, or Desktop System with Cisco Unified CM ......................................................................................................................... 18

Configure Cisco Unified CM for a Polycom Immersive, Room, or Desktop System .......... 19
Configure a Polycom Group Series System for Cisco Unified CM Registration ................ 27
Configure a Polycom HDX or Immersive System for Cisco Unified CM Registration ........29
Define your Polycom Immersive System in the Cisco TelePresence Server (Optional) ......33

**Configure SIP Integration Between a Polycom RealPresence Collaboration Server System and Cisco Unified CM** ..................................................................................................................................................33
Configure Cisco Unified CM for SIP Integration with RealPresence Collaboration Server ..34
Configure the RealPresence Collaboration Server for Cisco Unified CM SIP calls ...........37
Prepare the RealPresence Collaboration Server to Support TIP Calls (Optional) ..........40

Troubleshoot .......................................................................................................................................................47

Chapter 4: Direct Secure Registration of Polycom RealPresence Systems with Cisco Unified CM .........................................................................................................................................................49

Deployment Model Advantages ............................................................................................................................49
Supported Products for Deployment ..................................................................................................................50
Deployment Architecture ......................................................................................................................................51
Design Considerations ............................................................................................................................................51
Cisco Unified Communications Manager Considerations ..................................................................................51
Polycom Immersive Telepresence Systems Considerations ............................................................................52
Content Sharing in Telepresence Environments ..............................................................................................52
License Devices ....................................................................................................................................................53
Secure Media Methods .......................................................................................................................................53

**Securely Register a Polycom RealPresence Immersive, Room, or Desktop System with Cisco Unified CM** .................................................................................................................................................54
Configure Cisco Unified CM for a secure Polycom Immersive, Room, or Desktop System 55
Configure a Polycom HDX or Immersive System for Cisco Unified CM Registration ...........62
Define your Polycom Immersive System in the Cisco TelePresence Server (Optional) .....67

Troubleshoot .......................................................................................................................................................68

Chapter 5: Polycom RealPresence Platform SIP Integration with Cisco Unified CM ........................................................................................................................................................................69

Supported Products for Deployment ..................................................................................................................69
Deployment Architecture ........................................................................................................................................71
Design Considerations ...........................................................................................................................................71
Use a Dial Plan .......................................................................................................................................................71
Use Call Admission Control ...............................................................................................................................71
Share Content .......................................................................................................................................................71

**Configure SIP Integration between a Polycom DMA System and Cisco Unified CM** ....................................................................................................................................................................................72
Configure Cisco Unified CM for SIP Integration with DMA .............................................................................73
Configure DMA for SIP Integration with Cisco Unified CM .............................................................................79

Troubleshoot .......................................................................................................................................................84

Chapter 6: Polycom RealPresence Platform Integration with VCS ..................................................................87

Deployment Model Advantages ............................................................................................................................87
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Products for Deployment</td>
<td>87</td>
</tr>
<tr>
<td>Deployment Architecture</td>
<td>88</td>
</tr>
<tr>
<td>Design Considerations</td>
<td>89</td>
</tr>
<tr>
<td>Dial Plan</td>
<td>89</td>
</tr>
<tr>
<td>Call Admission Control</td>
<td>89</td>
</tr>
<tr>
<td>Protocol Conversion</td>
<td>90</td>
</tr>
<tr>
<td>Configure SIP Integration Between a Polycom DMA System and VCS</td>
<td>90</td>
</tr>
<tr>
<td>Configure VCS for SIP Integration with DMA</td>
<td>90</td>
</tr>
<tr>
<td>Configure DMA for SIP Integration with VCS</td>
<td>93</td>
</tr>
<tr>
<td>Configure H.323 Integration between a Polycom DMA System and VCS</td>
<td>97</td>
</tr>
<tr>
<td>Configure VCS for H323 Integration with DMA</td>
<td>97</td>
</tr>
<tr>
<td>Configure DMA for H323 Integration with VCS</td>
<td>101</td>
</tr>
<tr>
<td>Troubleshoot</td>
<td>104</td>
</tr>
</tbody>
</table>

Chapter 7: Polycom RealPresence Platform SIP Integration with Cisco CUBE SP Edition

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Model Advantages</td>
<td>106</td>
</tr>
<tr>
<td>Supported Products for Deployment</td>
<td>107</td>
</tr>
<tr>
<td>Deployment Architecture</td>
<td>108</td>
</tr>
<tr>
<td>Design Considerations</td>
<td>108</td>
</tr>
<tr>
<td>Configure SIP Integration between a Polycom DMA System and CUBE SP Edition</td>
<td>109</td>
</tr>
<tr>
<td>Configure CUBE SP for SIP Integration with DMA</td>
<td>109</td>
</tr>
<tr>
<td>Configure DMA for SIP Integration with CUBE SP</td>
<td>110</td>
</tr>
<tr>
<td>Troubleshoot</td>
<td>115</td>
</tr>
<tr>
<td>Configuration Example</td>
<td>117</td>
</tr>
</tbody>
</table>
About This Guide

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

Conventions Used in this Guide

This guide contains terms, graphical elements, and a few typographic conventions. Familiarizing yourself with these terms, elements, and conventions helps you complete tasks.

Terms and Writing Conventions

The following terms are used in this deployment guide.

### Polycom Components

<table>
<thead>
<tr>
<th>Polyclom Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMA</td>
<td>Polycom® RealPresence® Distributed Media Application™ (DMA®)</td>
</tr>
<tr>
<td>HDX</td>
<td>Polycom® HDX®</td>
</tr>
<tr>
<td>ITP</td>
<td>Polycom® Immersive Telepresence</td>
</tr>
<tr>
<td>RealPresence Collaboration Server</td>
<td>Polycom® RealPresence® Collaboration Server (RMX)</td>
</tr>
<tr>
<td>OTX</td>
<td>Polycom® Open Telepresence Experience®</td>
</tr>
<tr>
<td>MLA</td>
<td>Polycom® Multipoint Layout Application</td>
</tr>
</tbody>
</table>

### Cisco® Components

<table>
<thead>
<tr>
<th>Cisco® Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CM</td>
<td>Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>CTS</td>
<td>Cisco TelePresence System</td>
</tr>
<tr>
<td>TX</td>
<td>Cisco TelePresence System</td>
</tr>
<tr>
<td>TPS</td>
<td>Cisco TelePresence Server</td>
</tr>
<tr>
<td>VCS</td>
<td>Cisco TelePresence Video Communications Server</td>
</tr>
</tbody>
</table>
General Industry:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>TIP</td>
<td>Telepresence Interoperability Protocol</td>
</tr>
</tbody>
</table>

**Information Elements**

The following icons are used to alert you to important information in this guide.

**Icons Used in this Guide**

<table>
<thead>
<tr>
<th>Name</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td><img src="image" alt="Note Icon" /></td>
<td>The Note icon highlights information of interest or important information needed to successfully complete a procedure or understand a concept.</td>
</tr>
<tr>
<td>Administrator Tip</td>
<td><img src="image" alt="Administrator Tip Icon" /></td>
<td>The Administrator Tip icon highlights techniques, shortcuts, or productivity-related tips.</td>
</tr>
<tr>
<td>Caution</td>
<td><img src="image" alt="Caution Icon" /></td>
<td>The Caution icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.</td>
</tr>
<tr>
<td>Warning</td>
<td><img src="image" alt="Warning Icon" /></td>
<td>The Warning icon highlights an action you must perform or avoid to prevent information loss, damage your configuration setup, and/or affect component or network performance.</td>
</tr>
<tr>
<td>Web Info</td>
<td><img src="image" alt="Web Info Icon" /></td>
<td>The Web Info icon highlights online information such as documents or downloads.</td>
</tr>
<tr>
<td>Timesaver</td>
<td><img src="image" alt="Timesaver Icon" /></td>
<td>The Timesaver icon highlights a faster or alternative method for accomplishing task.</td>
</tr>
<tr>
<td>Power Tip</td>
<td><img src="image" alt="Power Tip Icon" /></td>
<td>The Power Tip icon highlights a faster or alternative method for advanced administrators.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td><img src="image" alt="Troubleshooting Icon" /></td>
<td>The Troubleshooting icon highlights information that can help you solve a problem or refer you to troubleshooting resources.</td>
</tr>
<tr>
<td>Settings</td>
<td><img src="image" alt="Settings Icon" /></td>
<td>The Settings icon highlights settings you might need to choose or access.</td>
</tr>
</tbody>
</table>
## Typographic Conventions

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

### Typographic Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Highlights interface items such as menus, soft keys, file names, and directories. Represents menu selections and text entry to the phone.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Emphasizes text, shows example values or inputs, and shows titles of reference documents available from the Polycom Support web site and other reference sites.</td>
</tr>
<tr>
<td><strong>Blue Text</strong></td>
<td>Indicates URL links to external web pages and internal hyperlinks to locations within the document.</td>
</tr>
<tr>
<td>Fixed-width-font</td>
<td>Represents code fragments and parameter names.</td>
</tr>
</tbody>
</table>
Chapter 1: Get Started

This deployment guide explains how to integrate Polycom® Unified Communications (UC) products into Cisco environments. Each chapter focuses on a distinct architecture, and each chapter contains a list of the Cisco and Polycom products tested with that architecture. This deployment guide is intended for administrators integrating Cisco with Polycom products and for support personnel working with customers to set up the solutions described in this guide.

This deployment guide focuses on several Cisco call control infrastructure scenarios. Cisco® Unified Communications Manager (Cisco Unified CM) CUCM is Cisco’s UC platform providing Internet Protocol (IP) telephony and advanced features. It is a multiprotocol-capable platform that has been migrating towards SIP endpoint connectivity. Cisco Video Communications Server (VCS) was inherited via Cisco’s acquisition of Tandberg, and has historically provided H.323 and SIP call control for video endpoints.

Polycom’s integrated suite of hardware devices and software applications enables you to integrate video and audio communications across Cisco platforms and provides Polycom customers new deployment opportunities and investment protection for existing deployments.

Web Info: See the Release Notes for Polycom Unified Communications for Cisco Environments

Find the latest release notes for Polycom Unified Communications for Cisco Environments at Polycom Unified Communications with Cisco.

Required Skills

Integrating Polycom infrastructure and endpoints with Cisco Unified Communications Manager environments requires planning and elementary knowledge of Polycom video conferencing and video conferencing administration.

Polycom assumes readers of this guide have a basic understanding Session Initiation Protocol (SIP) and Telepresence Interoperability Protocol (TIP), as well as Cisco and Polycom component base functions. Users should be comfortable navigating and configuring Cisco components such as Cisco Unified CM, VCS, and other infrastructure components.

Administrators should have knowledge of the following third-party products:

- Cisco® Unified Communications Manager (Cisco Unified CM)
- Cisco® Video Communications Server (VCS)
Cisco video and voice endpoints

Frequently Asked Questions

This section answers questions you might have about the solution before you begin.

Is a Telepresence Interoperability Protocol (TIP) license required on the RealPresence Collaboration Server bridge for Cisco environments?

No. TIP capability is built into the Polycom RealPresence Collaboration Server. However, if an immersive telepresence experience is required on, for example, multiscreen Polycom or Cisco endpoints, there is a telepresence license enabling TIP capability on the RealPresence Collaboration Server. Polycom RealPresence Collaboration Server can host immersive as well as nonimmersive video conferences.

Can a Polycom RealPresence solution integrate with a Cisco Video Communications Server (VCS)?

Yes. Refer to Polycom RealPresence Platform Integration with VCS for information on Cisco VCS integration deployments.

Is content sharing supported in a Polycom-Cisco integrated deployment?

Yes. Depending on the components involved, Polycom RealPresence infrastructure and endpoints support content sharing either via methods defined in TIP or via the SIP standards-based Binary Floor Control Protocol (BFCP) over User Datagram Protocol (UDP) feature.

Are audio-only calls also supported on the RealPresence Collaboration Server bridge for Cisco environments?

Yes. For Cisco Unified Communications Manager (Cisco Unified CM) telephony environments, audio-only calls from IP Phones or PSTN callers are supported on the RealPresence Collaboration Server bridge as well as audio-video calls.

What’s New?

In this release, the Polycom Unified Communications for Cisco Environments release adds support for the following:

- Cisco Jabber for Windows

Polycom supports updated versions of Cisco products within the supported architectures. Polycom is committed to updating support for new environments in future releases.

Get Help and Support Resources

For more information about installing, configuring, and administering Polycom products, refer to Documents and Downloads at Polycom Support.
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, 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.
Chapter 2: Polycom Unified Communications with Cisco Interoperability

This chapter provides an overview of the features offered in Cisco environments you can integrate Polycom Unified Communications (UC) products.

The Polycom video infrastructure allows you to integrate with Cisco Unified Communications Manager (Cisco Unified CM) or Cisco Video Communications Server (VCS) infrastructure to enable common dial plans between Polycom and Cisco Unified IP phones or video endpoints.

Supported Deployment Models

Polycom supports the following deployment models when integrating Polycom Unified Communications with Cisco environments.

**Direct Registration of Polycom RealPresence Systems with Cisco Unified CM**

When you SIP register your Polycom telepresence endpoints directly with Cisco Unified CM, you have a single source for call admission control and bandwidth management. Cisco endpoints can also use telephony functions like hold and transfer when on calls with Polycom endpoints.

When you install the TIP option key on Polycom telepresence endpoints, the Polycom endpoints can participate in calls with TIP-capable Cisco CTS endpoints and Cisco Multipoint Control Units (MCUs). Cisco Unified CM can also have direct SIP integration with a Polycom RealPresence Collaboration Server. The RealPresence Collaboration Server system inherently supports hosting TIP conference calls and can be licensed to handle Immersive Telepresence (ITP) multipoint conferences.

**Direct Secure Registration of Polycom RealPresence Systems with Cisco Unified CM**

When you SIP register your Polycom telepresence endpoints directly with Cisco Unified CM using Transport Layer Security (TLS) registration, you have a single source for call admission control and bandwidth management. Cisco endpoints can also use telephony functions like hold and transfer when on calls with Polycom endpoints.

When you install the TIP option key on Polycom telepresence endpoints, the Polycom endpoints can participate in calls with TIP-capable Cisco CTS endpoints and Cisco Multipoint Control


Units (MCUs). Cisco Unified CM can also have direct SIP integration with a Polycom RealPresence Collaboration Server. The RealPresence Collaboration Server system inherently supports hosting TIP conference calls and can be licensed to handle ITP multipoint conferences. Customers with security requirements can now securely implement direct registration with encrypted signaling and a choice of encrypted or unencrypted media communications.

**Polycom RealPresence Platform SIP Integration with Cisco Unified CM**

You can configure the Polycom RealPresence Distributed Media Application (DMA) system as a SIP proxy and registrar for your video environment. When you use the DMA system as a SIP peer to Cisco Unified CM, it can provide a Virtual Meeting Room (VMR) audio and video solution between Cisco endpoints that are registered with Cisco Unified CM and Polycom SIP and H.323 endpoints that are registered with the DMA system. The RealPresence Collaboration Server system inherently supports hosting TIP conference calls and can be licensed to handle ITP multipoint conferences. DMA integration also offers the strongest content sharing capabilities.

**Polycom RealPresence Platform Integration with VCS**

You can configure a Polycom DMA system as a SIP proxy and registrar for your video environment. For migrations or environments that call for integration with VCS, you can integrate Polycom DMA using either the SIP or H.323 protocol to provide bridge virtualization, scale, and redundancy. Polycom RealPresence infrastructure can host video calls between Cisco endpoints that are registered with VCS and Polycom SIP or H.323 endpoints and MCUs that are registered with the DMA system.

**Polycom RealPresence Platform SIP Integration with Cisco CUBE SP Edition**

Customers and service providers that provide protocol interworking, admission control, and security demarcation services using the Cisco Unified Border Element (CUBE) SP Edition feature on a Cisco 1000 series Aggregation Services Router (ASR) can also deploy Polycom RealPresence infrastructure in their environment. CUBE SP Edition enables direct IP-to-IP interconnect between domains, which may be offered by a vendor or service provider.
Chapter 3: Direct Registration of Polycom RealPresence Systems with Cisco Unified CM

The direct registration deployment model takes advantage of Polycom RealPresence systems SIP capabilities to integrate with Cisco Unified Communications Manager (Cisco Unified CM) IP Telephony. This model enables customers to integrate the video and IP Telephony “islands” and provide investment protection as well as freedom of choice to continue deploying Polycom solutions.

Deployment Model Advantages

Registering Polycom RealPresence endpoints with Cisco Unified Communications Manager enables you to integrate Polycom products with a Cisco deployment without additional network management overhead and provides a single source for call admission control. Polycom video endpoints can also take advantage of telephony functions—for example, hold or transfer call functions to another endpoint—when SIP-enabled and registered with Cisco Unified CM.

If your deployment includes a mixture of endpoints, the Polycom HDX, Polycom® Group Series®, and Polycom Immersive Telepresence (ITP) systems are able to make and receive calls with Cisco CTS endpoints. Polycom endpoints can also participate in multipoint calls hosted by either a RealPresence Collaboration Server bridge or a Cisco Telepresence Server.

To allow for flexible deployments and migrations, Polycom endpoints can be simultaneously SIP-registered with Cisco Unified CM and H.323-registered with a Polycom Distributed Media Application (DMA) system. For more information on DMA integrations, see Polycom RealPresence Platform SIP Integration with Cisco Unified CM and Polycom RealPresence Platform Integration with VCS.

Supported Products for Deployment

Verified Polycom Product Versions

<table>
<thead>
<tr>
<th>Polycom Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RealPresence Collaboration Server (RMX)</td>
<td>8.4 - MPMx card required for TIP support</td>
</tr>
<tr>
<td>1500/1800/2000/4000 systems</td>
<td></td>
</tr>
</tbody>
</table>
## Polycom Product

<table>
<thead>
<tr>
<th>Polycom Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Polycom HDX system</strong> (all models)</td>
<td>3.1.3.2</td>
</tr>
<tr>
<td></td>
<td>Requires TIP option key for Cisco Immersive Telepresence calls</td>
</tr>
<tr>
<td><strong>Polycom RealPresence Group Series (300, 500, and 700)</strong></td>
<td>4.1.3.2</td>
</tr>
<tr>
<td></td>
<td>Requires TIP option key for Cisco Immersive Telepresence calls</td>
</tr>
<tr>
<td><strong>Polycom® Touch Control for HDX systems</strong></td>
<td>1.9.0</td>
</tr>
<tr>
<td><strong>Polycom Touch Control for RealPresence Group Series</strong></td>
<td>4.1</td>
</tr>
<tr>
<td><strong>Immersive Solutions including:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Polycom® RealPresence® Experience (RPX™)</strong></td>
<td>3.1.3.2</td>
</tr>
<tr>
<td><strong>Polycom Open Telepresence Experience (OTX)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Polycom® Architected Telepresence Experience™ (ATX™)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Polycom Multipoint Layout Application</strong></td>
<td>3.1.2.8</td>
</tr>
</tbody>
</table>

## Verified Cisco Product Versions

<table>
<thead>
<tr>
<th>Cisco Product</th>
<th>Release(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>9.1.2.11900-12</td>
</tr>
<tr>
<td><strong>Cisco Unified IP Phones: 7960, 7961, 7962, 7965, 7975, 7985, 9971</strong></td>
<td>Cisco Unified CM 9.1 (2) Default Load</td>
</tr>
<tr>
<td>Cisco Jabber for Windows</td>
<td>9.7(0)</td>
</tr>
<tr>
<td>Cisco CTS500-32, TX1310, TX9000</td>
<td>6.1.2.1(5)</td>
</tr>
<tr>
<td>Cisco CTS500-37, CTS1300, CTS3010</td>
<td>1.10.5.1(4)</td>
</tr>
<tr>
<td>EX, C and SX Series</td>
<td>7.1.1</td>
</tr>
<tr>
<td>Cisco Telepresence Video Communications Server</td>
<td>X8.1.1</td>
</tr>
<tr>
<td>Cisco TelePresence Server</td>
<td>4.0(1.57)</td>
</tr>
</tbody>
</table>
Deployment Architecture

The following figure shows the reference architecture for this deployment model.

Architecture when Polycom telepresence endpoints are directly registered to Cisco Unified Communications Manager

Direct Registration of Polycom Telepresence Endpoints to CUCM

Design Considerations

Before you register Polycom RealPresence video endpoints to Cisco Unified Communications Manager, consider the following about interoperability between Cisco Unified CM and Polycom systems.

Cisco Unified Communications Manager Considerations

Make note of the following Cisco Unified CM considerations:

- Location settings should allow for video bandwidth when integrating Polycom video endpoints and infrastructure.
- Region settings should allow for a minimum of 256 K video bandwidth and should match the Polycom HDX system maximum call rate.
- Region settings should allow for a G.722 audio protocol for the best audio experience.
- Add the Polycom HDX system to a device pool in a Media Resource Group List that does not contain Media Transfer Protocol (MTP) resources.
Direct Registration of Polycom RealPresence Systems with Cisco Unified CM

Note: Insertion of Media Termination Point resources

Due to the nature of out-of-band DTMF signaling, Cisco Unified Communications Manager is capable of inserting Media Termination Point (MTP) resources in a call. This prevents video on the Polycom HDX Termination Point (MTP) resources from operating correctly. This is most common on H.323 and SIP trunk calls. To prevent this from occurring, the MTP resources should be removed from any Media Resource Groups and Media Resource Group lists used in the trunked calls.

- Since Cisco Unified CM is a SIP back-to-back user agent (B2BUA), it is involved in all signaling between two endpoints making a call. Because Cisco Unified CM strips out and does not allow audio or video codecs that it does not support, some advanced Polycom codecs such as Siren Lost Packet Recovery (LPR) audio or H.264 High Profile video are not negotiated—even between two Polycom endpoints if they are directly registered with Cisco Unified CM.

Polycom Immersive Telepresence Systems Considerations

Telepresence Interoperability Protocol (TIP) enables multiscreen or multicamera video systems to provide proper video alignment and spatial audio capabilities with other multiscreen or multicamera endpoints. For multiscreen immersive system connectivity, consider the following:

- The TIP option key is required in order to support TIP calls. Polycom telepresence endpoints support TIP version 7.
- If you have a Polycom ITP system, the TIP license is included; however, ensure that the TIP option key is installed on each codec within the ITP system.
- Each codec in a Polycom ITP system must be registered with Cisco Unified CM.
- You must predefine Polycom ITP endpoints on the Cisco TelePresence Server to allow them to participate in calls hosted by the Cisco TelePresence Server.

Share Content in Telepresence Environments

Within a Cisco telepresence environment, Polycom and Cisco endpoints can share content in a separate content channel. In point-to-point calls between Polycom endpoints registered to Cisco Unified CM, you can send and receive content only in the video (people) channel, including Polycom endpoints connecting to RealPresence Collaboration Server bridge calls. The reason is that, by default, TIP is not negotiated for a call between Polycom devices.

However, in HDX version 3.1.1, a new telnet command has been added (alwaysusetip) which, when set, prefers TIP connectivity when possible. Additionally, RealPresence Collaboration Server version 8.1.1 added a new conference profile TIP Compatibility option (Prefer TIP) which forces the RealPresence Collaboration Server to prefer TIP with Polycom endpoints. When Polycom devices are configured to prefer TIP, you can share content in a separate content channel with other TIP-capable endpoints. For more information, see Configure the HDX to Prefer TIP (Optional).
Enabling “force TIP” allows Polycom endpoints to fully share content on a separate content channel for full collaboration with TIP-enabled endpoints.

The following guidelines apply:

- Content sharing within a Polycom-Cisco environment is limited to extended graphics array (XGA) at 5 frames per second (FPS).
- Content sharing on Polycom ITP or HDX systems is only supported via VGA cable. USB content sharing is not supported.
- The Polycom® People + Content™ IP tool is not supported in Cisco telepresence environments.

License Devices

Device license units are assigned to each device connected to Cisco Unified Communications Manager. Each device is assigned a unit number based on the type and capabilities of the device. Devices with more complex and high-end capabilities are assigned a higher number of units than devices with basic capabilities. The following table shows the license units for Polycom devices. For more information, see your Cisco documentation.

<table>
<thead>
<tr>
<th>Polycom Device</th>
<th>Required Device License Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom HDX or Group Series System</td>
<td>One enhanced user license</td>
</tr>
<tr>
<td>Polycom ITP system</td>
<td>One enhanced user license per screen</td>
</tr>
</tbody>
</table>

Register a Polycom RealPresence Immersive, Room, or Desktop System with Cisco Unified CM

To register the Polycom RealPresence system with Cisco Unified CM, you need to perform steps in both the Cisco Unified CM and the Polycom RealPresence system.

For more information about the Cisco Unified Communications Manager, see the Cisco Unified Communications Manager Documentation Guide. For more information about Polycom HDX systems, see HDX Series on Polycom Support. For more information on Polycom Group series, see Group Series on Polycom Support.

Complete the following major steps:

- Configure Cisco Unified CM for a Polycom Immersive, Room, or Desktop System
- Configure a Polycom Group Series System for Cisco Unified CM Registration
- Configure a Polycom HDX or Immersive System for Cisco Unified CM Registration
Direct Registration of Polycom RealPresence Systems with Cisco Unified CM

- Define your Polycom Immersive System in the Cisco TelePresence Server (Optional)

Configure Cisco Unified CM for a Polycom Immersive, Room, or Desktop System

Before performing the tasks in the following section, review the Cisco Unified Communications Manager Considerations.

Create a Security Profile

You need to create a phone security profile for your Polycom systems. If you want to create a secure profile, you can choose to enable digest authentication to secure the Polycom endpoint system’s connection to Cisco Unified CM.

Note: Recommendation for digest authentication

Polycom recommends using digest authentication for Polycom endpoint registration.

You need to create a security profile for your Polycom HDX, Group Series, or ITP system. Because each endpoint uses the same security profile, you need to create only one security profile.

To configure security profiles:

1. Log into the Cisco Unified CM console.
2. Select System > Security Profile > Phone Security Profile.
3. Select Add New.
4. Select a Phone Security Profile Type. Select Third-party SIP Device (Advanced) and click Next.

![Phone Security Profile Configuration](image)
5 On the **Phone Security Profile Information** page, complete the following fields:
   
   a In the **Name** field, enter a profile name for the system.
   
   b In the **Description** field, enter a description for the security profile.
   
   c If you want to use digest authentication (recommended), select the **Enable Digest Authentication** check box. When you use digest authentication, a valid login password is required for devices to register.
   
   d Select the default values for all other fields. This example uses digest authentication.

![Phone Security Profile Configuration]

6 Click **Save**.

In the status bar near the top of the page, **Update Successful** displays.

**Add a System User**

You need to create a Cisco Unified CM system user for each Polycom HDX or Group Series endpoint. For ITP systems, create a system user for each codec. For example, if you are registering a Polycom OTX system that has three codecs, create a unique system user for each codec.

If you cannot add a user here, your system may be LDAP integrated. You can use an existing user ID (essentially associating the endpoint to an existing user) or have your LDAP administrator create a new user ID for each codec.

**To add a system user:**

1 Select **User Management > End User**.
2 Click Add New.

The End User Configuration screen displays.

3 Complete the required fields. User ID and Last name are the minimum required fields. The End User Password and PIN fields are arbitrary and are not used for registration.

   a To use digest authentication, enter the Digest Credentials (password) for the Polycom system.
   
   b In the Confirm Digest Credentials text box, enter the same value that you entered in step 3a.

4 Click Save.

   In the status bar near the top of the page, an Update Successful message displays.

Create a SIP Profile

Cisco Unified CM associates specific SIP parameters with an endpoint or trunk via a SIP Profile. In this task, you create a SIP profile in Cisco Unified CM that can be associated with Polycom system devices.
To create a SIP Profile:

1. Select Device > Device Settings > SIP Profile.

2. Click Find to see the list of existing SIP Profiles, and select the Standard SIP Profile (a default in Cisco Unified CM).

3. Once open, click Copy.

   Most of the SIP settings are likely at default. Consult a Cisco Unified CM administrator for information about SIP settings that may be specific to your deployment.

4. Change the Name field to something meaningful for your deployment, and configure the following.

   a. Select the Use Fully Qualified Domain Name in SIP Requests check box.

   b. Select the Allow Presentation Sharing using BFCP check box.

   c. Do NOT select the Early Offer support for voice and video calls check box.

The data shown in the following is an example.
### Direct Registration of Polycom RealPresence Systems with Cisco Unified CM

#### Parameters used in Phone

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer Invite Expires (seconds)</td>
<td>180</td>
</tr>
<tr>
<td>Timer Register Delta (seconds)</td>
<td>5</td>
</tr>
<tr>
<td>Timer Register Expires (seconds)</td>
<td>2600</td>
</tr>
<tr>
<td>Timer T1 (msec)</td>
<td>500</td>
</tr>
<tr>
<td>Timer T2 (msec)</td>
<td>4000</td>
</tr>
<tr>
<td>Retry INVITE</td>
<td>4</td>
</tr>
<tr>
<td>Retry Non-INVITE</td>
<td>10</td>
</tr>
<tr>
<td>Start Media Port</td>
<td>10384</td>
</tr>
<tr>
<td>Stop Media Port</td>
<td>32766</td>
</tr>
<tr>
<td>Call Pickup URI</td>
<td>x-cisco-serviceuri-pickup</td>
</tr>
<tr>
<td>Call Pickup Group Other URI</td>
<td>x-cisco-serviceuri-pickup</td>
</tr>
<tr>
<td>Call Pickup Group URI</td>
<td>x-cisco-serviceuri-pickup</td>
</tr>
<tr>
<td>Meet Me Service URI</td>
<td>x-cisco-serviceuri-meetme</td>
</tr>
<tr>
<td>DTMF DB Level</td>
<td>None</td>
</tr>
<tr>
<td>Call Hold Ring Back</td>
<td>Off</td>
</tr>
<tr>
<td>Anonymous Call Block</td>
<td>Off</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>Off</td>
</tr>
<tr>
<td>Do Not Disturb Control</td>
<td>Off</td>
</tr>
<tr>
<td>Tollrate Level for 7940 and 7980</td>
<td>Off</td>
</tr>
<tr>
<td>Timer Keep Alive Expires (seconds)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Timer Subscribe Expire (seconds)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Timer Subscribe Delta (seconds)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Maximum Redirections</td>
<td>Disabled</td>
</tr>
<tr>
<td>Off Hook To First Digit Timer (milliseconds)</td>
<td>120</td>
</tr>
<tr>
<td>Call Forward URI</td>
<td>120</td>
</tr>
<tr>
<td>Speed Dial (Abbreviated Dial) URI</td>
<td>70</td>
</tr>
<tr>
<td>RFC 2543 Hold</td>
<td>x-cisco-serviceuri-rfc2543</td>
</tr>
<tr>
<td>Semi Attended Transfer</td>
<td>x-cisco-serviceuri-meetme</td>
</tr>
<tr>
<td>Enable VAD</td>
<td>x-cisco-serviceuri-abbreviated</td>
</tr>
</tbody>
</table>

#### Trunk Specific Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reroute Incoming Request to new Trunk based on</td>
<td>Never</td>
</tr>
<tr>
<td>RSVP Over SIP</td>
<td>Local RSVP</td>
</tr>
<tr>
<td>Resource Priority Namespace List</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>Fall back to local RSVP</td>
<td></td>
</tr>
<tr>
<td>SIP ReLXX Options</td>
<td>Disabled</td>
</tr>
<tr>
<td>Video Call Traffic Class</td>
<td>Mixed</td>
</tr>
<tr>
<td>Calling Line Identification Presentation</td>
<td>Default</td>
</tr>
<tr>
<td>Deliver Conference Bridge Identifier</td>
<td></td>
</tr>
<tr>
<td>Early Offer support for voice and video calls</td>
<td></td>
</tr>
<tr>
<td>Send send-receive SDP in mid-call INVITE</td>
<td></td>
</tr>
<tr>
<td>Allow Presentation Sharing using BFCP</td>
<td></td>
</tr>
<tr>
<td>Allow IX Application Media</td>
<td></td>
</tr>
<tr>
<td>Allow Passthrough of Configured Line Device</td>
<td></td>
</tr>
<tr>
<td>Reject Anonymous Incoming Calls</td>
<td></td>
</tr>
<tr>
<td>Reject Anonymous Outgoing Calls</td>
<td></td>
</tr>
</tbody>
</table>

#### SIP OPTIONS Ping

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable OPTIONS Ping to monitor destination</td>
<td>None (Default)</td>
</tr>
<tr>
<td>status for Trunks with Service Type</td>
<td></td>
</tr>
<tr>
<td>Ping Interval for In-service and Partially</td>
<td>60</td>
</tr>
<tr>
<td>Ping Interval for Out-of-service Trunks</td>
<td>120</td>
</tr>
<tr>
<td>Ping Retry Timer (milliseconds)</td>
<td>500</td>
</tr>
<tr>
<td>Ping Retry Count</td>
<td>6</td>
</tr>
</tbody>
</table>
5 Click Save.

In the status bar near the top of the page, an Update Successful message displays.

Add a Device Entry

You need to create a Cisco Unified CM device entry for each endpoint system or each codec for a Polycom ITP system. For example, if you are registering a Polycom OTX system that has three codecs, you need to create a unique device entry for each codec.

This step adds a device to Cisco Unified CM, which in turn allows the device to register properly with Cisco Unified CM.

To add a device entry:

1 Select Device > Phone.
2 Click Add New.
3 Select Third-party SIP Device (Advanced), and click Next.
The following screen displays. The data shown in this section is an example.

4 Complete the required and optional information:

a In the **MAC Address** text box, enter a unique MAC Address for the HDX system. This can be any valid, unique MAC address. Cisco Unified CM uses the HDX user name to identify the HDX system. This field is arbitrary for third-party SIP Devices in Cisco Unified CM. Polycom recommends configuring the actual MAC address of the HDX system to avoid conflicts.

b (Optional) In the **Description** text box, enter a description.

c From the **Device Pool** list, select the device pool appropriate for your Cisco Unified Communications Manager system video devices.

d From the **Phone Button Template** list, select **Third-party SIP Device (Advanced)**.
e (Optional) If your Cisco Unified CM implementation uses partitions and call search spaces, from the **Calling Search Space** list, select an appropriate calling search space for the HDX system.

f If your Cisco Unified CM implementation uses the Cisco Unified CM locations-based Call Admission Control (CAC), select an appropriate location for the HDX system from the **Location** list. This location should contain video bandwidth.

Before making this selection, see **Design Considerations** and **Cisco Unified Communications Manager Considerations**.

5 Scroll to the **Protocol Specific Information** section.

<table>
<thead>
<tr>
<th>Protocol Specific Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLF Presence Group</td>
</tr>
<tr>
<td>MTP Preferred Originating Codec</td>
</tr>
<tr>
<td>Device Security Profile</td>
</tr>
<tr>
<td>Remotecalling Search Space</td>
</tr>
<tr>
<td>SUBSCRIBE Calling Search Space</td>
</tr>
<tr>
<td>SIP Profile</td>
</tr>
<tr>
<td>Digest User</td>
</tr>
<tr>
<td>Media Termination Point Required</td>
</tr>
<tr>
<td>Unattended Port</td>
</tr>
<tr>
<td>Require DTMF Reception</td>
</tr>
<tr>
<td>Allow Presentation Sharing using BFCP</td>
</tr>
<tr>
<td>Allow IX Applicable Media</td>
</tr>
</tbody>
</table>

5a From the **Device Security Profile** list, select the profile created in **Create a Security Profile**.

5b In the **Digest User** field, select the user created in **Add a System User**.

5c From the **SIP Profile** list, select the profile created in **Create a SIP Profile**.

5d Select the **Allow Presentation Sharing using BFCP** check box.

6 Click **Save**.

In the status bar near the top of the page, an **Update Successful** message displays and the **Association Information** section displays.

7 In the **Association Information** section, click **Line [1] - Add a new DN**.
Direct Registration of Polycom RealPresence Systems with Cisco Unified CM

8 Complete the following required fields:
   a In the Directory Number field, enter the phone’s extension number.
   b In the Route Partition field, choose the appropriate value for your Cisco Unified CM deployment.

9 Click Save.
   In the status bar near the top of the page, an Update Successful message displays.

10 Reset the Polycom system in Cisco Unified CM.

Configure a Polycom Group Series System for Cisco Unified CM Registration

Use the Polycom Group Series web administration interface to perform the following configurations.

Configure SIP Settings

You need to first configure the SIP settings for the Polycom Group Series endpoint.

To configure the SIP settings:

1 Open a browser window, and enter the Polycom Group Series system IP address or host name in the Address field.
2 Navigate to Admin Settings > Network > IP Network and select SIP.
Configure the settings in the SIP Settings section of the IP Network screen as shown in the following table.

### SIP Settings Fields and Their Descriptions

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Check this box to enable the HDX system to receive and make SIP calls.</td>
</tr>
<tr>
<td>SIP Server Configuration</td>
<td>Set this to Specify so a registrar and proxy server can be configured.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Specify the protocol used for SIP signaling. For Cisco Unified CM, select either Auto or TCP.</td>
</tr>
<tr>
<td>Sign-in Address</td>
<td>Enter the sign-in address used as the endpoint’s SIP URI. Set this to the directory number you assigned to the HDX system in Cisco Unified CM. This example is configured with a Directory Number of 2227.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specify the user name used to login. Set this to the directory number you assigned to the HDX system in Cisco Unified CM.</td>
</tr>
<tr>
<td>Password</td>
<td>Check this box to display two additional fields and enter the password. Use the digest credentials configured in To Add a System User.</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>Specify the IP address of the Cisco Unified CM Call processing subscriber you need to register to.</td>
</tr>
</tbody>
</table>
Direct Registration of Polycom RealPresence Systems with Cisco Unified CM

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server</td>
<td>If you leave this field blank, the registrar server is used. The recommended value is the IP address of the Cisco Unified CM call processing subscriber you need to register to.</td>
</tr>
<tr>
<td>Registrar Server Type</td>
<td>Specifies the type of registrar server. For Cisco Unified CM, set this to Unknown.</td>
</tr>
</tbody>
</table>

4 Click **Save**.
Your Polycom endpoint is now registered with Cisco Unified CM.

**Ensure the TIP Protocol is Enabled (Optional)**
If your Polycom endpoint needs to participate in TIP-based calls, verify that the TIP license is enabled for your endpoint.

**To verify that the TIP protocol is enabled:**

1 Open a browser window, and enter the Polycom Group Series system IP address or host name in the **Address** field.

2 Navigate to **Admin Settings > General Settings > Options**.

3 Verify that the TIP license option is included on your system.

![Image of Polycom System Settings](image)

If the TIP option is not available, contact your Polycom Sales Representative as this option must be purchased.

**Configure a Polycom HDX or Immersive System for Cisco Unified CM Registration**

When a Polycom endpoint is registered with a Cisco Unified CM, the endpoint can make calls to Cisco endpoints that are also registered to the Cisco Unified CM. Use the HDX web administrator interface to configure the following settings.
Configure SIP Settings

Configure the following SIP settings to register a Polycom HDX or ITP system with Cisco Unified CM.

To configure SIP settings:

1. Open a browser window, and enter the Polycom HDX system IP address or host name in the **Address** field.
2. Navigate to **Admin Settings > Network > IP Network** and select **SIP**.

3. Configure the settings in the **SIP Settings** section of the **IP Network** screen as shown in the following table.

### SIP Settings Fields and Descriptions

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Check this to enable the HDX system to receive and make SIP calls.</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>Specify the IP address of the Cisco Unified Communications Manager. If you leave this field blank, the value in Proxy Server is used.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Specify the IP address of the SIP Proxy Server. If you leave this field blank, the value in Registrar Server is used. If you leave both fields blank, no proxy server is used. Note that if you set Transport Protocol to TCP, the SIP signaling is sent to port 5060 on the proxy server. The syntax used for this field is the same used for the SIP Registrar Server field.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>The SIP network infrastructure that your Polycom HDX system is operating determines which protocol is required. For Cisco environments, select either Auto or TCP.</td>
</tr>
</tbody>
</table>
### Direct Registration of Polycom RealPresence Systems with Cisco Unified CM

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Specify the system’s SIP name. This is the SIP URI. Set this to the directory number you assigned to the HDX system.</td>
</tr>
<tr>
<td>Domain User Name</td>
<td>For Cisco environments, leave this field blank.</td>
</tr>
<tr>
<td>Password</td>
<td>When this field is enabled, you can specify and confirm a new password that authenticates the system to the SIP Registrar Server. If using digest authentication, select the Password check box and set the password to the digest credentials password you set for the Cisco Unified Communications user you created for this HDX system.</td>
</tr>
<tr>
<td>Directory: Microsoft Lync Server</td>
<td>Specifies whether the SIP Registrar Server is a Lync Server. For Cisco environments, leave this check box unselected.</td>
</tr>
</tbody>
</table>

### Ensure the TIP Protocol is Enabled (Optional)

If your Polycom endpoint needs to participate in TIP-based calls, ensure that the TIP license has been applied to your endpoint.

**To ensure the TIP protocol is enabled:**

1. Open a browser window, and enter the Polycom Group Series system IP address or host name in the **Address** field.
2. Navigate to **Admin Settings > General Settings > Options**.
3. Verify that the TIP license option is included on your system.
4 Navigate to **Admin Settings > Call Preference**. The following screen displays.

![Call Preference Screen](image)

5 Verify that TIP is enabled as a Call Preference and that the preferred and maximum call speeds for SIP (TIP) calls are at least 1024 kilobits per second (Kbps) or greater.

**Configure the HDX to Prefer TIP (Optional)**

To ensure the HDX is able to share content in a separate content channel in TIP-based calls with other Polycom endpoints or a Polycom RealPresence Collaboration Server, the HDX should be configured to prefer TIP.

**To ensure the TIP protocol is enabled:**

1 Telnet to the IP Address of the HDX using port 24.
2 If prompted, enter credentials for access.
3 Issue the command `alwaysusetip get`. The HDX returns the current status of this command.
4 Issue the command `alwaysusetip yes` to force the HDX to prefer TIP when communicating with other Polycom devices.
5 Issue the command `alwaysusetip get` to ensure the setting has changed.

**Note: Configuration change remains after reboot**

This configuration change remains even after the HDX reboots.
Define your Polycom Immersive System in the Cisco TelePresence Server (Optional)

If your Cisco environment includes a Cisco TelePresence Server as well as Polycom ITP endpoints, you need to predefine your Polycom ITP endpoints on the Cisco TelePresence Server to enable them to participate in calls hosted by Cisco TelePresence Server.

You need to define the Primary codec of your Polycom ITP system as a Legacy CTS endpoint.

To define your Polycom ITP endpoint:

1. Log onto the Cisco TelePresence Server.
2. Select **Endpoints > Add legacy Cisco CTS endpoint**.
3. In the **Add legacy Cisco CTS endpoint** dialog, complete the following fields:
   a. In the **Name** field, enter a name for your Polycom ITP system.
   b. In the **Address** field, enter the directory number you created for the primary codec of your Polycom ITP system.
4. Click **Add legacy Cisco CTS endpoint**.

Configure SIP Integration Between a Polycom RealPresence Collaboration Server System and Cisco Unified CM

You can configure Cisco Unified CM to route audio and video calls directly to a Polycom RealPresence Collaboration Server. To enable this integration, you need to perform steps in both the Cisco Unified CM and the Polycom RealPresence Collaboration Server system.

For more information about the Cisco Unified Communications Manager, see the [Cisco Unified Communications Manager Documentation Guide](#). For more information see [Collaboration and Conferencing Platforms](#) on Polycom Support.
Configure Cisco Unified CM for SIP Integration with RealPresence Collaboration Server

Perform the following tasks to create a SIP trunk in Cisco Unified CM to the RealPresence Collaboration Server system and establish the call routing infrastructure.

Create a SIP Profile
For instructions, see Create a SIP Profile.

Add a SIP Trunk
This task shows you how to add a SIP trunk in Cisco Unified CM.

To add a SIP trunk:

1. Navigate to Device > Trunk.
2. Click Add New in the upper left.
   a. For Trunk Type, select SIP Trunk.
   b. For Device Protocol, the default is SIP and cannot be changed.
   c. For Trunk Service Type, select None (Default).
3. Click Next.
4. Enter a Device Name for this trunk, and a description. The Device Name is arbitrary and should be a name meaningful for your deployment.
5. Fill out fields as appropriate for your deployment, and enter the following required values:
   a. For Call Classification, select OnNet.
   b. If your Cisco Unified CM implementation uses the Cisco Unified CM locations-based Call Admission Control (CAC), select an appropriate location for the Polycom system.
from the **Location** list. This location should contain appropriate video bandwidth for connectivity to the RealPresence Collaboration Server.

c Confirm that the **Media Termination Point Required** check box is NOT selected. The following is shown as an example.

d If your Cisco Unified CM implementation uses partitions and call search spaces, under **Inbound Calls** settings, select an appropriate calling search space for the Polycom system from the **Calling Search Space** list. This field affects *inbound* calls on this SIP trunk.

e In the **SIP Information** section, fill in the **Destination Address** with the RealPresence Collaboration Server signaling IP address.

f Select the Cisco Unified CM default **Non Secure SIP Trunk Profile**. Be sure to select a **SIP Profile** that allows BFCP.
g Select the SIP Profile created in Create a SIP Profile.
The following is shown as an example.

6 Click Save.
7 Click Apply Config to apply your changes.

Add a Route Pattern
In this task, you create a route pattern which defines a specific dial pattern or patterns that should be sent to the RealPresence Collaboration Server SIP trunk created in the previous section. Video calls are an automatic negotiation as part of the call setup.

To add a route pattern:

1 Navigate to Call Routing > Route/Hunt > Route Pattern.
2 Click Add New.
3 Add a route pattern representing a single E.164 conference extension or range of extensions available on the RealPresence Collaboration Server system.
   a In the Route Pattern field, enter a name for the pattern. This example uses 3XXX.
   b From the Gateway/Route List dropdown, select the SIP Trunk you created in Add a SIP Trunk.

Note: Using the route groups and route lists with RealPresence Collaboration Server
If your Cisco Unified CM implementation uses the route group, route list construct, it is also possible to add the RealPresence Collaboration Server SIP trunk to that construct. Associating the SIP trunk directly to a route pattern is shown here for simplicity.
c Enter all other information for your network, such as Route Partition or Calling Party Transformations if any digit manipulation is required.

d In the Call Classification field, select OnNet. The Provide Outside Dial Tone check box is typically NOT selected.

4 Click Save.

Note: Using route groups and route lists

If a route pattern is pointed directly at a trunk, any subsequent route patterns that you add are resets and ALL calls on the trunk are dropped. The use of route groups and route lists allows calls to stay active while adding route patterns and is highly recommended.

Once you complete the above steps, any Cisco endpoint with the correct call permissions registered to your Cisco Unified CM should now be able to initiate calls to the RealPresence Collaboration Server.

Configure the RealPresence Collaboration Server for Cisco Unified CM SIP calls

The following tasks are required to prepare the RealPresence Collaboration Server to receive and initiate SIP calls with Cisco Unified CM.
Enable the RealPresence Collaboration Server for SIP

The following steps enable the SIP protocol on the RealPresence Collaboration Server.

To enable SIP on the Polycom RealPresence Collaboration Server:

1. From the RealPresence Collaboration Server management interface, click the IP tab in the IP Network Services Properties dialog.
2. Confirm that the IP Network Type dropdown is set to SIP or H.323 & SIP.
3. Click OK.

At this point, the RealPresence Collaboration Server is capable of receiving SIP calls from Cisco Unified CM. However, take care to ensure the proper experience for conference attendees. Attending users may dial directly into a preconfigured meeting room conference ID or alternatively dial into an entry queue which prompts users to enter a conference ID. One entry queue in the system is designated as the transit entry queue that receives calls with dial strings containing incomplete or incorrect conference routing information. Furthermore, RealPresence Collaboration Server allows for configuration of an ad hoc entry queue that enables users to create meetings on the fly from the entry queue prompts.

For more information, see the “Meeting Rooms” and “Entry Queues, Ad Hoc Conferences and SIP Factories” sections in the Polycom RealPresence Collaboration Server (RMX) Administrator’s Guide.

Configure RealPresence Collaboration Server to Route Outbound SIP Calls to Cisco Unified CM (Optional)

If your deployment requires the RealPresence Collaboration Server to out-dial endpoints registered to Cisco Unified CM, configure the following steps on the RealPresence Collaboration Server.

To configure RealPresence Collaboration Server to route outbound SIP calls to Cisco Unified CM:

1. From the RealPresence Collaboration Server management interface, in the IP Network Services Properties dialog.
2. Click the SIP Servers tab and configure the following settings:
   a. In the SIP Server field, select Specify.
   b. In the SIP Server Type field, select Generic.
   c. Select Refresh Registration every 3600 seconds.
d  If not selected by default, change the Transport Type to TCP.

3  In the SIP Servers table, do the following:
   a  Enter the IP address of the primary call-processing Cisco Unified CM node in both the Server IP Address or Name and Server Domain Name fields.
   b  Ensure the Port field is set to its default value: 5060. Cisco Unified CM uses this port number by default.

4  In the Outbound Proxy Servers table, do the following:
   a  Enter the IP address in the Server IP Address or Name field. This is the same value entered in Step 3a.
   b  Ensure the Port field is set to its default value: 5060. (By default, the value in Outbound Proxy Servers is the same as in SIP Server.)

5  Ensure the IP network service configured in this task is assigned to any meeting rooms that require SIP out-dial to Cisco Unified CM. You can do this via the Default SIP Service designation or by directly configuring the meeting room.

For more information, see “Creating a New Meeting Room” in the Polycom RealPresence Collaboration Server (RMX) Administrator’s Guide.
Direct Registration of Polycom RealPresence Systems with Cisco Unified CM

Prepare the RealPresence Collaboration Server to Support TIP Calls (Optional)

If your environment includes Cisco TelePresence endpoints, you can configure the Polycom RealPresence Collaboration Server to support immersive telepresence calls that uses the TIP protocol. The following tasks prepare the RealPresence Collaboration Server for multiscreen ITP calls.

Confirm the RealPresence Collaboration Server Telepresence Mode License

To host ITP calls on the RealPresence Collaboration Server, a telepresence license must be applied to the system.

To confirm the telepresence licence on RealPresence Collaboration Server:

1. From the RealPresence Collaboration Server manager interface, go to Administration > System Information.

2. Confirm that Telepresence Mode is True, as shown next.
For detailed instructions on setting up your RealPresence Collaboration Server system for
telepresence conferencing, see the Polycom RealPresence Collaboration Server (RMX)
Administrator’s Guide.

Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag
The MIN_TIP_COMPATIBILITY_LINE_RATE system flag determines the minimum line rate at
which an entry queue or meeting room can be TIP enabled.

Polycom systems support TIP version 7, which requires a minimum line rate of 1024 Kbps and
rejects calls at lower line rates. The system flag must be set to 1024 Kbps or higher.

For more information, see “Modifying System Flags” in the Polycom RealPresence

Configure a TIP-Enabled Conference Profile
When you need to support TIP calls, you must ensure that there are conference profiles for the
RealPresence Collaboration Server meeting rooms that are enabled for TIP support. Note that
different profiles can be assigned to different meeting rooms only if they are TIP enabled.

When you enable TIP, content sharing capabilities are affected for TIP calls. See Share Content
in Telepresence Environments.

To configure a TIP-enabled profile:

1. Create a new conference profile for the meeting room or revise an existing profile. For
   more information, see “Defining Profiles” in the Polycom RealPresence Collaboration
   Server (RMX) Administrator’s Guide.

2. Click the General tab.
   a. Set the Line Rate to a value of at least that specified for the
      MIN_TIP_COMPATIBILITY_LINE_RATE system flag. This must be set to 1024 Kbps or
      higher for TIP calls.
   b. Set the Conferencing Mode to AVC only.

3. Click the Advanced tab.
   a. Select a TIP Compatibility mode of Video Only, Video & Content, or Prefer TIP. The
      TIP compatibility mode affects the user video and content experience.
A conference configured with a TIP compatibility of **Video Only** allows for audio and video connectivity using TIP signaling. TIP content is not part of the conference.

A conference configured with a TIP compatibility of **Video and Content** allows for separate audio, video, and content channels using TIP signaling.

A conference configured with a TIP compatibility of **Prefer TIP** is similar to **Video and Content**, but also allows Polycom endpoints that connect to the RealPresence Collaboration Server to negotiate the TIP protocol. Additionally, **Prefer TIP** allows all content formats to be exchanged in a call—for example H.239, Binary Floor Control Protocol (BFCP), and TIP—and is the preferred setting for all rooms requiring TIP. This setting is available in RealPresence Collaboration Server version 8.1.1 and later.

4 Click the **Video Quality** tab.

   a Set the **Maximum Resolution** to **Auto** or at least **HD 720**.

   b The **Content Settings** drop-down menu is disabled if **TIP Compatibility** is set to **Video and Content** in the **Advanced** tab.

5 Click the **Video Settings** tab.

   a Set the **Telepresence Mode** to **Auto** or **On**.

   b Set the **Telepresence Layout Mode** to the layout desired.
» Set to **Room Switch** for the most immersive experience with other multi-screen systems. Conference attendees see the multi-screen endpoint with the current active speaker for the conference.

» Set to **Continuous Presence** for meetings in which all or a subset of participants should be visible for the conference.

The **Send Content to Legacy Endpoints** configuration checkbox is disabled if the **TIP Compatibility Mode** was set to **Video and Content**.

Note that when **TIP Compatibility Mode** is set to **Prefer TIP**, the **Send Content to Legacy Endpoints** field becomes editable.

6 Assign this conference profile to a meeting room that you use for TIP telepresence conferences with Cisco CTS endpoints.

**Enable a Meeting Room for TIP Conferences**

Meeting rooms that are intended for immersive telepresence calls involving TIP must be configured with a TIP enabled conference profile.

**To enable meeting rooms:**

1 Under the **RealPresence Collaboration Server Management** menu, select **Meeting Rooms** and create a new meeting room or revise an existing one.

2 Under the **General** tab, ensure that the **Profile** dropdown associates a conference profile that has been TIP enabled as in **Configure a TIP-Enabled Conference Profile**.

For more information, see “Creating a New Meeting Room” in the *Polycom RealPresence Collaboration Server (RMX) Administrator’s Guide*. 
Configure Participant Properties for Dial Out Calls (Optional)

From the RealPresence Collaboration Server interface, you can create a conference and add participants. You can save participants to the RealPresence Collaboration Server address book for reuse at a later time. Participant properties should inherit their TIP settings from the conference profile you assigned to the conference. The following steps outline the process to add a participant for out-dial purposes.

To configure participant properties:

1. Under the Conferences menu, select New Conference, or select an existing active conference.
2. On the Participants tab, select New.
   a. Create a name.
   b. Set the Type field to SIP.
   c. Leave the IP Address field at default.
   d. Set the SIP Address in the format <Cisco Unified CM Directory Number>@<IP Address of Cisco Unified CM>. Set the Type field to SIP URI.

In the following example, 2103 is the directory number or extension for the Cisco Unified CM endpoint, and 1.1.1.1 is the IP address of the primary call processing Cisco Unified CM node.
Key:

- **Optionally click Add to Address Book** to make this a permanent entry, or click **OK**.

### Configure Polycom MLA for RealPresence Collaboration Server TIP Conferences

For telepresence mode conferences with CTS and Polycom ITP devices to provide the proper immersive experience, the Polycom Multipoint Layout Application (MLA) must be associated with the RealPresence Collaboration Server. Polycom recommends setting MLA to automatic layout for telepresence mode conferences. The following steps highlight the configuration after adding the RealPresence Collaboration Server to the MLA interface.

For more information on MLA deployment and configuration, see the latest *Polycom MLA User's Guide*. 
To configure Polycom MLA for RealPresence Collaboration Server TIP conferences:

1. From the main MLA window, select Preferences.

2. Under the Connections category, ensure that Automatic Layout Active checkbox is selected for the RealPresence Collaboration Server in your deployment.

You can also create custom templates and manually configure layouts. For more information on MLA templates and layouts, see the latest MLA User Guide.

Operations During Ongoing Conferences

You cannot move participants between TIP enabled meetings and non-TIP enabled meetings.
To display participants properties:

1. In the Participant List pane, double-click the participant entry. The Participant Properties - General dialog opens.

2. Click the SDP tab. The following are indicated in the Remote Capabilities, Remote Communication Mode and Local Communication Mode panes:
   - AAC_LD
   - Audio Protocol
   - Main Profile
   - Video protocol

Troubleshoot

This section provides assistance troubleshooting issues you might have with direct registration of Polycom RealPresence systems with Cisco Unified CM.

No video in calls between a Cisco endpoint and a Polycom endpoint

Possible Cause: Cisco Unified CM regions settings do not allow for video.

Workaround: Check Cisco Unified CM regions settings. Determine the device pool associated with each endpoint and the corresponding region assigned to the respective device pools. Once you know the regions, check the region relationships in the Cisco Unified CM region settings to confirm the maximum video call bit rate is set properly.

Cisco CTS endpoints cannot connect to the RealPresence Collaboration Server

Possible Cause: The Cisco Unified CM SIP trunk to the RealPresence Collaboration Server is configured as OffNet.

Workaround: Check Cisco Unified CM trunk settings.

In the Cisco Unified CM SIP trunk settings, confirm the Call Classification setting for the trunk is set to OnNet. Cisco CTS endpoints do not connect to endpoints classified as OffNet.

Polycom endpoints do not register to Cisco Unified CM

Possible Cause: The assigned directory number is already in use on another device.

Workaround: Check the directory number and assign a new extension if it is shared with another device.

Ensure the directory number assigned to the third-party advanced SIP endpoint added to Cisco Unified CM is not shared with any other devices. If partitions are included in your Cisco Unified CM deployment, ensure the directory number is unique within its partition.
Cisco endpoint shows “No bandwidth available” and does not connect to a Polycom endpoint

Possible Cause: Cisco Unified CM locations-based Call Admission Control (CAC) does not have proper video bandwidth allocated.

Workaround: Allocate a proper amount of video bandwidth.

If the two devices are configured for different locations within Cisco Unified CM, confirm that there is adequate video bandwidth to allow for the call under the Locations settings.
Chapter 4: Direct Secure Registration of Polycom RealPresence Systems with Cisco Unified CM

The direct secure registration deployment model takes advantage of Polycom RealPresence systems SIP capabilities to integrate with Cisco Unified Communications Manager (Cisco Unified CM) IP Telephony using Transport Layer Security (TLS) registration. This enables customers to integrate the video and IP telephony “islands” they have deployed, providing investment protection as well as freedom of choice to continue to deploy Polycom solutions. Customers with security requirements may now implement direct registration securely with encrypted signaling and a choice of encrypted or unencrypted media communications.

Deployment Model Advantages

For environments with strict security requirements, registering Polycom RealPresence endpoints with encrypted signaling to Cisco Unified CM enables you to integrate Polycom products within a Cisco deployment without additional network management overhead. This model provides a single source for call admission control and enables Polycom video endpoints to use telephony functions such as being placed on hold or transferred to another SIP-enabled endpoint registered with Cisco Unified CM. Once endpoints are securely registered, customers have the option to use encrypted or unencrypted media.

In an enterprise using a mixture of telepresence equipment, Polycom HDX, Polycom Group Series, and Polycom Immersive Telepresence (ITP) systems are able to make and receive secure calls with Cisco CTS endpoints. Polycom endpoints can also participate in secure multipoint calls hosted by an RealPresence Collaboration Server system that is SIP trunked to Cisco Unified CM and a Cisco TelePresence Server. Polycom Group Series systems do not support secure registration or calls.

To allow for flexible deployments and migrations, Polycom endpoints can be simultaneously SIP_TLS-registered with Cisco Unified CM and H323-registered with a Polycom Distributed Media Application (DMA) system.
## Supported Products for Deployment

### Verified Polycom Product Versions

<table>
<thead>
<tr>
<th>Polycom Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 systems</td>
<td>8.4 - MPMx card required for TIP support</td>
</tr>
<tr>
<td>Polycom HDX system (all models)</td>
<td>3.1.3.2</td>
</tr>
<tr>
<td>Requires TIP option key for Cisco Immersive Telepresence calls</td>
<td></td>
</tr>
<tr>
<td>Polycom Touch Control for HDX systems</td>
<td>v1.9.0</td>
</tr>
<tr>
<td>Immersive Solutions including:</td>
<td></td>
</tr>
<tr>
<td>Polycom RealPresence Experience (RPX)</td>
<td>3.1.3.2</td>
</tr>
<tr>
<td>Polycom Open Telepresence Experience (OTX)</td>
<td></td>
</tr>
<tr>
<td>Polycom Architected Telepresence Experience (ATX)</td>
<td></td>
</tr>
<tr>
<td>Polycom Multipoint Layout Application</td>
<td>v3.1.2.8</td>
</tr>
<tr>
<td>Polycom® RealPresence® Resource Manager</td>
<td>v7.1</td>
</tr>
<tr>
<td>Polycom RealPresence DMA</td>
<td>v6.1.0</td>
</tr>
</tbody>
</table>

### Verified Cisco Product Versions

<table>
<thead>
<tr>
<th>Cisco Product</th>
<th>Release(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>9.1.2.11900-12</td>
</tr>
<tr>
<td>Cisco Unified IP Phones: 7960, 7961, 7962, 7965, 7975, 7985, 9971</td>
<td>Cisco Unified CM 9.1(2) Default Load</td>
</tr>
<tr>
<td>Cisco Jabber for Windows</td>
<td>9.7(0)</td>
</tr>
<tr>
<td>Cisco CTS500-32, TX1310, TX9000</td>
<td>6.1.2.1(5)</td>
</tr>
<tr>
<td>Cisco CTS500-37, CTS1300, CTS3010</td>
<td>1.10.5.1(4)</td>
</tr>
<tr>
<td>EX, C and SX Series</td>
<td>7.1.1</td>
</tr>
<tr>
<td>Cisco TelePresence Server</td>
<td>4.0(1.57)</td>
</tr>
</tbody>
</table>
Deployment Architecture

The following figure shows the reference architecture for this deployment model.

Architecture when Polycom telepresence endpoints are directly securely registered to Cisco Unified Communications Manager

Design Considerations

Before you register any Polycom RealPresence video endpoints to Cisco Unified CM, consider the following points about interoperability between Cisco Unified CM and Polycom systems.

Cisco Unified Communications Manager Considerations

Make note of the following Cisco Unified CM considerations:

- Location settings should allow for video bandwidth when integrating Polycom video endpoints and infrastructure.
- Region settings should allow for a minimum of 256 K video bandwidth. Region settings should match the Polycom HDX system maximum call rate.
- Region settings should allow for G.722 audio protocol for the best audio experience.
- Since Cisco Unified CM is a SIP back-to-back user agent (B2BUA), it is involved in all signaling between two endpoints making a call. Cisco Unified CM strips out and does not allow unfamiliar audio or video codecs. For this reason, some advanced Polycom codecs such as Siren LPR audio or H.264 high profile video are not negotiated between two Polycom endpoints directly registered with Cisco Unified CM.
Direct Secure Registration of Polycom RealPresence Systems with Cisco Unified CM

Note: Insertion of Media Termination Point resources

Due to the nature of out-of-band dual-tone multi-frequency (DTMF) signaling, Cisco Unified CM is capable of inserting Media Termination Point (MTP) resources in a call. This prevents video on the Polycom HDX system from operating correctly. This is most common on H.323 and SIP trunk calls. To prevent this from occurring, the MTP resources should be removed from any media resource groups and media resource group lists used in the trunked calls.

Polycom Immersive Telepresence Systems Considerations

The Telepresence Interoperability Protocol (TIP) enables multiscreen or multicamera video systems to provide video alignment and spatial audio capabilities with other multiscreen or multicamera endpoints. For multiscreen, immersive system connectivity, consider the following:

- The TIP option key is required in order to support TIP calls. Polycom telepresence endpoints support TIP version 7.
- If you have a Polycom ITP system, the TIP license is included. Ensure that the TIP option key is installed on each HDX system.
- The TIP license is required in order to register securely as a generic multi- or single-screen room system using SIP TLS.
- You must redefine Polycom ITP endpoints to enable them to participate in calls hosted by the Cisco TelePresence Server.

Content Sharing in Telepresence Environments

Within a Cisco telepresence environment, Polycom and Cisco endpoints can share content in a separate content channel. In point-to-point calls between Polycom endpoints registered to Cisco Unified CM, content is normally sent over BFCP. This includes Polycom endpoints connecting to RealPresence Collaboration Server bridge calls.

However, in HDX version 3.1.1, a new telnet command has been added (alwaysusetip) which, when set, prefers TIP connectivity when possible. Additionally, RealPresence Collaboration Server version 8.1.1 has added a new conference profile TIP Compatibility option (Prefer TIP), which forces the RealPresence Collaboration Server to prefer TIP with Polycom endpoints. When Polycom devices are configured to prefer TIP, you can share content in a separate content channel with other TIP-capable endpoints. For more information, see Configure the HDX to Prefer TIP (Optional).

Note that when using the telnet command on ITP systems, register only the center codec instead of all three codecs.

The following guidelines apply:

- Content sharing within a Polycom-Cisco environment is limited to XGA at 5 FPS.
• In multipoint calls hosted by the Polycom RealPresence Collaboration Server system, Polycom endpoints registered to Cisco Unified CM cannot send content to or receive content from Cisco TelePresence Systems (CTS) connected to the conference unless the RealPresence Collaboration Server and Polycom endpoints have been configured to prefer TIP.

• Content sharing on Polycom ITP or HDX systems is only supported via VGA cable. USB content sharing is not supported.

• The Polycom People + Content IP tool is not supported in Cisco telepresence environments.

License Devices

Device license units are assigned to each device connected to Cisco Unified Communications Manager. Each device is assigned a unit number based on the type and capabilities of the device. Devices with more complex and high-end capabilities are assigned a higher number of units than devices with basic capabilities. The following table shows the license units for Polycom devices. For more information, see your Cisco documentation.

<table>
<thead>
<tr>
<th>Required Device License Units</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Polycom Device</strong></td>
</tr>
<tr>
<td>Polycom HDX or Group Series Systems</td>
</tr>
<tr>
<td>Polycom ITP systems</td>
</tr>
</tbody>
</table>

Secure Media Methods

Cisco devices support three methods for exchanging Secure Real-time Transport Protocol (SRTP) keys for different functional call flows, and Polycom HDX and ITP systems support each method. The method in use depends on the environment, the version of Cisco Unified CM, and the version of CTS firmware. In Methods 1 and 2, Datagram Transport Layer Security (DTLS) provides communication privacy for the audio and video media streams. Method 3 uses Session Description Protocol Security (SDES) to negotiate the key for SRTP.

Method 1: Opportunistic DTLS

HDX systems use this method for backward compatibility to interoperate with previous versions of CTS (version 1.8 and earlier) and telepresence servers. These system versions do not announce Secure Audio Video Profile (SAVP) in their Session Description Protocol (SDP) offer or answer. For this reason, Cisco recommends that if the response from the far-end comes with Audio Video Profile (AVP) in the SDP, attempt an opportunistic DTLS for SRTP-key exchange.
and then fallback to establish a nonsecure session based upon messages received on RTP-channel (TIP messaging).

For successful interoperability with these versions, the HDX or ITP system’s TIP call flow makes an opportunistic DTLS handshake on RTP-transport addresses when AVP is received in a SIP-SDP message and the HDX or ITP system’s Advanced Encryption Standard (AES) Encryption setting is enabled. The audio/video media channels each have their own client/server DTLS context to exchange SRTP keys with far-end systems.

**Method 2: DTLS Fingerprint in SIP-SDP**

Cisco TIP-enabled systems and Cisco Unified CM version 8.6.2 and later provide a mechanism to announce use of DTLS-SRTP negotiation in SIP-SDP with fingerprint SRTP_AES128_HMAC_SHA1_80 SRTP/SRTCP protection profiles.

When negotiated through SIP-SDP, the HDX or ITP system attempts DTLS. Before the exchange of SRTP-keys, if the HDX or ITP system receives a TIP-message (RTCP subtype set to 1), the ongoing DTLS-handshake is aborted and one of the following scenarios occurs:

- When AES Encryption is set to **When Available**, the HDX or ITP system continues the session with non-encrypted media exchange.
- When AES Encryption is set to **Always Required**, the HDX or ITP system terminates the call.

**Method 3: SDES Keys for SRTP Encryption Key Exchange in SIP-SDP (Preferred)**

The best interoperability with TIP-secure devices occurs with Cisco Unified CM version 8.6.2 and later and with the latest versions of CTS firmware. These versions provide support of SDES with SRTP_AES128_HMAC_SHA1_32SRTP/SRTCP protection profiles. Session Description Protocol Security Descriptions (SDES) is the fallback security method in case DTLS is not negotiated.

**Securely Register a Polycom RealPresence Immersive, Room, or Desktop System with Cisco Unified CM**

To securely register the Polycom RealPresence system with Cisco Unified CM, complete the following steps in both the Cisco Unified CM and the Polycom RealPresence system.

For more information about the Cisco Unified Communications Manager, see the Cisco Unified Communications Manager Documentation Guide. For more information about Polycom HDX systems, see the Administrator's Guide for HDX Systems. For more information on Polycom Group series, see the Administrator's Guide for Group Series.
Configure Cisco Unified CM for a secure Polycom Immersive, Room, or Desktop System

Use the Cisco Unified CM web administrator interface to perform the following tasks. Before performing these tasks, review the Cisco Unified Communications Manager Considerations.

Create a Security Profile

You need to create a phone security profile for your Polycom systems. If you want to create a secure profile, you can choose to enable digest authentication to secure the Polycom endpoint system’s connection to Cisco Unified CM.

Note: Recommendation for digest authentication
Polycom recommends using digest authentication for Polycom endpoint registration.

You need to create a security profile to use with your Polycom HDX, Group Series, or ITP system. Because each endpoint uses the same security profile, you need to create only one security profile.

To configure security settings:

1. Log into the Cisco Unified CM console.
2. Select System > Security Profile > Phone Security Profile.
3. Select Add New.
4. Select a Phone Security Profile Type. Select Generic Single Screen Room System (or select Multiple for ITP systems) and click Next.
5. On Phone Security Profile Information page, complete the following fields:
   a. In the Name text box, enter a profile name for the system.
   b. In the Description field, enter a description for the security profile.
   c. Set the Device Security Mode to Encrypted.
   d. Set the Transport Type to TLS.
   e. Select the Digest Authentication check box (optional).
Set the SIP Phone Port to 5061.

6. Click Save.

In the status bar near the top of the page, Update Successful displays.

Add a System User

You need to create a Cisco Unified CM system user for each Polycom HDX or ITP system endpoint. When adding secure ITP systems, only a single system user is required for each generic single or multiple screen room system device added in Cisco Unified CM.

If you cannot add a user here, your system may be integrated with LDAP. If that is the case, you can use an existing user ID, essentially associating the endpoint to an existing user, or have your LDAP administrator create a new user ID for each Cisco Unified CM device.

To add a system user:

1. Select User Management > End User.

2. Click Add New.
Direct Secure Registration of Polycom RealPresence Systems with Cisco Unified CM

The following screen displays.

![End User Configuration Screen]

3 Complete the required fields. **User ID** and **Last Name** are required fields. The End User Password and PIN fields are arbitrary and are not used for secure registration.
   
   a To use digest authentication, enter the **Digest Credentials** (password) for the Polycom system.
   
   b In the **Confirm Digest Credentials** field, enter the same value you entered in step a.

4 Click **Save**.
   
   In the status bar near the top of the page, an **Update Successful** message displays.

Create a SIP Profile

Cisco Unified CM associates specific SIP parameters with an endpoint or trunk via a SIP profile. This step creates a SIP profile in Cisco Unified CM that can be associated with the Polycom system devices.

To create a SIP Profile:

1 Select **Device > Device Settings > SIP Profile**.
2. Click **Find** to see the list of existing SIP Profiles, and select the **Standard SIP Profile**. This is the default value in Cisco Unified CM.

3. Once open, select **Copy**.
   Most of the SIP settings are left at default. Consult your Cisco Unified CM administrator about SIP settings specific to your deployment.

4. Change the **Name** field to something meaningful for your deployment, and configure the following:
   a. Select the **Use Fully Qualified Domain Name in SIP Requests** check box.
   b. Select the **Allow Presentation Sharing using BFCP** check box.
   c. Do NOT select the **Early Offer support for voice and video calls** check box.
   The following shows an example.
5 Click **Save**.

In the status bar near the top of the page, an **Update Successful** message displays.
Add a Device Entry

You need to create a Cisco Unified CM device entry for each endpoint system. To securely register a Polycom HDX or ITP system with Cisco Unified CM, a **Generic Single Screen Room System** (GSSRS) device must be added for single-screen systems, and a **Generic Multiple Screen Room System** (GMSRS) must be added for multi-screen systems. This step adds a device to Cisco Unified CM, which in turn allows the device to securely register with Cisco Unified CM.

To add a device entry:

1. Select **Device > Phone**.
2. Click **Add New**.
3. Select **Generic Single Screen Room System** or **Generic Multiple Screen Room System** as appropriate for the Polycom endpoint, and click **Next**.

The following screen displays. The data shown in this section is an example.

![Device Information Screen](image)

In the **MAC Address** field, enter the unique MAC Address for the HDX system. For secure registration, this **must** be the actual MAC Address of the HDX or ITP system (use the center codec for ITP systems).
b (Optional) In the Description text box, enter a description.

c From the Device Pool list, select the device pool appropriate for your Cisco Unified Communications Manager system video devices.

d From the Phone Button Template list, select Generic Single Screen Room System or Generic Multiple Screen Room System.

e (Optional) If your Cisco Unified CM implementation uses partitions and call search spaces, select an appropriate calling search space for the HDX system from the Calling Search Space list.

f If your Cisco Unified CM implementation uses the Cisco Unified CM locations-based Call Admission Control (CAC), select an appropriate location for the HDX system from the Location list. This location should contain video bandwidth. Before making this selection, see Design Considerations and Cisco Unified Communications Manager Considerations.

4 Scroll to the Protocol Specific Information section.

<table>
<thead>
<tr>
<th>Protocol Specific Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Capture Mode</td>
<td>None</td>
</tr>
<tr>
<td>Packet Capture Duration</td>
<td>0</td>
</tr>
<tr>
<td>BLF Presence Group</td>
<td>Standard Presence group</td>
</tr>
<tr>
<td>MTP Preferred Originating Code</td>
<td>711law</td>
</tr>
<tr>
<td>Device Security Profile</td>
<td>Secure SIPSRS</td>
</tr>
<tr>
<td>Rerouting Calling Search Space</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>SUBSCRIBE Calling Search Space</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>SIP Profile</td>
<td>Standard SIP Profile plus BFCP</td>
</tr>
<tr>
<td>Digest User</td>
<td>1120</td>
</tr>
<tr>
<td>Media Termination Point Required</td>
<td></td>
</tr>
<tr>
<td>Unattended Port</td>
<td></td>
</tr>
<tr>
<td>Require DTMF Reception</td>
<td></td>
</tr>
<tr>
<td>Allow Presentation Sharing using BFCP</td>
<td></td>
</tr>
<tr>
<td>Allow IX Applicable Media</td>
<td></td>
</tr>
</tbody>
</table>

a From the Device Security Profile list, select the profile created in Create a Security Profile.

b In the Digest User field, select the user created in Add a System User.

c From the SIP Profile list, select the profile created in Create a SIP Profile.

d Select the Allow Presentation Sharing using BFCP check box.

5 Click Save.

In the status bar near the top of the page, an Update Successful message displays.

After you have saved the new device, the Association Information section displays.
6 In the **Association Information** section, click **Line [1] - Add a new DN**.

![](image)

7 Complete the following required fields:

   a In the **Directory Number** field, enter the phone’s extension number.

   b In the **Route Partition** field, choose the appropriate value for your Cisco Unified CM deployment.

![](image)

8 Click **Save**.

   In the status bar near the top of the page, an **Update Successful** message displays.

9 Reset the Polycom system in Cisco Unified CM.

**Configure a Polycom HDX or Immersive System for Cisco Unified CM Registration**

When a Polycom endpoint is securely registered with a Cisco Unified CM, the endpoint can make calls to Cisco endpoints that are also registered to the Cisco Unified CM and can make encrypted media calls. Use the HDX web administrator interface to perform the following tasks.
Configure SIP Settings

Configure the following SIP settings to securely register a Polycom HDX (or Immersive Telepresence) system with Cisco Unified CM. For ITP systems, only the center codec needs to be configured for secure registration.

To configure SIP settings:

1. Open a browser window and in the **Address** field enter the Polycom HDX system IP address or host name.

2. Navigate to **Admin Settings > Network > IP Network** and select **SIP**.

3. Configure the settings in the **SIP Settings** section of the **IP Network** screen. For guidance, see the following table.

### SIP Settings Fields and Their Descriptions

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Select this check box to enable the HDX system to receive and make SIP calls.</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>Specify the IP address of the Cisco Unified Communications Manager. If you leave this field blank, the Proxy Server is used.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Specify the IP address of the SIP Proxy Server. If you leave this field blank, the Registrar Server is used. If you leave both fields blank, no Proxy Server is used.</td>
</tr>
<tr>
<td>Settings</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required. For secure registration, select TLS.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specify the system’s SIP name. This is the SIP URI. Set this to the directory number you assigned to the HDX system and includes the suffix of “@&lt;ip_address&gt;” or “@&lt;dns_name&gt;” of the Cisco Unified CM call processing subscriber node to register with.</td>
</tr>
<tr>
<td>Domain User Name</td>
<td>This should match the username created in in Task2 of “Configuring Cisco Unified CM for a secure Polycom Immersive, Room, or Desktop System”</td>
</tr>
<tr>
<td>Password</td>
<td>When enabled, allows you to specify and confirm a new password that authenticates the system to the SIP Registrar Server. If using Digest Authentication, select the Password check box and set the password to the Digest Credentials password you set for the Cisco Unified Communications user you created for this HDX system.</td>
</tr>
<tr>
<td>Directory: Microsoft Lync</td>
<td>Specifies whether the SIP Registrar Server is a Lync Server. For Cisco environments, leave this check box unselected.</td>
</tr>
</tbody>
</table>

**Import a Certificate to Polycom HDX or Immersive System**

The following process outlines the steps to import a valid certificate for Cisco Unified CM. To support the SRTP/TLS feature, Polycom endpoints support the import of Cisco Unified Communications Manager X509v3 certificates. The supported certificate format is Privacy Enhanced Mail (PEM). Correspondingly, the PEM format is supported for Polycom HDX and ITP import.

**To import a Certificate:**

1. Open a browser window and in the **Address** field enter the Polycom HDX system IP address or host name.

2. Navigate to **Admin Settings > General Settings > Security > Certificates**.

3. Click on the **Create** button for a **Client Certificate Signing Requests**.

4. Fill out the following fields:
   - **Type**  Client
   - **Hash Algorithm**  SHA-1
   - **Common Name (CN)**  This must be of the format “Polycom-SEP<MAC_Address>” where the MAC Address is the actual MAC of the HDX or ITP endpoint (center codec for ITP systems).
5 Fill in the other fields as appropriate for your deployment and click **Create**.

```
<table>
<thead>
<tr>
<th>Create Certificate Signing Request (CSR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Hash Algorithm</td>
</tr>
<tr>
<td>Common Name (CN):</td>
</tr>
<tr>
<td>Organizational Unit (OU):</td>
</tr>
<tr>
<td>Organization (O):</td>
</tr>
<tr>
<td>City or Locality (L):</td>
</tr>
<tr>
<td>State or Province (ST):</td>
</tr>
<tr>
<td>Country (C):</td>
</tr>
</tbody>
</table>
```

6 Once the CSR is created, download the client CSR “client_csr.pem” file and reboot the HDX or ITP center codec.

7 At this point, the CSR must be taken to a valid Certificate Authority (CA) that is also trusted by Cisco Unified CM, so a Certificate can be generated for the HDX or ITP system.

8 Once the CSR is signed and a Certificate is generated, navigate to **Admin Settings > General Settings > Security > Certificates**.

9 Under **Add a Certificate**, browse to the certificate .pem file and add the file.

```
<table>
<thead>
<tr>
<th>Certificates</th>
<th>Restart System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any changes made to this page will automatically submit this page.</td>
<td>The system must restart for changes to take effect.</td>
</tr>
</tbody>
</table>

Maximum Peer Certificate Chain Depth: 2
Always Validate Peer Certificates from Browsers: [ ]
Always Validate Peer Certificates from Servers: [ ]
Add a Certificate: [Browse] [Add]
```

Once successfully added, it should show on the page. The following is an example:

```
<table>
<thead>
<tr>
<th>Issued To</th>
<th>Issued By</th>
<th>Expiration Date</th>
<th>Type</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>ms3-VM-SERVER-11-CA</td>
<td>ms3-VM-SERVER-11-CA</td>
<td>Wednesday, February 24, 2016</td>
<td></td>
<td>Remove</td>
</tr>
<tr>
<td>Polycom-SEP00E0DB0BC72F</td>
<td>ms3-VM-SERVER-11-CA</td>
<td>Wednesday, December 17, 2014</td>
<td></td>
<td>Remove</td>
</tr>
</tbody>
</table>
```
10 Restart the HDX or ITP center codec.

Ensure the TIP Protocol is Enabled

If your Polycom endpoint needs to participate in TIP-based calls, check to see that the TIP license has been applied to your endpoint. For secure registration, TIP must be enabled for Generic Single or Multiple Screen Room System type devices in Cisco Unified CM.

To ensure the TIP protocol is enabled:

1. Open a browser window and enter the Polycom Group Series system IP address or host name in the **Address** field.

2. Navigate to **Admin Settings > General Settings > Options**.

3. Verify that the TIP license option is included on your system.

4. Navigate to **Admin Settings > Call Preference**. The following screen displays.

5. Verify that TIP is enabled as a Call Preference and that the preferred and maximum call speeds for SIP (TIP) calls are at least 1024 Kbps or greater.
6 Use the setting `pbox alwaysusetip true` on the command line of the HDX or ITP system to support compatibility with TIP systems.

**Enable Encrypted Media Calls**

To enable encrypted audio and video media communications, configure the following settings.

**To enable encrypted media:**

1. Open a browser window and enter the Polycom HDX system IP address or host name in the **Address** field.
2. Navigate to **Admin Settings > General Settings > Security Settings**.
3. Configure **AES Encryption** to either **When Available** or **Required for All Calls** as appropriate for your deployment.

![Image of AES Encryption settings](image)

**Note: Setting AES Encryption**

AES Encryption must at least be set to **When Available** for successful secure registration.

**Define your Polycom Immersive System in the Cisco TelePresence Server (Optional)**

If your Cisco environment includes a Cisco TelePresence Server as well as Polycom ITP endpoints, you need to predefine your Polycom ITP endpoints on the Cisco TelePresence Server for them to participate in calls hosted by Cisco TelePresence Server.

You need to define the Primary codec of your Polycom ITP system as a **Legacy CTS endpoint**.

**To define your Polycom ITP endpoint:**

1. Log onto the Cisco TelePresence Server.
2. Select **Endpoints > Add legacy Cisco CTS endpoint**.
3. In the **Add legacy Cisco CTS endpoint** dialog, complete the following fields:
   a. In the **Name** field, enter a name for your Polycom ITP system.
In the **Address** field, enter the Directory Number you created for the Primary codec of your Polycom ITP system.

4. Click **Add legacy Cisco CTS endpoint**.

**Troubleshoot**

This section provides assistance in troubleshooting any issues you may have with Direct Secure Registration of Polycom RealPresence Systems with Cisco Unified CM.

**No video in calls between a Cisco endpoint and a Polycom endpoint**

**Possible Cause:** Cisco Unified CM regions settings do not allow for video.

**Workaround:** Check Cisco Unified CM regions settings. Determine the device pool associated with each endpoint and the corresponding region assigned to the respective device pools. Once you know the regions, check the region relationships in the Cisco Unified CM region settings to confirm the **Max Video Call Bit Rate** is set properly.

**Cisco CTS endpoints cannot connect to the RealPresence Collaboration Server**

**Possible Cause:** The Cisco Unified CM SIP trunk to the RealPresence Collaboration Server is configured as **OffNet**.

**Workaround:** Check Cisco Unified CM trunk settings.

In the Cisco Unified CM SIP trunk settings, confirm the **Call Classification** setting for the trunk is set to **OnNet**. Cisco CTS endpoints do not connect to endpoints classified as **OffNet**.

**Cisco endpoint shows “No bandwidth available” and does not connect to a Polycom endpoint**

**Possible Cause:** Cisco Unified CM locations-based Call Admission Control (CAC) does not have proper video bandwidth allocated.

**Workaround:** Allocate a proper amount of video bandwidth.

If the two devices are configured for different locations within Cisco Unified CM, confirm that there is adequate Video Bandwidth allocated to allow for the call under the **Locations** settings.
You can configure the Polycom Distributed Media Application (DMA) system as a SIP peer and registrar for your environment.

When you incorporate a Polycom DMA system as a SIP peer within your Cisco environment, you can do the following:

- Use the Polycom DMA system to manage and virtualize conferences on your Polycom RealPresence Collaboration Server systems.
- Route outgoing calls from the DMA system to the Cisco Unified Communications Manager (Cisco Unified CM).
- Route incoming calls from Cisco Unified CM to endpoints and systems registered to the DMA system.

See the *Polycom DMA 7000 System Operations Guide* for more information about using the Polycom DMA system.

Integrating Polycom RealPresence infrastructure with a Cisco Unified CM environment using DMA SIP peering capabilities offers an open and flexible integration that combines the strength of a Polycom RealPresence solution with the advantages of Cisco Unified CM telephony. A Polycom RealPresence solution can provide video conferencing services to a wide variety of Cisco Unified CM endpoints, including multiscreen Cisco CTS systems using TIP for immersive telepresence conferences. In addition, DMA can also provide bridge virtualization capabilities to ensure a highly available solution with market-leading scale. DMA's flexible SIP capabilities allow for the most open architecture and also can provide simultaneous integration with other systems such as Microsoft Lync.

## Supported Products for Deployment

### Verified Polycom Product Versions

<table>
<thead>
<tr>
<th>Polycom Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Distributed Media Application (DMA) 7000</td>
<td>6.1</td>
</tr>
<tr>
<td>Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 systems</td>
<td>8.4 - MPMx card required for TIP support</td>
</tr>
<tr>
<td><strong>Polycom Product</strong></td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Polycom HDX system (all models) | 3.1.3.2  
Requires TIP option key for Telepresence |
| Polycom RealPresence Group Series 300, 500, and 700 | 4.1.3.2  
Requires TIP option key for Cisco Immersive Telepresence calls |
| Polycom Touch Control for HDX systems  
Polycom Touch Control for RealPresence Group Series | 1.9.0  
4.1 |
| Immersive Solutions including:  
Polycom RealPresence Experience (RPX)  
Polycom Open Telepresence Experience (OTX)  
Polycom Architected Telepresence Experience (ATX) | 3.1.3.2 |

**Verified Cisco Product Versions**

<table>
<thead>
<tr>
<th><strong>Cisco Product</strong></th>
<th><strong>Release(s)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>9.1.2.11900-12</td>
</tr>
</tbody>
</table>
| Cisco Unified IP Phones: 7960, 7961, 7962, 7965, 7975, 7985, 9971 | Cisco Unified CM 9.1(2)  
Default Load |
| Cisco Jabber for Windows | 9.7(0) |
| Cisco CTS500-32, TX1310, TX9000 | 6.1.2.1(5) |
| Cisco CTS500-37, CTS1300, CTS3010 | 1.10.5.1(4) |
| EX, C and SX Series | 7.1.1 |
| Cisco TelePresence Video Communications Server | X8.1.1 |
| Cisco TelePresence Server | 4.0(1.57) |
Deployment Architecture

The following figure shows the reference architecture for this deployment model.

Architecture when using Polycom RealPresence Platform SIP integration with Cisco Unified CM

Design Considerations

Use a Dial Plan

When integrating Polycom DMA with Cisco Unified CM, it is important to keep in mind that they are both call control entities. Dial plan considerations are vital to the design prior to implementation—it should not be a trivial discussion that is solved during deployment. Creating an organized numbering scheme and coordinating extensions assigned to endpoints on each system to be in contiguous (summarizable) blocks on each system is ideal when possible.

Use Call Admission Control

The Call Admission Control (CAC) mechanism for both DMA and Cisco Unified CM are configured and administered separately. Care should be taken to avoid having different endpoints from the same site or location registered with both DMA and Cisco Unified CM unless the bandwidth restrictions take this into account.

Share Content

Cisco Unified CM provides general support for Binary Floor Control Protocol (BFCP) over User Datagram Protocol (UDP) as of version 8.6. Polycom RealPresence endpoints and infrastructure also support this SIP method of content sharing. For Cisco devices that support
Polycom RealPresence Platform SIP Integration with Cisco Unified CM

BFCP over UDP, dual stream (separate channels for video and content) content sharing is supported with a Polycom RealPresence solution.

The following considerations apply to content sharing for TIP-enabled immersive conferences when Polycom endpoints are registered to a Polycom DMA system that has been configured as a SIP peer with Cisco Unified CM.

**Content Sharing When Polycom Endpoint Registered to Polycom DMA System as a SIP Peer**

<table>
<thead>
<tr>
<th>Call Types</th>
<th>People + Content Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(dual stream with separate channels for video and for content)</td>
</tr>
<tr>
<td>Point to Point Calls</td>
<td></td>
</tr>
<tr>
<td>HDX/ITP/Group Series system to</td>
<td>Yes</td>
</tr>
<tr>
<td>HDX/ITP/Group Series system</td>
<td></td>
</tr>
<tr>
<td>HDX/ITP system to Cisco CTS</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco CTS to HDX/ITP system</td>
<td>Yes</td>
</tr>
<tr>
<td>Multipoint Calls on Polycom RealPresence Collaboration Server</td>
<td></td>
</tr>
<tr>
<td>HDX/ITP system to HDX/ITP system</td>
<td>Yes</td>
</tr>
<tr>
<td>HDX/ITP system to Cisco CTS</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco CTS to HDX/ITP system</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note: When a TIP License is required**

For a Polycom RealPresence Platform SIP Integration with Cisco Unified CM, a TIP license is only required on Polycom endpoints for point to point multiscreen calls with other Cisco multiscreen or multicamera endpoints. Multipoint immersive TIP conferences on the Polycom RealPresence Collaboration Server do not require the Polycom endpoints to have a TIP license with this deployment model.

**Configure SIP Integration between a Polycom DMA System and Cisco Unified CM**

You can configure Cisco Unified CM to route audio and video calls to Polycom endpoints or bridge resources via a Polycom DMA. To enable this integration, you need to perform steps in both the Cisco Unified CM and the Polycom DMA system.
For more information about the Cisco Unified Communications Manager, see the Cisco Unified Communications Manager Documentation Guide. For more information about Polycom DMA systems, see the Administrator's Guide for Polycom DMA Systems.

Configure Cisco Unified CM for SIP Integration with DMA

Perform the following steps to create a SIP integration in Cisco Unified CM to the DMA system and establish the call routing infrastructure.

Create a SIP Profile

Cisco Unified CM associates specific SIP parameters with an endpoint or trunk via a SIP Profile. This step creates a SIP profile in Cisco Unified CM that can be associated with the SIP trunk used to connect to Polycom DMA in Add a SIP Trunk.

To create a SIP Profile:

1. Select Device > Device Settings > SIP Profile.
2. Click Find to see the list of existing SIP Profiles, and select the Standard SIP Profile (a default in Cisco Unified CM).
3. Once open, select Copy.
   Most of the SIP settings are left at default; however the Cisco Unified CM administrator should be consulted for any SIP settings that may be specific to your deployment.
4. Change the Name to something meaningful for your deployment, and then ensure the following is configured.
   a. Select the Use Fully Qualified Domain Name in SIP Requests check box.
   b. Select the Allow Presentation Sharing using BFCP check box.
   c. Do NOT select the Early Offer support for voice and video calls check box.
The data shown in this section is shown as an example.

### SIP Profile Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Ready</td>
</tr>
<tr>
<td>All SIP devices using this profile must be restarted before any changes will take effect.</td>
<td></td>
</tr>
</tbody>
</table>

#### SIP Profile Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Polycom RealPresence Platform SIP Integration with Cisco Unified CM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Default MTP Telephony Event Payload Type</td>
</tr>
<tr>
<td>Resource Priority Namespace List</td>
<td>None</td>
</tr>
<tr>
<td>Early Offer for G-Clear Calls</td>
<td>None</td>
</tr>
<tr>
<td>SDP Session-level Bandwidth Modifier for Early Offer and Re-invites</td>
<td>None</td>
</tr>
<tr>
<td>User-Agent and Server header Information</td>
<td>None</td>
</tr>
<tr>
<td>Redirect by Application</td>
<td>None</td>
</tr>
<tr>
<td>Disable Early Media on 180</td>
<td>None</td>
</tr>
<tr>
<td>Outgoing 1.20 INVITE include audio on line</td>
<td>None</td>
</tr>
<tr>
<td>Enable ANAT</td>
<td>None</td>
</tr>
<tr>
<td>Require SDP Inactive Exchange for Mid-Call Media Change</td>
<td>None</td>
</tr>
<tr>
<td>Use Fully Qualified Domain Name In SIP Requests</td>
<td>None</td>
</tr>
</tbody>
</table>

#### Parameters used in Phone

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer Invite Expires (seconds)</td>
<td>180</td>
</tr>
<tr>
<td>Timer Register Delta (seconds)</td>
<td>5</td>
</tr>
<tr>
<td>Timer Register Expires (seconds)</td>
<td>3600</td>
</tr>
<tr>
<td>Timer T1 (msec)</td>
<td>100</td>
</tr>
<tr>
<td>Timer T2 (msec)</td>
<td>300</td>
</tr>
<tr>
<td>Retry INVITE</td>
<td>10</td>
</tr>
<tr>
<td>Retry Non-INVITE</td>
<td>10</td>
</tr>
<tr>
<td>Start Media Port</td>
<td>16384</td>
</tr>
<tr>
<td>Stop Media Port</td>
<td>32766</td>
</tr>
<tr>
<td>Call Pickup URI</td>
<td>x-disco-serviceuri-pickup</td>
</tr>
<tr>
<td>Call Pickup Group Other URI</td>
<td>x-disco-serviceuri-pickup</td>
</tr>
<tr>
<td>Call Pickup Group URI</td>
<td>x-disco-serviceuri-pickup</td>
</tr>
<tr>
<td>Meet Me Service URI</td>
<td>x-disco-serviceuri-meetme</td>
</tr>
<tr>
<td>User Info</td>
<td>None</td>
</tr>
<tr>
<td>CTMF DB Level</td>
<td>Nominal</td>
</tr>
<tr>
<td>Call Hold Ring Back</td>
<td>Off</td>
</tr>
<tr>
<td>Anonymous Call Block</td>
<td>Off</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>Off</td>
</tr>
<tr>
<td>Do Not Disturb Control</td>
<td>Off</td>
</tr>
<tr>
<td>Telnet Level for 7540 and 7960</td>
<td>Disabled</td>
</tr>
<tr>
<td>Timer Keep Alive Expires (seconds)</td>
<td>120</td>
</tr>
<tr>
<td>Timer Subscribe Expires (seconds)</td>
<td>120</td>
</tr>
<tr>
<td>Timer Subscribe Delta (seconds)</td>
<td>5</td>
</tr>
<tr>
<td>Maximum Redirects</td>
<td>70</td>
</tr>
<tr>
<td>Off Hook To First Digit Timer (milliseconds)</td>
<td>5000</td>
</tr>
<tr>
<td>Call Forward URI</td>
<td>x-disco-serviceuri-cfwall</td>
</tr>
<tr>
<td>Speed Dial (Abbreviated Dial) URI</td>
<td>x-disco-serviceuri-abbrevdial</td>
</tr>
<tr>
<td>Conference Join Enabled</td>
<td>x-disco-serviceuri-pickup</td>
</tr>
<tr>
<td>RFC 2543 Hold</td>
<td>x-disco-serviceuri-pickup</td>
</tr>
<tr>
<td>Semi Attended Transfer</td>
<td>x-disco-serviceuri-abbrdiaan</td>
</tr>
<tr>
<td>Enable VAD</td>
<td>False</td>
</tr>
<tr>
<td>Stutter Message Waiting</td>
<td>x-disco-serviceuri-pickup</td>
</tr>
</tbody>
</table>
To add a SIP trunk:

1. Navigate to Device > Trunk.
2. Click Add New in the upper left.
   a. For Trunk Type, select SIP Trunk.
   b. For Device Protocol, the default is SIP and cannot be changed.
   c. For Trunk Service Type, select None (Default).
3 Click **Next**.

4 Enter a **Device Name** for this trunk, and a description. (The Device Name is arbitrary and should be something meaningful to your deployment.)

5 Fill out most fields as appropriate for your deployment, paying attention to the following specific parameters:

   **a** For **Call Classification**, select **OnNet**.

   **b** If your Cisco Unified CM implementation uses the Cisco Unified CM locations-based Call Admission Control (CAC), select an appropriate location for the Polycom system from the **Location** list. This location should contain appropriate video bandwidth for connectivity to the RealPresence Collaboration Server.

   **c** Confirm that the **Media Termination Point Required** check box is NOT selected.

The following is shown for example.

<table>
<thead>
<tr>
<th>Trunk Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Trunk Configuration Interface" /></td>
</tr>
</tbody>
</table>

### Device Information
- **Product**: Polycom RealPresence
- **Device Name**: RMX_Trunk
- **SIP Trunk**: SIP
- **SIP Trunk to**: Polycom
- **Location**: HQ

### Media Termination Point Required
- **Check Box**: Not selected

---

76
d Under **Inbound Calls** settings, if your Cisco Unified CM implementation uses partitions and call search spaces, select an appropriate calling search space for the Polycom system from the **Calling Search Space** list. This affects *inbound* calls on this SIP trunk.

e In the **SIP Information** section, fill in the **Destination Address** with the DMA virtual IP address or supercluster call server FQDN.

f Select the Cisco Unified CM default **Non Secure SIP Trunk Profile**.

g Select the SIP Profile created in **Create a SIP Profile**.

The following example shows the destination DMA system with the virtual IP address “10.10.10.10”.

![SIP Information](image)

6 Click **Save**.

7 Click **Apply Config** to apply your changes.

**Add a Route Pattern**

In this task, you create a route pattern which defines a specific dial pattern or patterns that should be sent to the DMA SIP trunk created in **Add a SIP Trunk**. Video calls are an automatic negotiation as part of the call setup.

---

**Note: Using the route groups and route lists with a DMA system**

If your Cisco Unified CM implementation uses the route group, route list construct, it is also possible to add the DMA SIP trunk to that construct. Associating the SIP trunk directly to a route pattern is shown here for simplicity.
To add a route pattern:

1. Navigate to **Call Routing > Route/Hunt > Route Pattern**.

2. Click **Add New**.

3. Add a route pattern representing a single E.164 conference extension or range of extensions available on the DMA system.
   
   a. In the **Route Pattern** field, enter a name for the pattern. This example uses 6071XXXX.
   
   b. From the **Gateway/Route List** dropdown, select the **SIP Trunk** you created in Add a SIP Trunk.
   
   c. Fill in all other pertinent information for your network, such as **Route Partition** or **Calling Party Transformations** if any digit manipulation is required.
   
   d. In the **Call Classification** field, select **OnNet**.
      
      The **Provide Outside Dial Tone** check box is typically NOT selected.

4. Click **Save**.

---

**Note:** Using route groups and route lists

If a route pattern is pointed directly at a trunk, any subsequent route patterns that you add are resets and ALL calls on the trunk are dropped. The use of route groups and route lists allows calls to stay active while adding route patterns and is highly recommended.
Configure DMA for SIP Integration with Cisco Unified CM

On the DMA system, you need to configure an external SIP peer for Cisco Unified CM. This allows the DMA system to route and receive SIP calls to devices registered to Cisco Unified CM.

Configure a SIP Peer

The following steps configure the DMA System with a SIP Peer for Cisco Unified CM.

To configure a SIP peer:

1. Log into the DMA System.
2. Navigate to Network > External SIP Peer.
3. In the Actions menu, click Add.
4. Click on the External SIP Peer tab.
   a. Type a name and description for the SIP Peer.
   b. Ensure that the Enabled check box is selected.
   c. In the Next hop address field, type the IP address or DNS-resolvable name of the primary call processing Cisco Unified CM node.
   d. In the Port field, enter the SIP port to use. The default port is 5060.
   e. (Optional) In the Prefix Range field, enter the prefix associated with the Cisco Unified CM.
      Associating a prefix with your Cisco Unified CM depends on how you have set up dial plans and rules within your DMA system. For detailed information, see the Polycom DMA System Operations Guide.
      For redundant integrations, do not configure a Prefix Range directly on the DMA SIP peer.
   f. In the Type drop-down list, select Other.
   g. In the Transport Type drop-down list, select either TCP or UDP. This depends on the settings of the Cisco Unified CM SIP Trunk Security Profile configuration associated with the Cisco Unified CM SIP trunk.
h. Ensure the **Register Externally** check box is not selected.

5. Click on the **Postliminary** tab.
   
a. Clear the **Copy all parameters of original “To” headers** check box.

b. In the **Format** drop-down list, select **With Display, use peer’s next hop address as host**.
6 Click OK.

7 (Optional) If you want redundancy to more than one Cisco Unified CM call processing node, repeat steps 1-6 for up to two other active call processing nodes on the same Cisco Unified CM cluster.

Set up a Dial Rule (Optional)

If you have configured a prefix directly on the SIP peer, this task is not required. For redundant integrations, this step is required. As a best practice, the dial rule configured for Cisco Unified CM should be last in your logical list of dial rules.

See the “Dial Rules” section of the “Call Server Configuration” chapter in the DMA system Operations Guide for detailed information about using dial rules.

To set up a dial rule for Cisco Unified CM calls:

1 Select Admin > Call Server > Dial Rules.

2 Click Add.

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

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

5 In the Available SIP Peers area, select the SIP peers you created for Cisco Unified CM in Configure a SIP Peer and move them to the Selected SIP Peers area using the ">") button.

6 Select the Enabled check box.
7 Select the Preliminary tab.

8 Enter a DMA Script that identifies calls to numbers with the desired prefix. This example uses a script to identify extensions beginning with the prefix 6555.

![EDIT-DIAL-RULE](image)

For more information and examples on DMA scripting capabilities, please refer to the DMA Operators Guide.

9 Click OK.

Create a TIP-Enabled Conference Template (Optional)

If you are using the Polycom DMA system to route telepresence conferences to Virtual Meeting Rooms (VMRs), you need to create a conference profile that is TIP-enabled and supports a minimum of 1024 Kbps.

To create a TIP-enabled conference profile:

1 Log onto your DMA system.

2 Select Admin > Conference Manager > Conference Templates.

3 Click Add.

4 Select the Common Settings tab to enter a name and description for your template.

5 Select the RealPresence Collaboration Server General Settings tab.
   a In the Line rate field, select a line rate of 1024 Kbps or higher.
b In the **TIP compatibility** field, select **Video Only**, **Video and Content** or **Prefer TIP**, depending on what you want to support.

6 Select the **RealPresence Collaboration Server Video Quality** tab.
   a Set the **Max resolution (v7)** to **Auto** or at least **HD 720**.
   b Disregard the **Content Video Definition** settings.

7 Select the **RealPresence Collaboration Server Video Settings** tab.
a Set the **Telepresence Mode** to **Auto** or **On**.

b Set the **Telepresence Layout Mode** to the layout desired. This affects the video experience of the conference.

Set to **Room Switch** for the most immersive experience with other multiscreen systems. Conference attendees sees the multiscreen endpoint with the current active speaker for the conference.

Set to **Continuous Presence** for meetings in which all or a subset of participants should be viewable for the conference.

![Add Conference Template](image)

8 Click **OK**.

**Troubleshoot**

This section provides assistance in troubleshooting any issues you may have with Polycom RealPresence Platform SIP Integration with Cisco Unified CM.

**Cisco Unified CM sends calls to a DMA registered endpoint but endpoint does not ring**

**Possible Cause:** Cisco Unified CM is sending the SIP URI as `<alias>@<ip_address_of_DMA>`.

**Workaround:** In Cisco Unified CM, if the customer adds the DMA SIP peer as an IP address, then Cisco Unified CM sends the call in this format. There are two options. In Cisco Unified CM, add the DMA peer destination as a FQDN and ensure the **SIP Profile** associated with the Cisco Unified CM SIP trunk is configured with **Use Fully Qualified Domain Name in SIP Requests** enabled.
Alternatively, in DMA under **Call Server > Domains**, add the IP address of the DMA server as a domain and calls are accepted by DMA in this format.

**Cisco Unified CM SIP endpoint calls to DMA H323 endpoints may be denied due to bandwidth**

**Possible Cause:** When DMA invokes its SIP-to-H323 gateway feature, it is forced to look at bandwidth settings for H.323. The Cisco Unified CM SIP peer destination may not be defined in any sites in DMA (or RealPresence Resource Manager if integrated), so it denies the call.

**Workaround:** Add the Cisco Unified CM node’s subnet to the customer’s site topology. DMA doesn’t look at bandwidth parameters for SIP calls—only H323. You should add the Cisco Unified CM SIP peer to the site topology.

**Calls from a Cisco CTS are not able to connect to a DMA registered endpoint or RealPresence Collaboration Server**

**Possible Cause:** The Cisco CTS IP address may not be defined in the site topology.

**Workaround:** Add the Cisco CTS’s subnet or IP to the customer’s site topology in DMA under **Network > Site Topology > Sites**. If the DMA is integrated with RealPresence Resource Manager, add it to the site topology there.

**Calls from a Cisco CTS are not able to connect to a DMA VMR**

**Possible Cause:** DMA conference settings may be limiting the maximum bit rate for calls.

**Workaround:** In DMA under **Admin > Conference Manager > Conference Settings**, check that the **Default maximum bit rate (kbps)** is at least 4096 for CTS immersive connectivity.

![Configuring conference settings in DMA](image-url)
Calls from a DMA-registered HDX endpoint are denied by Cisco Unified CM

Possible Cause: If there are spaces in the HDX system name, DMA fills these in with “%20”, as shown next.

![From: <sip:UCALAB%20HDX%207002-1@10.47.48.26>;tag=0275ee566901](image)

Workaround: Remove spaces from the HDX system name.
Chapter 6: Polycom RealPresence Platform Integration with VCS

For customers that have existing investments with Cisco Video Communications Server (VCS) but wish to enhance or migrate the solution to Polycom RealPresence infrastructure, Polycom supports a SIP integration as well as an H.323 integration between a Polycom DMA system and VCS.

See the Polycom DMA 7000 System Operations Guide for more information about using the Polycom DMA system.

Deployment Model Advantages

Integrating Polycom RealPresence infrastructure with a Cisco VCS environment using DMA SIP peering or H.323 Gatekeeper neighboring capabilities offers an open and flexible path both for integrations as well as migrations. Companies with new acquisitions and service providers alike can benefit from Polycom’s open approach to unified communications. DMA can also provide bridge virtualization capabilities for ad-hoc VMR environments to ensure a highly available solution with market-leading scale. DMA’s flexible SIP capabilities allow for the most open architecture on the market and also can provide simultaneous integration with other systems such as Microsoft Lync.

Supported Products for Deployment

**Verified Polycom Product Versions**

<table>
<thead>
<tr>
<th>Polycom Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Distributed Media Application (DMA) 7000</td>
<td>6.1</td>
</tr>
<tr>
<td>Polycom RealPresence Collaboration Server 1500/1800/2000/4000 systems</td>
<td>8.4 - MPMx card required for TIP support</td>
</tr>
<tr>
<td>Polycom HDX system (all models)</td>
<td>3.13.2</td>
</tr>
<tr>
<td>Polycom RealPresence Group Series 300, 500, and 700</td>
<td>4.1.3.2</td>
</tr>
<tr>
<td></td>
<td>Requires TIP option key for Cisco Immersive Telepresence calls</td>
</tr>
<tr>
<td>Polycom VVX 1500</td>
<td>4.1</td>
</tr>
</tbody>
</table>
Verified Cisco Product Versions

<table>
<thead>
<tr>
<th>Cisco Product</th>
<th>Release(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Video Communications Server</td>
<td>X8.1.1</td>
</tr>
<tr>
<td>Cisco C Series</td>
<td>7.1.1</td>
</tr>
<tr>
<td>Cisco EX Series</td>
<td>7.1.1</td>
</tr>
<tr>
<td>Cisco SX Series</td>
<td>7.1.1</td>
</tr>
<tr>
<td>Cisco TelePresence MCU</td>
<td>4.3</td>
</tr>
</tbody>
</table>

Deployment Architecture

The following figure shows the SIP reference architecture for this deployment model.

Architecture when using Polycom DMA System SIP peering to Cisco VCS
Design Considerations

Dial Plan

When integrating Polycom DMA with VCS, it is important to keep in mind that they are both call control entities. Dial plan considerations are a vital aspect of the design prior to implementation and often must also account for the telephony or IP PBX solution in the environment. Creating an organized numbering scheme and coordinating extensions to be in contiguous (summarizable) blocks on each system is ideal when possible.

In the case of SIP and SIP Uniform Resource Identifiers (URI), the domain of each system must be configured as well. If VCS is responsible for the subdomain abc.company.com, it may be advantageous to have DMA be responsible for its own subdomain, for example, xyz.company.com.

In the case of H.323, naming conventions for H323-IDs should also be considered.

Call Admission Control

The Call Admission Control (CAC) for each system is configured and administered separately. Care should be taken to avoid having different endpoints from the same site or location registered with both DMA and VCS unless the bandwidth restrictions take this into account.
Protocol Conversion

When designing the integration between VCS and DMA, consider use cases where either DMA or VCS performs H.323-to-SIP or SIP-to-H.323 conversion services. VCS uses a licensing method for each conversion that occurs, so it is important to note when a particular use case invokes a license. DMA does not license these calls separately, but has separate capacity limits for these calls.

Note: DMA system gateway function usage

The DMA system’s gateway function is used only for calls to registered endpoints, SIP peers, and H.323 gatekeepers. It’s not used for calls to virtual meeting rooms (VMRs), virtual entry queues (VEQs), external addresses, or IP addresses.

See the Polycom DMA 7000 System Operations Guide for more information about protocol conversion capabilities and limits on the Polycom DMA system.

See the VCS Configuration Guides for more information about VCS traversal licenses.

Configure SIP Integration Between a Polycom DMA System and VCS

You can configure VCS to route audio and video calls to Polycom endpoints or bridge resources via a SIP integration to Polycom DMA. To enable this integration, you need to perform steps in both VCS and the Polycom DMA system.

Configure VCS for SIP Integration with DMA

Complete the following tasks to create a SIP integration in VCS to the DMA system and establish the call routing infrastructure.

Add a Neighbor Zone

VCS uses the concept of “zones” to configure neighbors.

To add a SIP neighbor zone:

1. From the VCS web administration pages, select VCS Configuration > Zones.
2. Click New to create a new neighbor.
3. Configure a Name that is meaningful for your deployment, and select Neighbor from the Type dropdown list. The Neighbor Zone configuration parameters are then displayed.
4. Many settings can be left at default, but note the following parameters.
   a. Under H.323, select a Mode of Off from the dropdown list.
b Under **SIP**, first set **Transport** to **TCP** and then change the **Port** setting to **5060**.

c Under **Location**, configure the **Peer 1 address** with the virtual IP address of your DMA node. Alternatively, you can configure the Fully Qualified Domain Name (FQDN) of the DMA supercluster.

d Under **Advanced**, the default **Zone profile** works for most deployments; however, the VCS administrator should be consulted for any custom SIP attributes that are specific to your deployment.

---

**Add a Dial Plan Search Rule**

A VCS dial plan search rule identifies when calls should be routed to the DMA neighbor zone.
To add a dial plan search rule:

1. From the VCS web administration pages, select VCS Configuration > Dial plan > Search rules.

2. Click New to create a new search rule.

3. Configure a Rule name that is meaningful for your deployment, and select parameters that are specific to the call routing for your environment.

   a. From the Target dropdown, select the neighbor zone configured in Add a Neighbor Zone. Note the example below is different than the example in shown previously.

   b. If a numeric prefix defines endpoints registered to the DMA system, configure the following:
      » Select Alias pattern match for Mode.
      » Select Prefix for Pattern type.
      » Enter a Pattern string.

   In the example shown next, calls are forwarded to extensions beginning with 71 to the Polycom DMA system.

   ![Edit search rule](image)

   c. If a unique subdomain defines endpoints registered to the DMA system, configure the following:
      » Select Alias pattern match for Mode.
      » Select Regex for Pattern type.
» Enter a regular expression in **Pattern string**.

In the example shown next, calls are forwarded to SIP URIs ending in `dma.company.com` to the Polycom DMA system.

Verify Bandwidth Configuration and Restrictions (Optional)

To complete this step, check with the VCS administrator to confirm the bandwidth limit settings in VCS.

To **verify bandwidth configuration and restrictions:**

1. From the VCS web administration pages, select **VCS Configuration > Bandwidth > Configuration**.
2. Verify the default call bandwidth
3. From the VCS web administration pages, select **VCS Configuration > Local Zone > Subzones**.
4. For endpoints in subzones or sites that access this integration, ensure any subzone bandwidth restrictions allow for bandwidths expected by the solution.

**Configure DMA for SIP Integration with VCS**

On the DMA system, you need to configure an external SIP peer for VCS. This allows the DMA system to route and receive SIP calls to devices registered to VCS.
Configure a SIP Peer

The following steps configure the DMA System with a SIP Peer for VCS.

To configure a SIP Peer:

1. Log into the DMA System.
2. Navigate to Network > External SIP Peer.
3. In the Actions menu, click Add.
4. Click on the External SIP Peer tab.
   a. Type a name and description for the SIP Peer.
   b. Ensure that the Enabled check box is selected.
   c. In the Next hop address field, type the IP address or DNS-resolvable name of the primary VCS node.
   d. In the Port field, enter the SIP port to use. The default port is 5060.
   e. (Optional) In the Prefix Range field, enter the prefix associated with the VCS.

   Associating a prefix with VCS depends on how you have set up dial plans and rules within your DMA system. For detailed information, see the Polycom DMA System Operations Guide.

   For redundant integrations, do not configure a Prefix Range directly on the DMA SIP Peer.
   f. In the Type drop-down list, select Other.
   g. In the Transport Type drop-down list, select TCP.
   h. Ensure the Register Externally check box is unchecked.
5 Click on the **Domain List** tab (optional).

a If calls should be routed to the VCS according to a unique subdomain for the environment, enter that domain here and click **Add**.

6 Click on the **Postliminary** tab.

a Select the **Copy all parameters of original “To” headers** check box.

b In the **Format** drop-down list, select **Use original request’s To**.

7 Click **OK**.

8 (Optional) If you want redundancy to more than one VCS node, repeat steps 1-6 for up to two other active nodes on the same VCS cluster.
Set up a Dial Rule (optional)

If you have configured a prefix directly on the SIP peer, this task is not required. For redundant integrations, this step is required. As a best practice, the dial rule configured for VCS should be last in your logical list of dial rules.

See the “Dial Rules” section of the of the “Call Server Configuration” chapter in the *DMA System Operations Guide* for detailed information about using dial rules.

To set up a dial rule for VCS calls:

1. Select Admin > Call Server > Dial Rules.
2. Click Add.
3. In the Add Dial Rule dialog, enter a description for your dial rule.
4. In the Action drop-down menu, select Resolve to external SIP peer.
5. In the Available SIP Peers area, select the SIP peers you created for VCS in Configure a SIP Peer and move them to the Selected SIP Peers area using the “>” button.
6. Ensure you selected the Enabled check box.
7. Select the Preliminary tab.
8. Select the Enabled check box.
9. Enter a DMA Script that identifies calls to numbers with the desired prefix. This example uses a script to identify extensions beginning with the prefix 72.
Configure H.323 Integration between a Polycom DMA System and VCS

You can configure VCS to route audio and video calls to Polycom endpoints or bridge resources via an H.323 integration to Polycom DMA. To enable this integration, you need to perform steps in both VCS and the Polycom DMA system.

Configure VCS for H323 Integration with DMA

Perform the following tasks to create an H323 integration in VCS to the DMA system and establish the call routing infrastructure.

Add a Neighbor Zone

VCS uses the concept of zones to configure neighbors.

To add a H323 neighbor zone:

1. From the VCS web administration pages, select VCS Configuration > Zones.
2. Click New to create a new neighbor.
3 Configure a **Name** that is meaningful for your deployment, and select **Neighbor** from the **Type** dropdown list. The neighbor zone configuration parameters are then displayed.

4 Many settings can be left at default, but not the following parameters.

   a Under **H.323**, select a **Mode** of **On** from the dropdown list.

   b Under **SIP**, select a **Mode** of **Off** from the dropdown list.

   c Under **Location**, configure the Peer 1 address with the virtual IP address of your DMA node. Alternatively, you can configure the Fully Qualified Domain Name (FQDN) of the DMA supercluster.
Under **Advanced**, the default **Zone profile** works for most deployments; however, the VCS administrator should be consulted for any custom H.323 attributes that are specific to your deployment.

--

**Add a Dial Plan Search Rule**

A VCS Dial Plan Search Rule identifies when calls should be routed to the DMA neighbor zone.

**To add a dial plan search rule:**

1. From the VCS web administration pages, select **VCS Configuration > Dial plan > Search rules**.
2 Click **New** to create a new search rule.

3 Configure a **Rule name** that is meaningful for your deployment, and select parameters that are specific to the call routing for your environment.
   
   a From the **Target** dropdown, select the Neighbor Zone configured in Add a Neighbor Zone.

   b If a numeric prefix defines endpoints registered to the DMA system, configure the following:
      
      » Select **Alias pattern match** for **Mode**.
      » Select **Prefix** for **Pattern type**.
      » Enter a **Pattern string**.

   In the example shown next, calls are forwarded to extensions beginning with **72** to the Polycom DMA system.

![Create search rule](image)

**Verify Bandwidth Configuration and Restrictions (Optional)**

To complete, check with the VCS administrator to confirm the bandwidth limit settings in VCS.
To verify bandwidth configuration and restrictions:

1. From the VCS web administration pages, select **VCS Configuration > Bandwidth > Configuration**.
2. Verify the default call bandwidth.
3. From the VCS web administration pages, select **VCS Configuration > Local Zone > Subzones**.
4. For endpoints in subzones or sites that access this integration, ensure any subzone bandwidth restrictions allow for bandwidths expected by the solution.

Configure DMA for H323 Integration with VCS

On the DMA system, you need to configure an external gatekeeper for VCS. This allows the DMA system to route and receive H323 calls to devices registered to VCS.

**Configure an External Gatekeeper**

The following steps configure the DMA System with an H.323 gatekeeper neighbor relationship with VCS.

**To configure an external gatekeeper:**

1. Log into the DMA System.
2. Navigate to **Network > External Gatekeeper**.
3. In the **Actions** menu, click **Add**.
4. Click on the **External Gatekeeper** tab.
   a. Type a name and description for the SIP peer.
   b. Ensure that the **Enabled** check box is selected.
   c. In the **Address** field, type the IP address or DNS-resolvable name of the primary VCS node.
   d. In the **RAS Port** field, enter the H.323 neighbor port to use. The default port is **1719**.
   e. (Optional) In the **Prefix Range** field, enter the prefix associated with the VCS. If this prefix should be stripped prior to sending a location request to VCS, select the **Strip prefix** check box.

Associating a prefix with VCS depends on how you have set up dial plans and rules within your DMA system. For detailed information, see the *Polycom DMA System Operations Guide*.

For redundant integrations, do not configure a **Prefix Range** directly on the DMA external gatekeeper.
(Optional) If you want redundancy to more than one VCS node, repeat steps 1 to 4 for up to two other active nodes on the same VCS cluster.

Set up a Dial Rule (optional)

If you have configured a prefix directly on the external gatekeeper, this task is not required. For redundant integrations, this step is required. As a best practice, the dial rule configured for VCS should be last in your logical list of dial rules.

See the “Dial Rules” section of the of the “Call Server Configuration” chapter in the DMA System Operations Guide for detailed information about using dial rules.

To set up a dial rule for VCS calls:

1. Select Admin > Call Server > Dial Rules.
2. Click Add.
3. In the Add Dial Rule dialog, enter a description for your dial rule.
4. In the Action drop-down menu, select Resolve to external gatekeeper.
5. In the Available gatekeepers area, select the gatekeepers you created for VCS in Configure an External Gatekeeper and move them to the Selected gatekeepers area using the “>” button.
6 Select the **Enabled** check box.

7 Select the **Preliminary** tab.

8 Select the **Enabled** check box.

9 Enter a DMA Script that identifies calls to numbers with the desired prefix. This example uses a script to identify extensions beginning with the prefix **83**.

```plaintext
//FILTER (Inverted)
// Do not match on this rule unless the dial string has prefix 83
// non-83 --> NEXT_RULE
if(!Dial_STRING.match('^83'))
{
    return NEXT_RULE;
}
```

103
For more information and examples on DMA scripting capabilities, refer to the *DMA Operators Guide*.

Click OK.

**Troubleshoot**

This section provides assistance in troubleshooting any issues you may have with Polycom DMA SIP peering with VCS.

**VCS SIP endpoint calls to DMA H323 endpoints may be denied due to bandwidth**

**Possible Cause:** When DMA invokes its SIP_to_H323 gateway feature, it is forced to look at bandwidth settings for H.323. The VCS SIP peer destination may not be defined in any sites in DMA (or RealPresence Resource Manager if integrated), so it denies the call.

**Workaround:** Add the VCS node’s subnet to the customer’s site topology. DMA doesn’t look at bandwidth parameters for SIP calls—only H.323. You should add the VCS SIP peer to the site topology.

**Calls from a Cisco VCS-registered endpoint are not able to connect to a DMA-registered endpoint or RealPresence Collaboration Server**

**Possible Cause:** The Cisco VCS endpoint’s IP Address may not be defined in the site topology.

**Workaround:** Add the Cisco VCS endpoint’s subnet or IP to the customer’s site topology in DMA under **Network > Site Topology > Sites**. If DMA is integrated with RealPresence Resource Manager, add it to the site topology there.

**Calls from DMA to VCS using SIP may get denied**

**Possible Cause:** When DMA forms the SIP Invite, it uses the format: `<extension/host>@<IP_Address/DNS name of configured SIP peer>`. VCS may not like this and may prefer to see `<extension/host>@<VCS domain/sub-domain>`.

**Workaround:** In DMA under the **External SIP Peer** configuration, in the **Destination Network** field, fill in the domain/sub-domain that VCS is responsible for, as shown next.
Then under **Postliminary, Request URI options**, choose the Format **Original user, configured peer’s Destination Network or next hop address**.
Chapter 7: Polycom RealPresence Platform SIP Integration with Cisco CUBE SP Edition

Customers and service providers that provide protocol interworking, admission control, and security demarcation services with the Cisco Unified Border Element (CUBE) SP Edition feature on a Cisco 1000 series Aggregation Services Router (ASR) have the flexibility to also deploy Polycom RealPresence infrastructure in their environment. CUBE SP Edition enables direct IP-to-IP interconnect between domains, which may be a vendor or a service provider service offering. This chapter covers the supported versions and deployment scenario for environments with CUBE SP Edition on Cisco ASR and a Polycom Distributed Media Application (DMA) virtualization server.

See the Polycom DMA 7000 System Operations Guide for more information about using the Polycom DMA system.


Deployment Model Advantages

Integrating Polycom RealPresence infrastructure with a CUBE SP Edition Cisco ASR provides service providers with more flexibility and choice in their video collaboration services, and it also offers end customers who have already deployed CUBE SP Edition for voice services investment protection and the extension of video collaboration to their deployment. Companies with new acquisitions and service providers alike can benefit from Polycom’s open approach to unified communications.

DMA can also provide bridge virtualization capabilities for ad-hoc VMR environments to ensure a highly available solution with market-leading scale. DMA’s flexible SIP capabilities allow for the most open architecture on the market and also can provide simultaneous integration with other systems such as Microsoft Lync.
## Supported Products for Deployment

### Verified Polycom Product Versions

<table>
<thead>
<tr>
<th>Polycom Product</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Distributed Media Application (DMA) 7000</td>
<td>6.1</td>
</tr>
<tr>
<td>Polycom RealPresence Collaboration Server (RMX) 1500/2000/4000 systems</td>
<td>8.4 - Mom card required for TIP support</td>
</tr>
<tr>
<td>Polycom Multipoint Layout Application</td>
<td>3.1.2.8</td>
</tr>
<tr>
<td>RealPresence Resource Manager</td>
<td>8.2</td>
</tr>
<tr>
<td>Polycom HDX system (all models)</td>
<td>3.1.4</td>
</tr>
<tr>
<td></td>
<td>Requires TIP option key for Cisco Immersive Telepresence calls</td>
</tr>
</tbody>
</table>

### Verified Cisco Product Versions

<table>
<thead>
<tr>
<th>Cisco Product</th>
<th>Release(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 1000 Series (CUBE SP Edition)</td>
<td>IOS-XE 15.1(3)S2, (SBC 3.4.4) 15.2(4)S3 (SBC 3.7.3S)</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>9.1.2.11900-12</td>
</tr>
<tr>
<td>Cisco CTS500-32, TX1310, TX9000</td>
<td>6.1.2.1(5)</td>
</tr>
<tr>
<td>Cisco CTS500-37, CTS1300, CTS3010</td>
<td>1.10.5.1(4)</td>
</tr>
<tr>
<td>EX, C, MX and SX Series</td>
<td>7.1.1</td>
</tr>
<tr>
<td>Cisco Video Communications Server</td>
<td>X8.1.1</td>
</tr>
<tr>
<td>Cisco Telepresence Server</td>
<td>4.0(1.57)</td>
</tr>
</tbody>
</table>
Deployment Architecture

The following figure shows the SIP reference architecture for this deployment model.

**Design Considerations**

For secure deployments, careful considerations should be made with respect to certificate requests, trusted root certificate authorities (CAs), and the installed certificates themselves. It is important that certificates on all components needing to communicate in an encrypted fashion have a common trusted root CA.

*Note: Mandatory use of certificate authority with DMA*

While the use of a certificate authority (CA) is preferred, certificates may be exchanged between devices to establish the trust relationships. Use of a CA is mandatory if using the shared number dialing (Virtual Entry Queue) feature on DMA.
Polycom features such as High Profile and Siren22 (and other Polycom specific audio and video codecs) are currently not operational in this environment.

**Configure SIP Integration between a Polycom DMA System and CUBE SP Edition**

You can configure a CUBE SP Edition to route registrations and audio and video call invites to Polycom DMA via a SIP integration. To enable this integration, you need to perform steps in both CUBE SP Edition and the Polycom DMA system.


For more information about Polycom DMA systems, see the *Administrator’s Guide for Polycom DMA Systems*.

**Configure CUBE SP for SIP Integration with DMA**

Perform the following high-level steps to allow a SIP trunk integration in CUBE SP to the DMA system and establish the call routing infrastructure. It is recommended to have separate adjacencies specifically for unencrypted and encrypted traffic.

**Note: Configuration of CISCO IOS-XE operating system outside document scope**

It is outside the scope of this documentation to provide specific configuration syntax on the Cisco IOS-XE Operating System that runs on the Cisco ASR. High-level configuration steps will be noted, but you must consult Cisco documentation for actual configuration syntax.

**To configure the CUBE SP for SIP Integration with DMA**

1. (Optional) If the deployment requires encrypted signaling, upload a **crypto pike certificate chain** to the Cisco ASR.

   Ensure that this certificate and the one used for DMA are issued from the same trusted root CA.

2. After setting up the SBC interfaces and IP Addressing, under **SBC** configuration, create an **adjacency** for DMA. Alternate adjacencies are required to complete the SBC setup and allow traffic to flow to DMA and RealPresence Collaboration Server.

   a. If encryption is required, ensure that **security trusted-encrypted** is configured for the adjacency. Also, typically both sides communicate using port **5061**; configure this for the **signaling-port** and **signaling-peer-port** unless different for your deployment.
b If registrations should be allowed through this CUBE SP Edition, ensure a **registration target address** and **port** are configured pointing to the DMA server virtual IP or FQDN. The DNS server used by the SBC must have all DMA systems defined with a proper FQDN to function properly in normal operation and DMA failover modes.

c Configure a **realm** to assign a specific media address to this adjacency (for a later step; realm is NOT required but strongly recommended).

d The following example does not include all the commands contained under adjacency configuration. For this example, the IP address used by CUBE for this adjacency is 10.10.10.10, DMA has a FQDN of “callserver-site-1.callservers.domain.com”, secure communication is required, and registrations are allowed through this Cisco ASR:

```plaintext
! adjacency sip DMA-TLS
   security trusted-encrypted
   signaling-address ipv4 10.10.10.10
   signaling-port 5061
   signaling-peer callserver-site-1.callservers.domain.com
   signaling-peer-port 5061
   registration target address callserver-site-1.callservers.domain.com
   registration target port 5061
   realm DMA-TLS-MEDIA
   attach
```

3 Configure a **cac-policy-set** with **entry** configuration to allow for SRTP if encrypted media is required.

4 Configure a **call-policy-set** as required to allow calls between adjacencies.
   
   See the chapter **Configuration Example** for a full configuration example.

### Configure DMA for SIP Integration with CUBE SP

If your deployment requires DMA to handle unencrypted calls only coming from CUBE SP Edition, DMA handles this without the following tasks. If encrypted signaling and outbound calls are required from your DMA node or supercluster, then the following tasks allow the DMA system to route and receive SIP calls to other adjacent domains configured on the CUBE SP ASR.

### Upload Security Certificate (optional)

If your deployment requires encrypted SIP TLS signaling, the following steps add a security certificate to DMA.

For secure deployments, it is vital that the certificate uploaded to DMA and CUBE SP Edition have the same trusted root certificate authorities (CA). It is important that certificates on all components needing to communicate in an encrypted fashion have a common trusted root CA.
To upload a certificate:

1. Log into the DMA System.
2. Navigate to Admin > Local Cluster > Certificates.
3. In the Actions menu, click Create Certificate Signing Request and copy the encoded request. Follow your procedures for getting this request signed by a Trusted Root CA for your environment.
4. Once a Trusted Root CA has generated the certificate for DMA, click on the Add Certificates tab in the Actions menu and either upload the certificate file or paste the certificate text as requested.

For more information on uploading certificates to DMA, see the DMA System Operations Guide.

Configure a SIP Peer (optional)

If your deployment requires that outbound calls are made toward the CUBE SP Edition router, the following steps configure the DMA system with a SIP peer for routing these calls:

To configure a SIP peer:

1. Log into the DMA system.
2. Navigate to Network > External SIP Peer.
3. In the Actions menu, click Add.
4. Click on the External SIP Peer tab.
   a. Type a name and description for the SIP Peer.
   b. Ensure that the Enabled check box is selected.
   c. In the Next hop address field, type the IP address or DNS-resolvable name of the CUBE SP SIP peer address for this adjacency.
   d. In the Port field, enter the SIP port to use. The default port is 5060. Typical secure deployments requiring SIP TLS signaling use port 5061. Ensure the signaling port matches what is configured in the CUBE SP.
   e. (Optional) In the Prefix Range field, enter the prefix associated with calls that should be routed to CUBE SP Edition.

Associating a prefix with this external SIP peer depends on how you have set up dial plans and rules within your DMA system. For detailed information, see the Polycom DMA System Operations Guide.

For redundant integrations, do not configure a Prefix Range directly on the DMA SIP Peer.

f. In the Type drop-down list, select Other.
In the **Transport Type** drop-down list, select **TCP** for unencrypted signaling, or if your deployment requires encrypted signaling, select **TLS**.

Ensure the **Register Externally** check box is cleared.

5 Click on the **Domain List** tab (optional).
   
   a If calls should be routed to the CUBE SP Edition router according to a unique subdomain for the environment, enter that domain here and click **Add**.

6 Click on the **Postliminary** tab.
   
   a Select the **Copy all parameters of original “To” headers** check box.
b In the **Format** drop-down list, select **Use original request’s To**.

7 Click **OK**.

**Set up a Dial Rule (optional)**

If you have configured a prefix directly on the SIP peer, this task is not required. For redundant integrations, this step is required. As a best practice, the dial rule configured for CUBE SP Edition should be last in your logical list of dial rules.

See the “Dial Rules” section of the of the “Call Server Configuration” chapter in the *DMA System Operations Guide* for detailed information about using dial rules.

**To set up a dial rule for CUBE SP calls:**

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

2 Click **Add**.

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

4 In the **Action** drop-down menu, select **Resolve to external SIP peer**.
5 In the **Available SIP Peers** area, select the SIP peers you created for VCS in **Configure a SIP Peer (optional)** and move them to the **Selected SIP Peers** area using the “>” button.

6 Select the **Enabled** check box.
7 Select the **Preliminary** tab.
8 Select the **Enabled** check box.
9 Enter a DMA Script that identifies calls to numbers with the desired prefix. This example uses a script to identify extensions beginning with the prefix 72.

For more information and examples on DMA scripting capabilities, please refer to the DMA Operators Guide.

10 Click OK.

Troubleshoot

This section provides assistance in troubleshooting any issues you may have with Polycom DMA SIP peering with CUBE SP Edition.

Cisco Unified CM sends calls to a DMA registered endpoint but endpoint does not ring

Possible Cause: Cisco Unified CM is sending the SIP URI as <alias>@<ip_address_of_DMA>

Workaround: In Cisco Unified CM, if the customer adds the DMA SIP peer as an IP address, then Cisco Unified CM sends the call in this format.

There are two options. In Cisco Unified CM, add the DMA peer destination as a FQDN and ensure the SIP Profile associated with the Cisco Unified CM SIP trunk is configured with Use Fully Qualified Domain Name in SIP Requests enabled.

Alternatively, in DMA under Call Server > Domains, add the IP address of the DMA server as a domain, and calls will be accepted by DMA in this format.
Cisco Unified CM SIP endpoint calls to DMA H.323 endpoints may be denied due to bandwidth

Possible Cause: When DMA invokes its SIP_to_H323 gateway feature, it is forced to look at bandwidth settings for H.323. The Cisco Unified CM SIP peer destination may not be defined in any sites in DMA (or RealPresence Resource Manager if integrated), so it denies the call.

Workaround: Add the Cisco Unified CM node’s subnet to the customer’s site topology. DMA does not look at bandwidth parameters for SIP calls—only H.323. You should add the Cisco Unified CM SIP peer to the site topology.

Calls from a Cisco CTS cannot connect to a DMA registered endpoint or RealPresence Collaboration Server

Possible Cause: The Cisco CTS IP Address may not be defined in the site topology.

Workaround: Add the Cisco CTS’s subnet or IP to the customer’s site topology in DMA under Network > Site Topology > Sites. If DMA is integrated with RealPresence Resource Manager, add it to the site topology there.

Calls from a Cisco CTS cannot connect to a DMA VMR

Possible Cause: DMA conference settings may be limiting the maximum bit rate for calls.

Workaround: In DMA under Admin > Conference Manager > Conference Settings, check that the Default maximum bit rate (kbps) is at least 4096 for CTS immersive connectivity.
Configuration Example

The following is a detailed configuration that shows all configuration entries necessary to make the SBC function for Polycom and Cisco equipment with detailed explanations:

! - Interface commands are required to build the address space that the SBC will be allowed to use for its operation
! - If the address space being assigned to a particular adjacency should NOT be routable anywhere else use of multiple interface commands as shown below is required

interface SBC1
ip address 172.20.0.130 255.255.255.224 secondary
ip address 172.20.0.131 255.255.255.224 secondary
ip address 172.20.0.132 255.255.255.224 secondary
ip address 172.20.0.133 255.255.255.224 secondary
ip address 172.20.0.134 255.255.255.224 secondary
ip address 172.20.0.135 255.255.255.224 secondary
ip address 172.20.0.136 255.255.255.224 secondary
ip address 172.20.0.137 255.255.255.224 secondary
ip address 172.20.0.138 255.255.255.224 secondary
ip address 172.20.0.139 255.255.255.224 secondary
ip address 172.20.0.140 255.255.255.224 secondary
ip address 172.20.0.139 255.255.255.224

interface SBC2
ip address 172.20.0.162 255.255.255.224 secondary
ip address 172.20.0.163 255.255.255.224 secondary
ip address 172.20.0.164 255.255.255.224 secondary
ip address 172.20.0.165 255.255.255.224 secondary
ip address 172.20.0.166 255.255.255.224 secondary
ip address 172.20.0.167 255.255.255.224 secondary
ip address 172.20.0.168 255.255.255.224 secondary
ip address 172.20.0.169 255.255.255.224 secondary
ip address 172.20.0.170 255.255.255.224 secondary
ip address 172.20.0.171 255.255.255.224 secondary
ip address 172.20.0.172 255.255.255.224 secondary

sbc plcm-sbc
sbe

! - “secure media” is required to support the passing of SRTP and DTLS - media through the SBC properly
secure-media
script-set 1 lua
! - “srtp-secure-media” script is required to allow SRTP and DTLS
! - SIP headers to pass through the SBC unchanged
    ! - this script must be loaded in the flash file system of the SBC
script srtp-secure-media
    filename bootflash:srtp_secure_media.lua
    load-order 100
    type full
    complete
! - “active-script-set” statement is required to turn on Lua scripts
active-script-set 1
    sip editor-type editor
! - all *-profile and *-editor configuration entries must be used exactly
! - as seen to permit the proper SIP headers and contacts to pass through
! - the SBC
    sip header-profile default
    header Allow entry 1
        action pass
    header Min-SE entry 1
        action pass
    header Reason entry 1
        action pass
    header SERVER entry 1
        action pass
    header Require entry 1
        action pass
    header Call-Info entry 1
        action pass
    header DIVERSION entry 1
        action pass
    header User-Agent entry 1
        action pass
    header Allow-Events entry 1
        action pass
    header session-expiry entry 1
        action pass
    header Remote-Party-ID entry 1
        action pass
    header Session-Expires entry 1
        action pass
    header RESOURCE-PRIORITY entry 1
        action pass
    header P-Asserted-Identity entry 1
        action pass
sip method-profile default
  pass-body
  method ACK
    action pass
  method INFO
    action pass
  method REFER
    action pass
  method INVITE
    action pass
  method NOTIFY
    action pass
  method OPTION
    action pass
  method UPDATE
    action pass
  method SUBSCRIBE
    action pass
sip option-profile default
  option TIMER
  option REPLACES
  sip header-editor in
    blacklist
    store-rule entry 1
      condition header-name session-expires header-value regex-match ";\(.*\)" store-as refreshparam
      header session-expires entry 1
        action replace-value value "1800"
        condition variable refreshparam is-defined eq false
      header session-expires entry 2
        action replace-value value "1800;$\{refreshparam\}"
        condition variable refreshparam is-defined eq true
! - The following three header-editor sections are required to allow
! - the X-cisco-srtp-fallback header to pass through the SBC
  sip header-editor tp-to-supported
    header x-supported entry 1
      action replace-name value "supported"
      condition status-code eq "200"
    header x-supported entry 2
      action replace-name value "supported"
      condition status-code eq "200"
    header x-supported entry 3
      action replace-name value "supported"
      condition status-code eq "200"
sip header-editor tp-add-x-srtp-fb
header srtp-fb entry 1
  action replace-name value "supported"
  condition status-code eq "200"
sip header-editor tp-to-x-supported
header srtp-fb entry 1
  action add-first-header value "X-cisco-srtp-fallback"
  condition status-code eq "200"
header supported entry 1
  action replace-name value "x-supported"
  condition status-code eq "200"
header supported entry 2
  action replace-name value "x-supported"
  condition status-code eq "200"
header supported entry 3
  action replace-name value "x-supported"
  condition status-code eq "200"
sip header-editor default
blacklist ! if using 3.7.2 replace “blacklist” with “whitelist”
header allow entry 1
  action pass
header min-se entry 1
  action pass
header reason entry 1
  action pass
header server entry 1
  action pass
header require entry 1
  action pass
header call-info entry 1
  action pass
header diversion entry 1
  action pass
header allow-events entry 1
  action pass
header session-expiry entry 1
  action pass
header remote-party-id entry 1
  action pass
header session-expires entry 1
  action pass
header resource-priority entry 1
  action pass
header p-asserted-identity entry 1
action pass
sip method-editor default
blacklist
method ack
  action pass
method info
  action pass
method refer
  action pass
method invite
  action pass
method notify
  action pass
method option
  action pass
method update
  action pass
method subscribe
  action pass
sip option-editor default
blacklist
option TIMER
option REPLACES
  ! - The first adjacency listed represents the “inside” unencrypted
  ! - call leg for DMA
adjacency sip DMA-Inside
nat force-off
editor-type editor
  ! - The following header editor statement is required to support
  ! - the passing of the X-cisco-srtp-fallback header
header-editor inbound tp-to-supported
  ! - the inherit profile statement pre-sets the way the SBC will treat
  ! - the traffic on this adjacency. This command is required on all
  ! - adjacency legs that represent the “inside” network
inhibit profile preset-core
hunting-trigger 408 500 503
preferred-transport tcp
  ! - security trusted-unencrypted forces the SBC to trust the inside
  ! - connection to DMA without TLS being active
security trusted-unencrypted
  ! - The DMA will see the address listed below in all communication
  ! - with the SBC, all registrations will also show up as being
  ! - from this IP Address
signaling-address ipv4 172.20.0.129
Configuration Example

! - signaling port is used to specify what port on the DMA is used
! - for inbound REGISTER and INVITE messages to the DMA
signaling-port 5060
signaling-peer <dns-name for site in DMA>
! - The following three lines permit REGISTER messages to be sent
registration target address <dns-name for site in DMA>
registration target port 5060
registration monitor
editor-list before-receive
editor 1 to_rtp_avp
   editor 2 tp-to-x-supported
editor-list after-send
editor 1 to_rtp_savp
! - the realm command allows specific addresses or address pools for
! - media to be used with this adjacency
realm dma-in
attach
! - This adjacency represents the “outside” half of the DMA-Inside
! - adjacency, it likewise is unencrypted
adjacency sip Cisco Unified CM-Outside
nat force-off
editor-type editor
   ! - The following header editor statement is required to support
   ! - the passing of the X-cisco-srtp-fallback header
header-editor outbound tp-add-x-srtp-fb
! - the inherit profile command shown here pre-sets the SBC to treat
! - calls and registrations traversing this adjacency to be on the
! - “outside” of the SBC
inherit profile preset-access
hunting-trigger 408 500 503
preferred-transport tcp
signaling-address ipv4 172.20.0.161
statistics method summary
signaling-port 5060
! - “Signaling-peer” allows this adjacency to accept calls from the
! - IP Address listed (as well as allows REGISTER messages from
! - any devices to pass through the adjacency)
signaling-peer 10.223.84.1
! - The following registration command is required to change the
! - contact headers in SIP REGISTER messages so that the SBC
! - can easily track and manage these devices
registration rewrite-register
! - The monitor command allows the registration process and device
! - counts to be monitored via the SBC CLI or SNMP
registration monitor
   ! - These “editor-list” commands are required to ensure DTLS
   ! - messages and crypto messages pass through this adjacency
editor-list before-receive
   editor 1 to_rtp_avp
editor-list after-send
   editor 1 to_rtp_savp
realm cucm-out
attach
   ! - This adjacency represents the inside leg of TLS encrypted
   ! - call traffic. Most configuration items here are exactly the
   ! - same as those for unencrypted adjacencies. Differences are
   ! - noted below.
adjacency sip TLS-Inside
nat force-off
editor-type editor
inherit profile preset-core
header-editor inbound tp-to-supported
preferred-transport tcp
   ! - “trusted-encrypted” forces the use of TLS. TCP or
   ! - unencrypted signaling traffic is not allowed to pass
   ! - this adjacency.
security trusted-encrypted
signaling-address ipv4 172.20.0.130
   ! - TLS typically uses port 5061.
signaling-port 5061
signaling-peer <DMA DNS site name>
   ! - This specifies the local signaling port that the SBC uses to
   ! - contact DMA.
signaling-peer-port 5061
registration target address <DMA DNS site address>
registration target port 5061
registration monitor
editor-list before-receive
   editor 1 to_rtp_avp
       editor 2 tp-to-x-supported
editor-list after-send
   editor 1 to_rtp_savp
realm dma-tls-in
attach
   ! - This adjacency represents the outside half of the TLS encrypted
   ! - call control traffic.
adjacency sip TLS-Outside
nat force-off
editor-type editor
header-editor outbound tp-add-x-srtp-fb
  inherit profile preset-access
hunting-trigger 408 500 503
security trusted-encrypted
signaling-address ipv4 172.20.0.162
signaling-port 5061
signaling-peer 10.223.84.1
signaling-peer-port 5061
registration rewrite-register
  ! - The “header-name” configuration entry is required to maintain the
  ! - use of TLS for all aspects of call control traffic.
header-name Contact add tls-param
editor-list before-receive
  editor 1 to_rtp_avp
editor-list after-send
  editor 1 to_rtp_savp
realm tls-out
attach
  ! - QoS policy statements determine how the SBC will mark, or pass
  ! - packets requiring QoS.
qos voice qvoice
marking passthrough
qos video qvideo
marking passthrough
qos sig qsig
marking passthrough
  ! - The “cac-policy-set” statement determines the call-admission
  ! - control for all calls flowing through the SBC. The settings
  ! - shown below are all required (excepting QoS) to make TIP/DTLS
  ! - encryption functional with TIP/CTS endpoints.
cac-policy-set 3
first-cac-table Plcm
first-cac-scope call
cac-table Plcm
table-type policy-set
entry 1
cac-scope call
srtp support allow
callee-video-qos-profile qvideo
callee-voice-qos-profile qvoice
callee-sig-qos-profile qsig
caller-video-qos-profile qvideo
caller-voice-qos-profile qvoice
caller-sig-qos-profile qsig
media bandwidth-field ignore
caller secure-media
callee secure-media
generic-stream caller my-stream
generic-stream callee my-stream
action cac-complete

complete
! - A call-policy-set is required to specify how traffic may pass into
! - and out of an adjacency. A bi-directional path must be built per
! - pair of adjacency configurations otherwise traffic will not pass.
call-policy-set 4
first-call-routing-table INCOMING
first-reg-routing-table INCOMING
rtg-src-adjacency-table INCOMING
  entry 1
  match-adjacency Cisco Unified CM-Outside
dst-adjacency DMA-Inside
  action complete
  entry 2
  match-adjacency DMA-Inside
dst-adjacency Cisco Unified CM-Outside
  action complete
  entry 3
  match-adjacency TLS-Outside
dst-adjacency TLS-Inside
  action complete
  entry 4
  match-adjacency TLS-Inside
dst-adjacency TLS-Outside
  action complete
complete
call-policy-set default 4
network-id 19267
sip timer
tcp-idle-timeout 180000
! - The following SIP dns commands set the TTL for all resolved
! - names on DMA to timeout immediately after use permitting DMA
! - to determine which callserver is the active server
sip dns
  support-type sip-dns-srv
  cache lifetime 0
  cache limit 0
!
! - Additional custom stream is required to allow BFCP to pass through the SBC properly
stream-list my-stream
generic-stream media-type application transport udp protocol BFCP
! SBC default blacklist settings apply.
! show sbc <name> sbe blacklist configured-limits
!
! - media commands are required to let the SBC pass media between adjacencies correctly. A single address or a pool may be used for each entry. If a “realm” is specific on an adjacency, it must also be specified on a media address or pool so that the adjacency will handle media
media-address ipv4 172.20.0.138 realm dma-in
  port-range 16384 32767 any
media-address ipv4 172.20.0.139 realm dma-tls-in
  port-range 16384 32767 any
media-address ipv4 172.20.0.169 realm cucm-out
  port-range 16384 32767 any
media-address ipv4 172.20.0.170 realm tls-out
  port-range 16384 32767 any
media-timeout 300
activate
!
!